PRÁCTICAS DE LABORATORIO

Guillermina Antonaccio

Vigésimo segundo laboratorio (267):

Creación de su VPC y lanzamiento de un servidor web

Instructor:
Roberto Landa

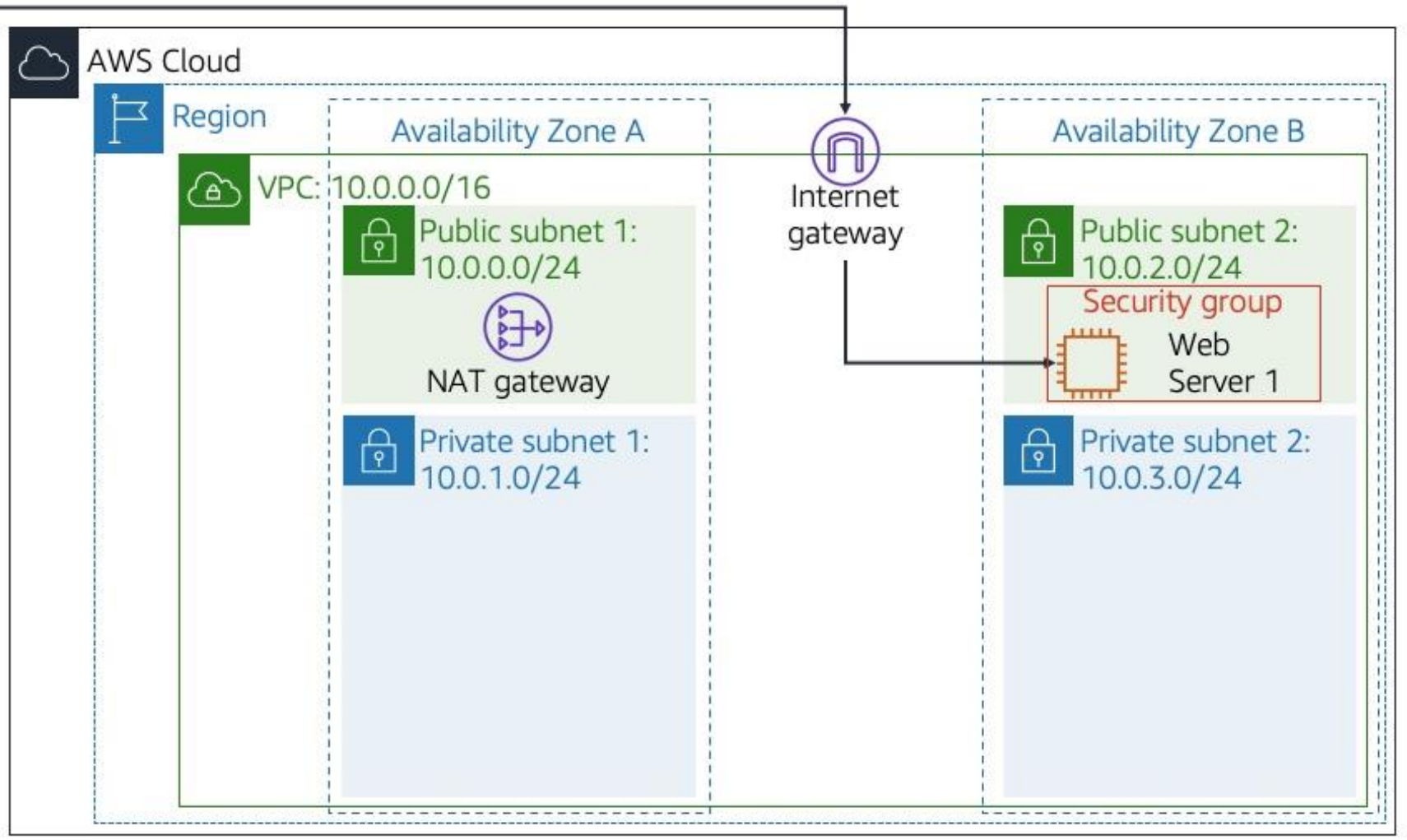
Arquitectura que debíamos realizar:

Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT Gateway

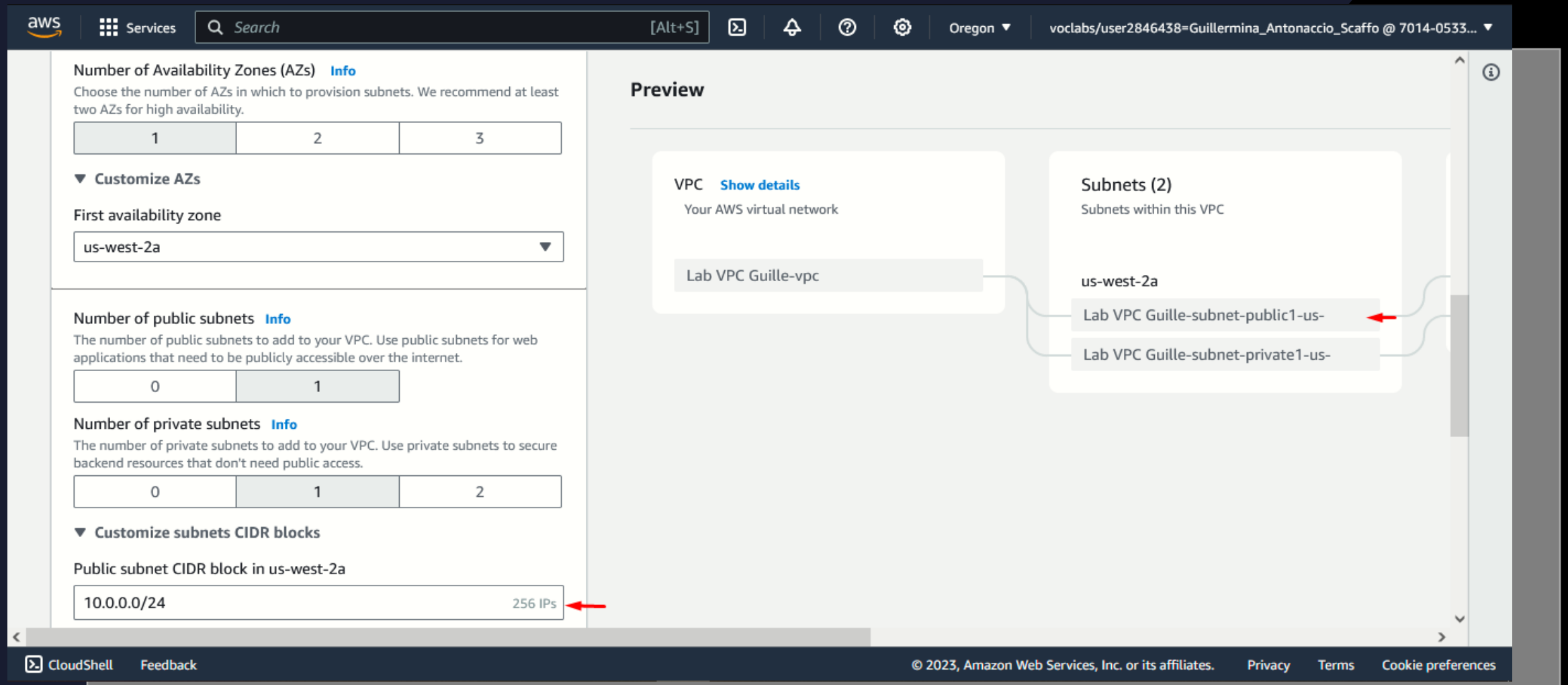


TAREA 1: 

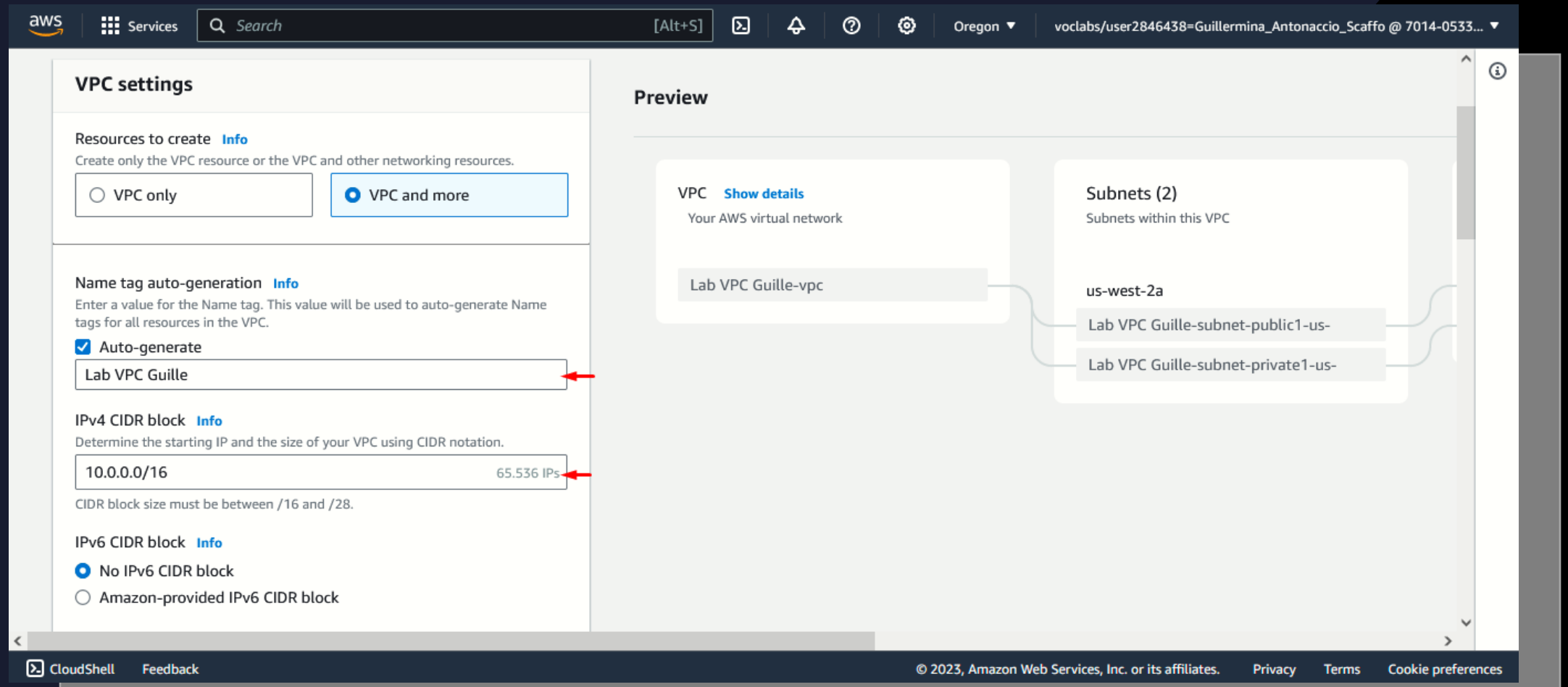
En esta tarea, debíamos crear la VPC con las siguientes características:

1-Un bloque CIDR 10.0.0.0/16
2- Una zona de disponibilidad (a)
3- Una subnet publica con CIDR: 10.0.0.0/24
4-Una subnet privada con CIDR:10.0.1.0/24
5-Una puerta de enlace NAT para proporcionar conectividad a internet a instancias EC2 en subredes privadas

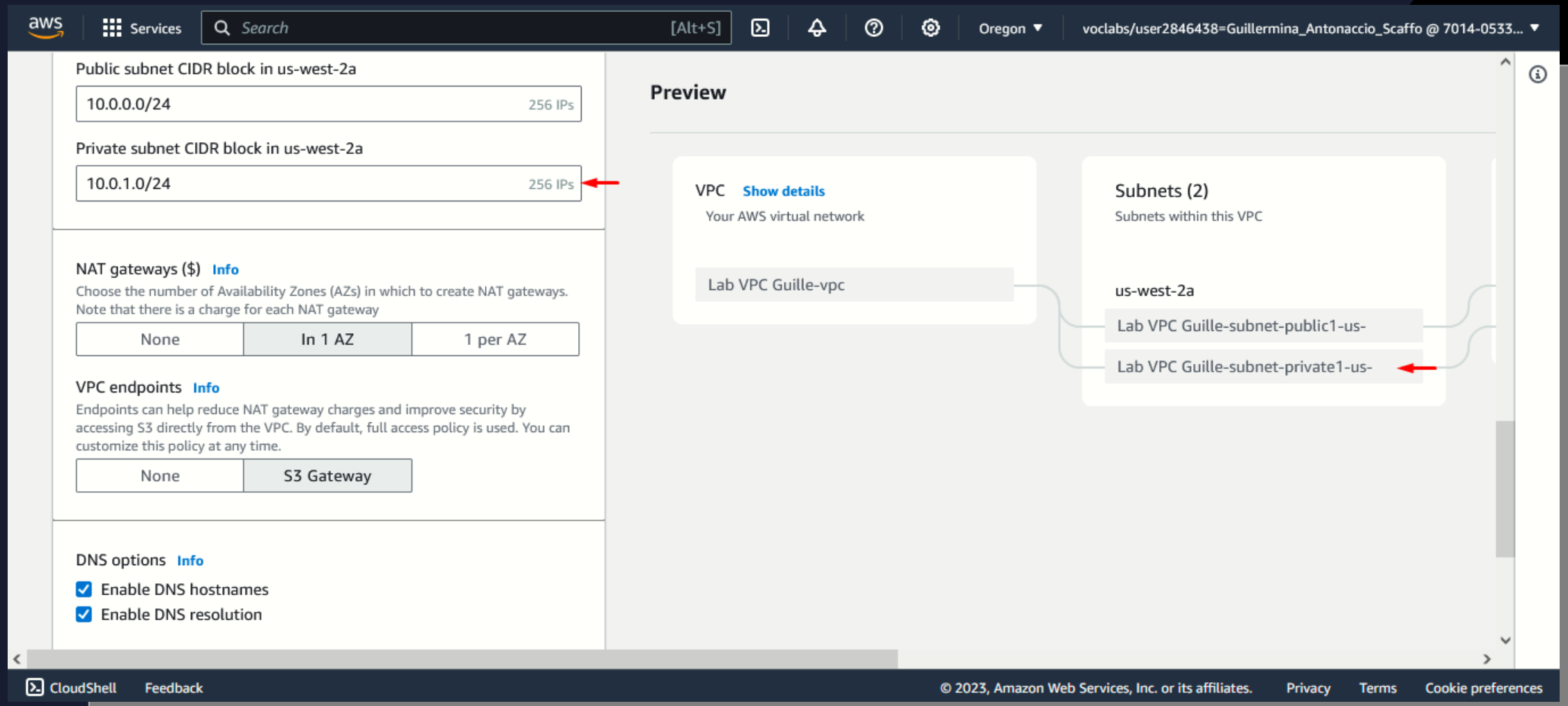
En esta parte asignamos el número de subnets públicas y privadas, la zona de disponibilidad y el bloque CIDR de la subnet pública:



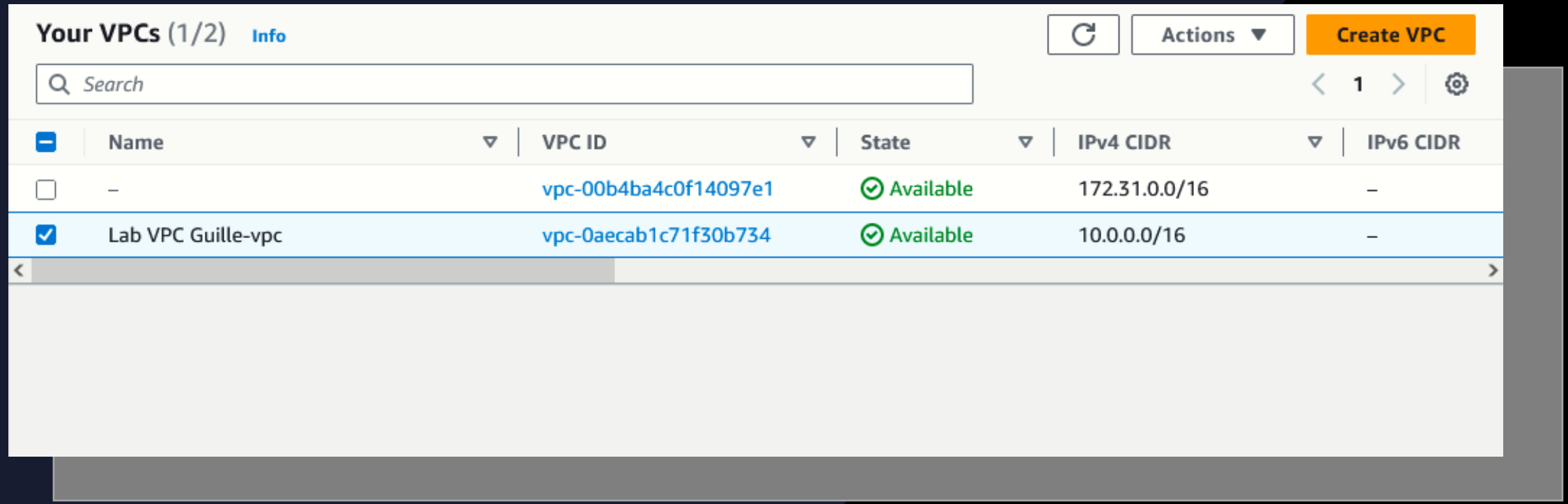
A continuación se muestran imágenes de la configuración del bloque CIDR de la VPC:



Aquí asignamos el bloque CIDR de la subnet privada y colocamos una NAT gateway en nuestra AZ:



Así se ve la VPC una vez creada con éxito:

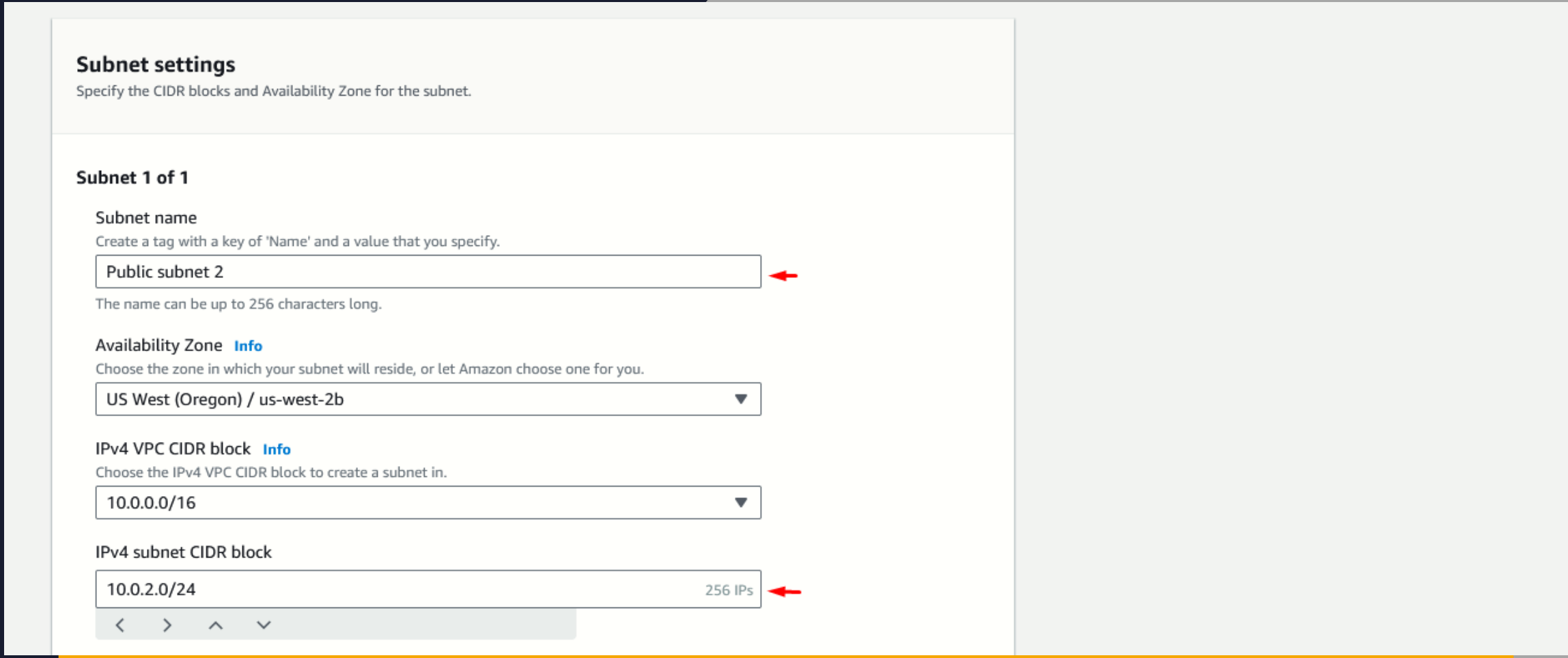


TAREA 2:

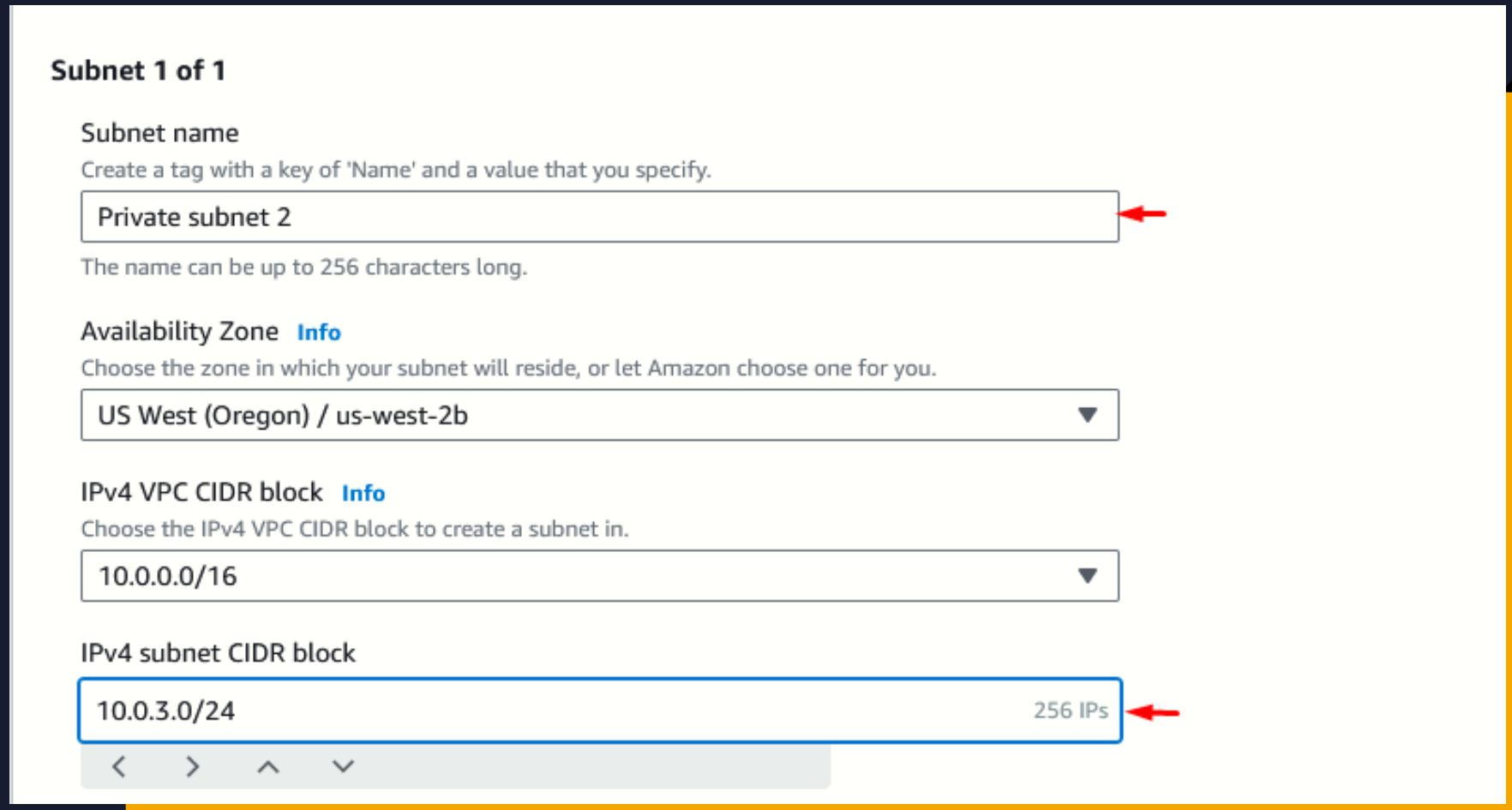
En esta tarea, debíamos crear subredes adicionales en nuestra VPC y que las mismas estuvieran en otra AZ.

1-Debiamos crear una subnet publica con un bloque CIDR: 10.0.2.0/24 que estuviera en la AZ (b)
2-Luego creamos una subnet privada con un bloque CIDR:10.0.3.0/24 esta también debía estar en la AZ (b)

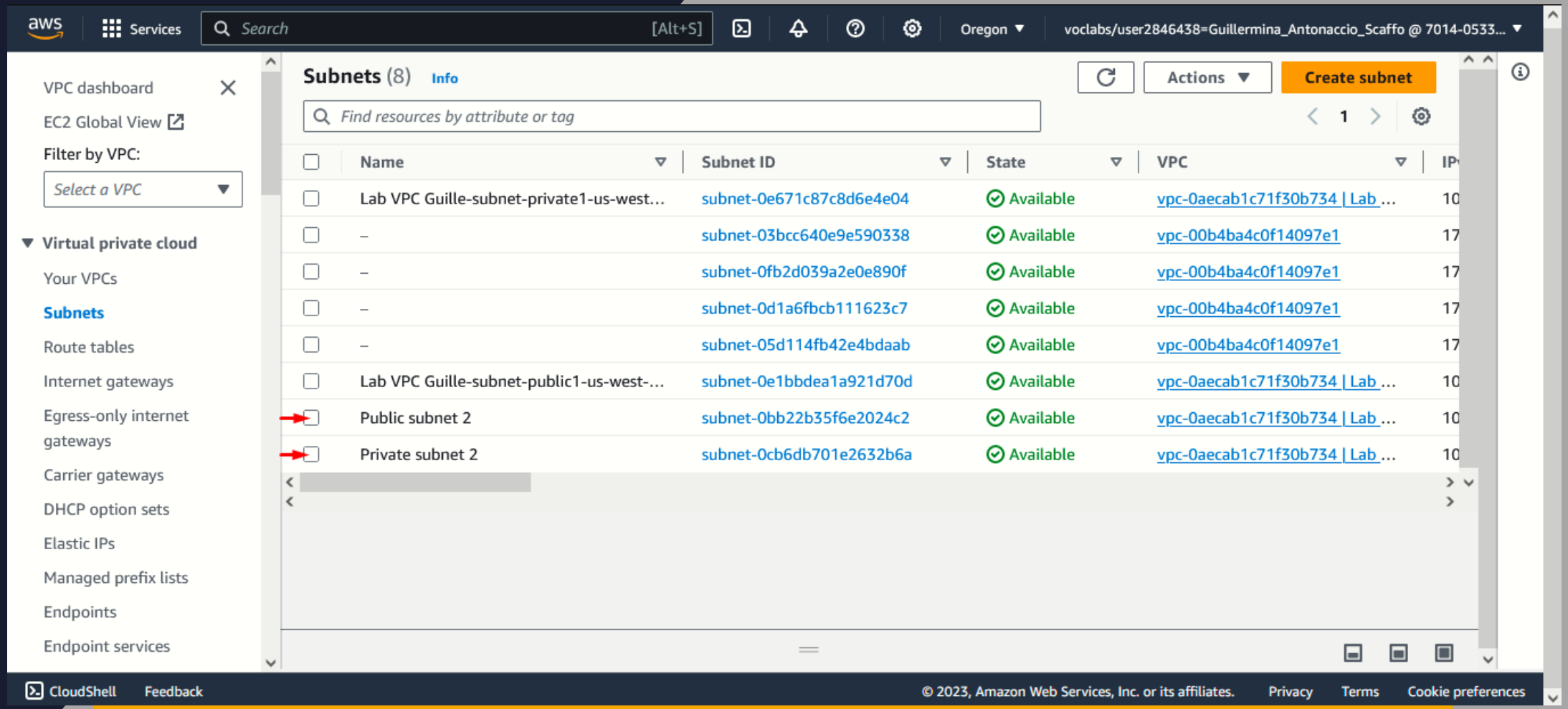
En esta imagen podemos observar la creación de las subnet pública y su zona de disponibilidad.



Aquí se ve la creación de la subnet privada:



Las subnets una vez creadas:

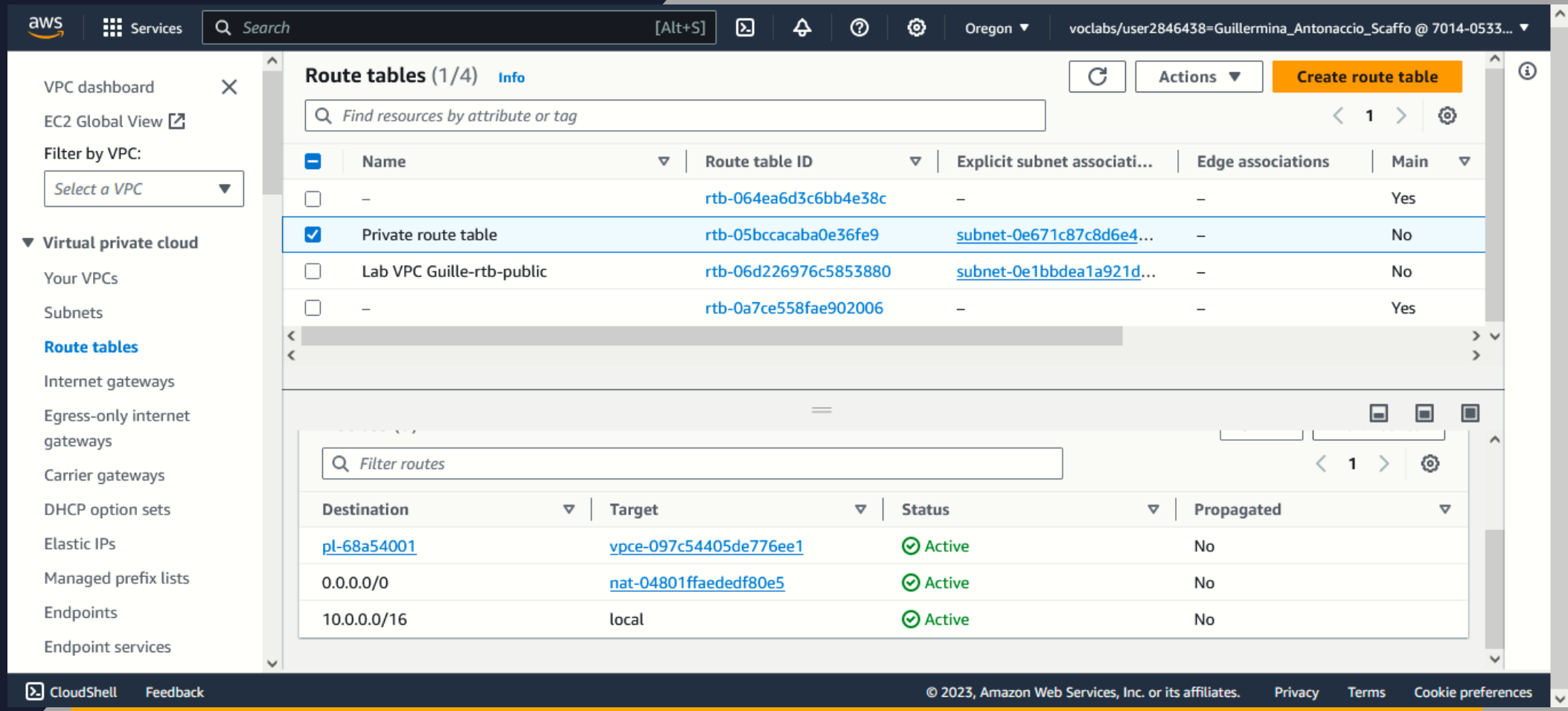


TAREA 3:

En esta consigna, debíamos configurar la tabla de rutas, para esto lo que hicimos fue:

1-En el panel de tabla de rutas buscamos la que se llamaba Lab VPC en la columna nombre y la seleccionamos.
2-En el apartado de abajo, en rutas, destination aparecía configurado para 0.0.0.0/0 y target estaba configurado en nat-xxxxxx esto lo que significa es que esa tabla de rutas se utiliza para enrutar el tráfico desde subredes privadas.
3-Cambiamos el nombre de la tabla de rutas Lab VPC, por Private Route Table.

En esta imagen cambiamos el nombre *"Lab VPC"* por *"Private route table"*, y si vemos en el apartado de abajo, aparece destination 0.0.0.0/0 y target nat, esto significa que esta tabla de rutas es para enrutar el tráfico de subredes privadas.



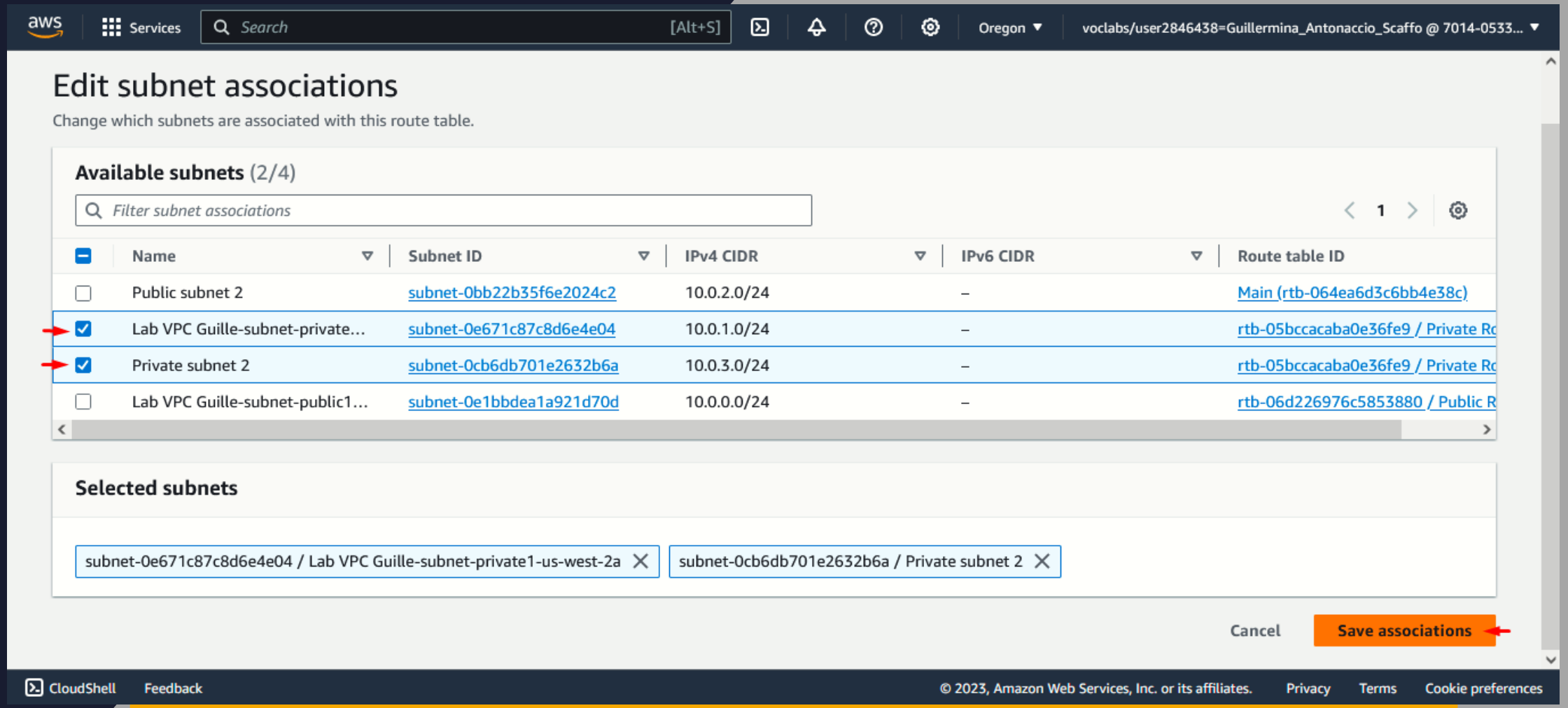
TAREA 4:

En esta tarea, teníamos que fijarnos en las tablas de enrutamiento, la que se llamaba Lab VPC public, esta es una tabla de enrutamiento pública ya que tenía destination 0.0.0.0/0 y target igw (internet gateway) por lo tanto la renombramos y le pusimos: Public Route Table.

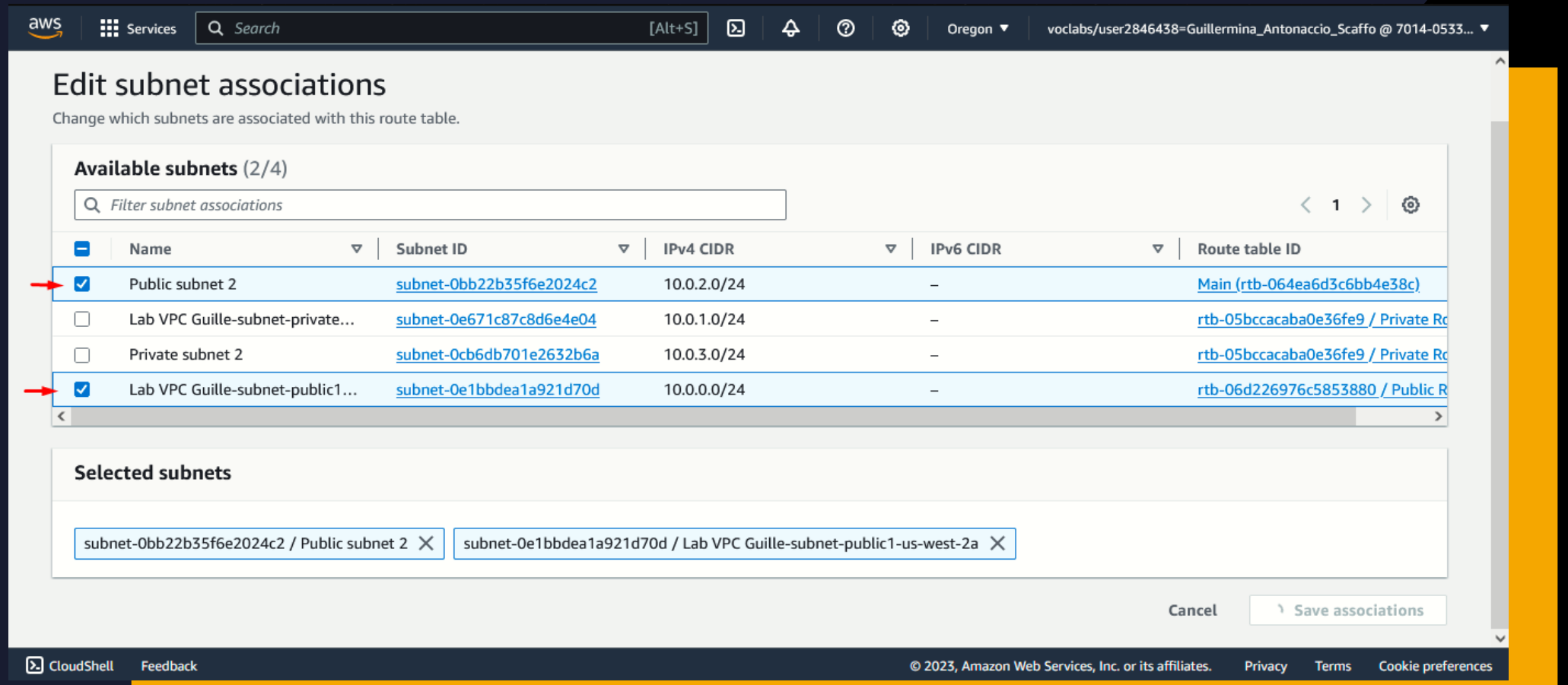
Una vez hecho esto, tenemos las dos tablas de rutas hechas, por lo que ahora debíamos asociar las subnets a cada ruta correspondiente.

1-Asociamos las dos subredes públicas (la de AZ a y AZ b) a Public Route Table
2-Asociamos las dos subredes privadas (la de AZ a y AZ b) a Private Route Table

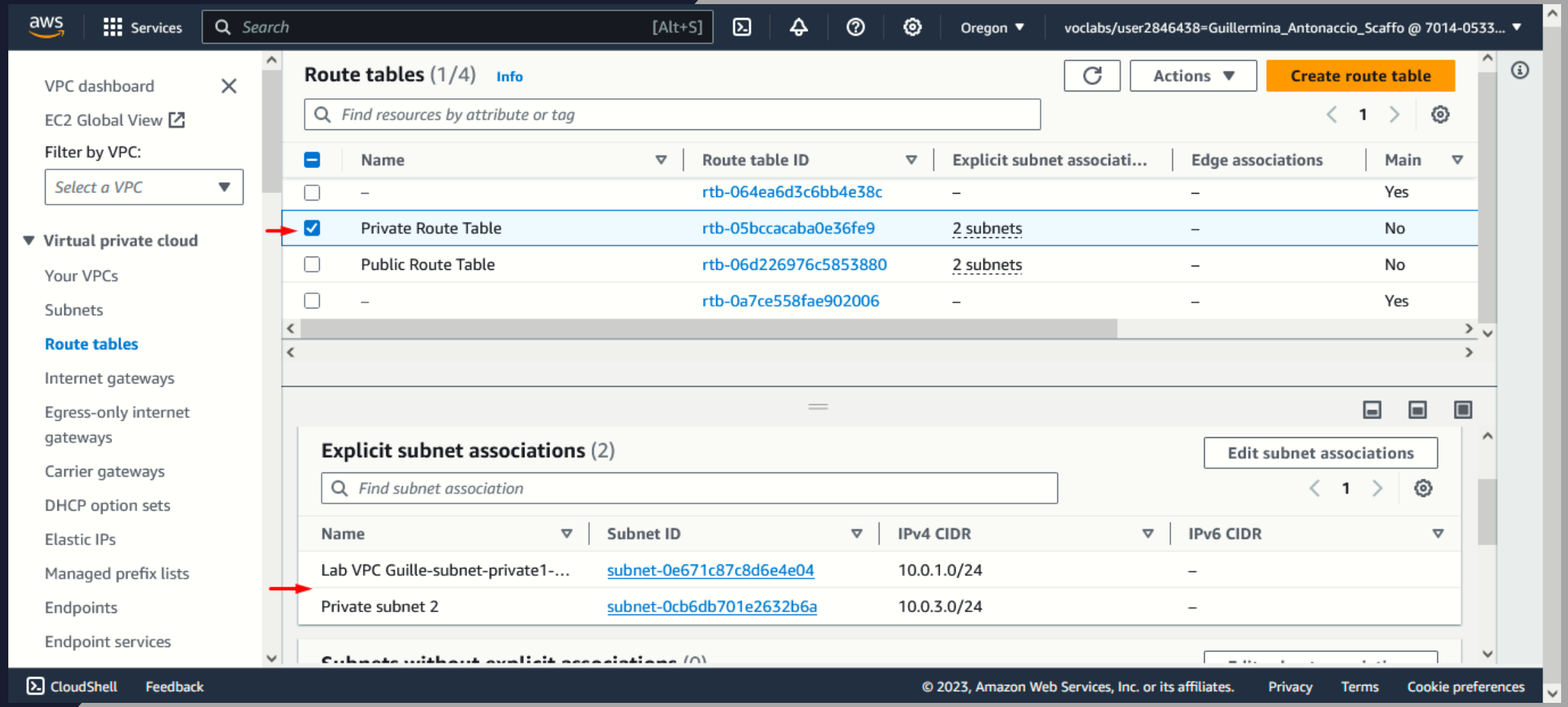
Aquí podemos ver la asociación de las dos subnets privadas a la Tabla de enrutamiento privado



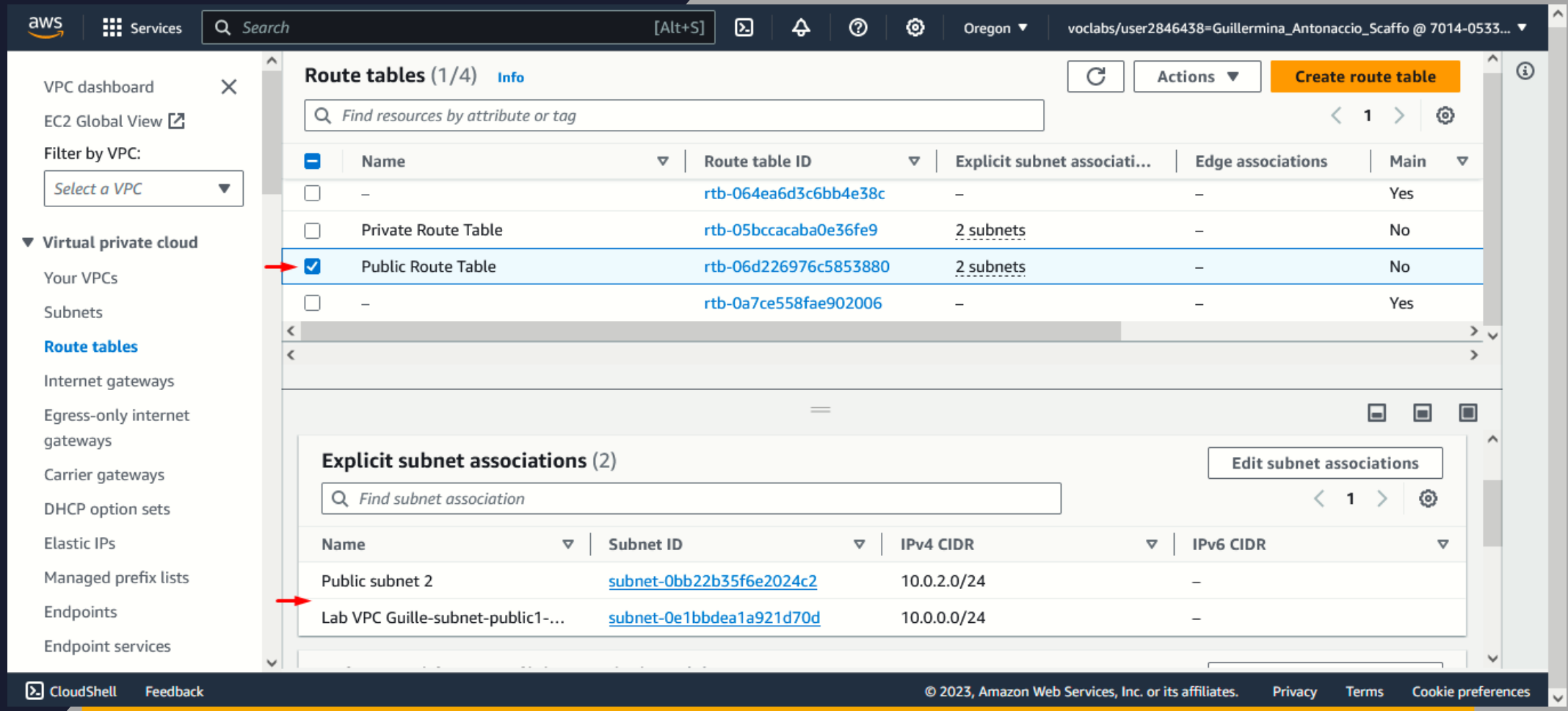
Asociación de las subnets públicas a la tabla de enrutamiento pública:



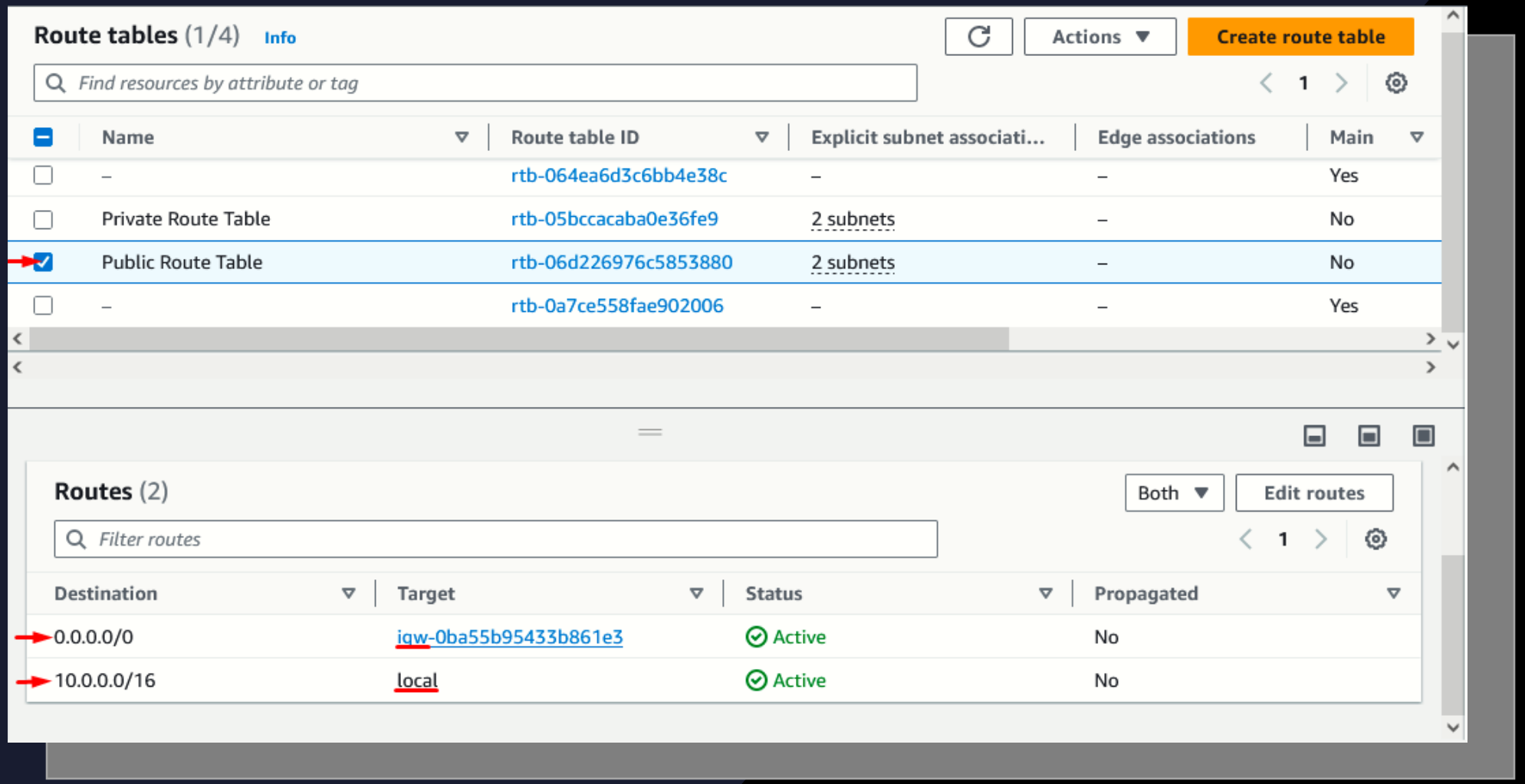
Cuando seleccionamos la tabla de enrutamiento privada, podemos ver que las subnets privadas se asociaron con éxito.



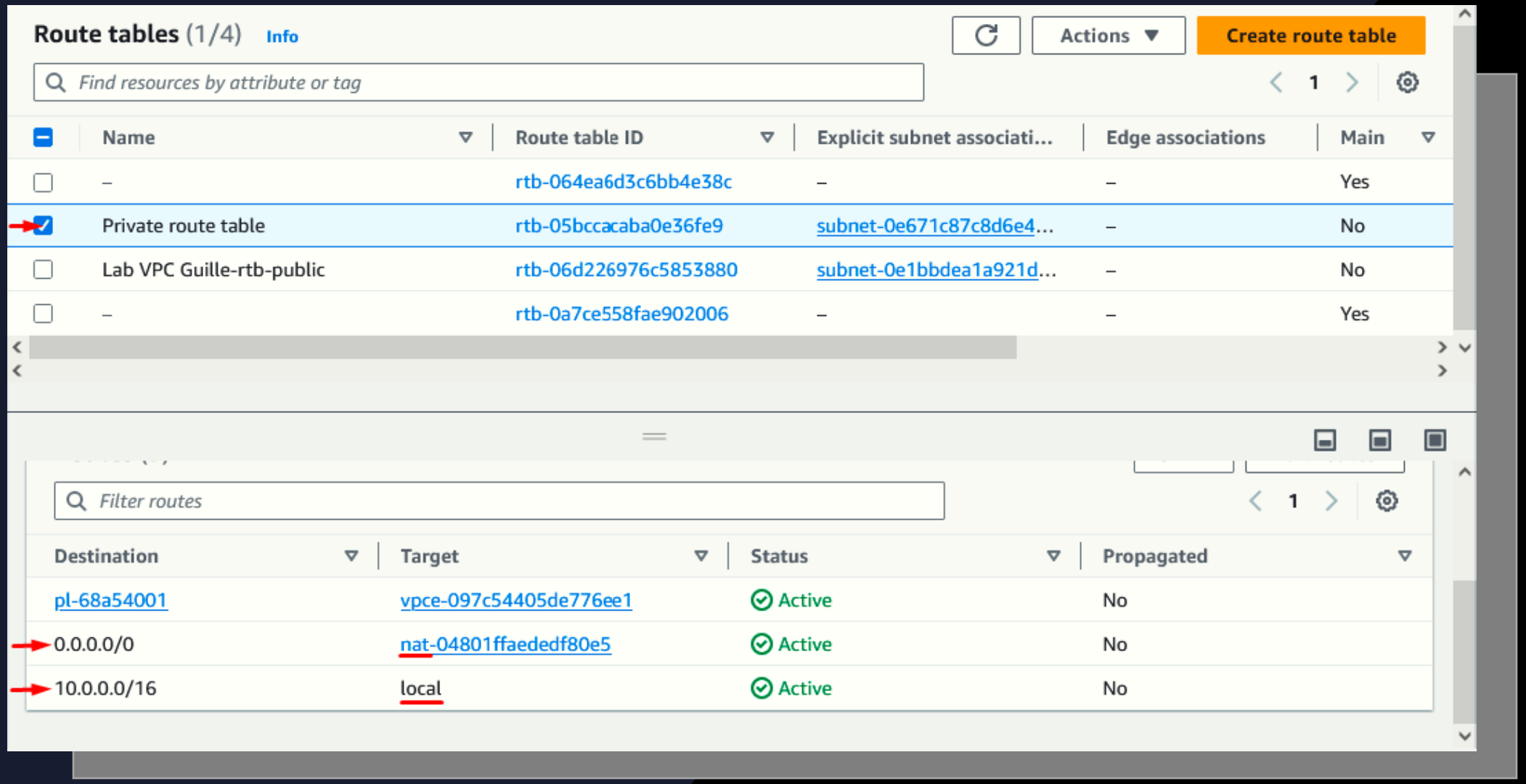
Lo mismo ocurre para la tabla de enrutamiento pública.



Por ultimo podemos ver como en la tabla de enrutamiento publica, las rutas que tienen son igw (internet gate way) y local, por lo tanto con esto confirmamos que la tabla sí es pública.

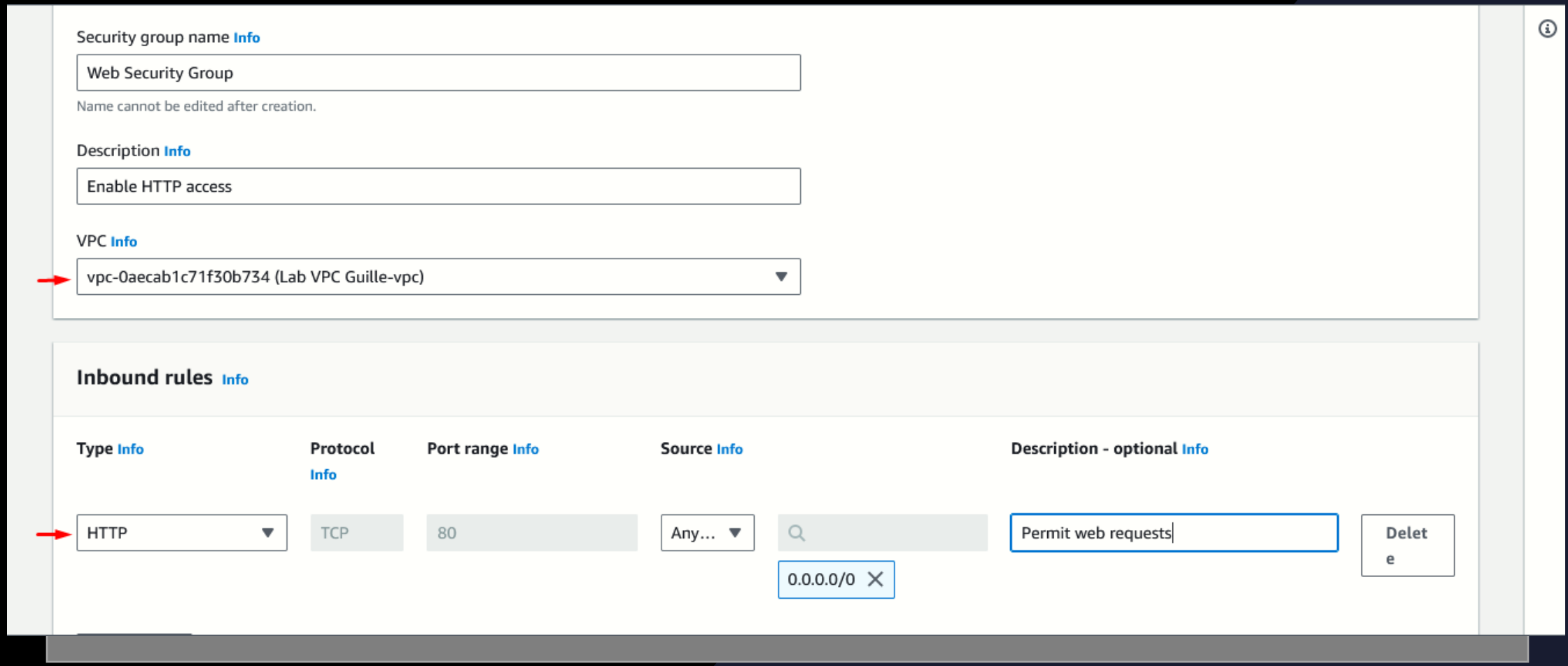


Lo mismo podemos confirmar con la tabla de enrutamiento privada, ya que tiene como rutas NAT y local.

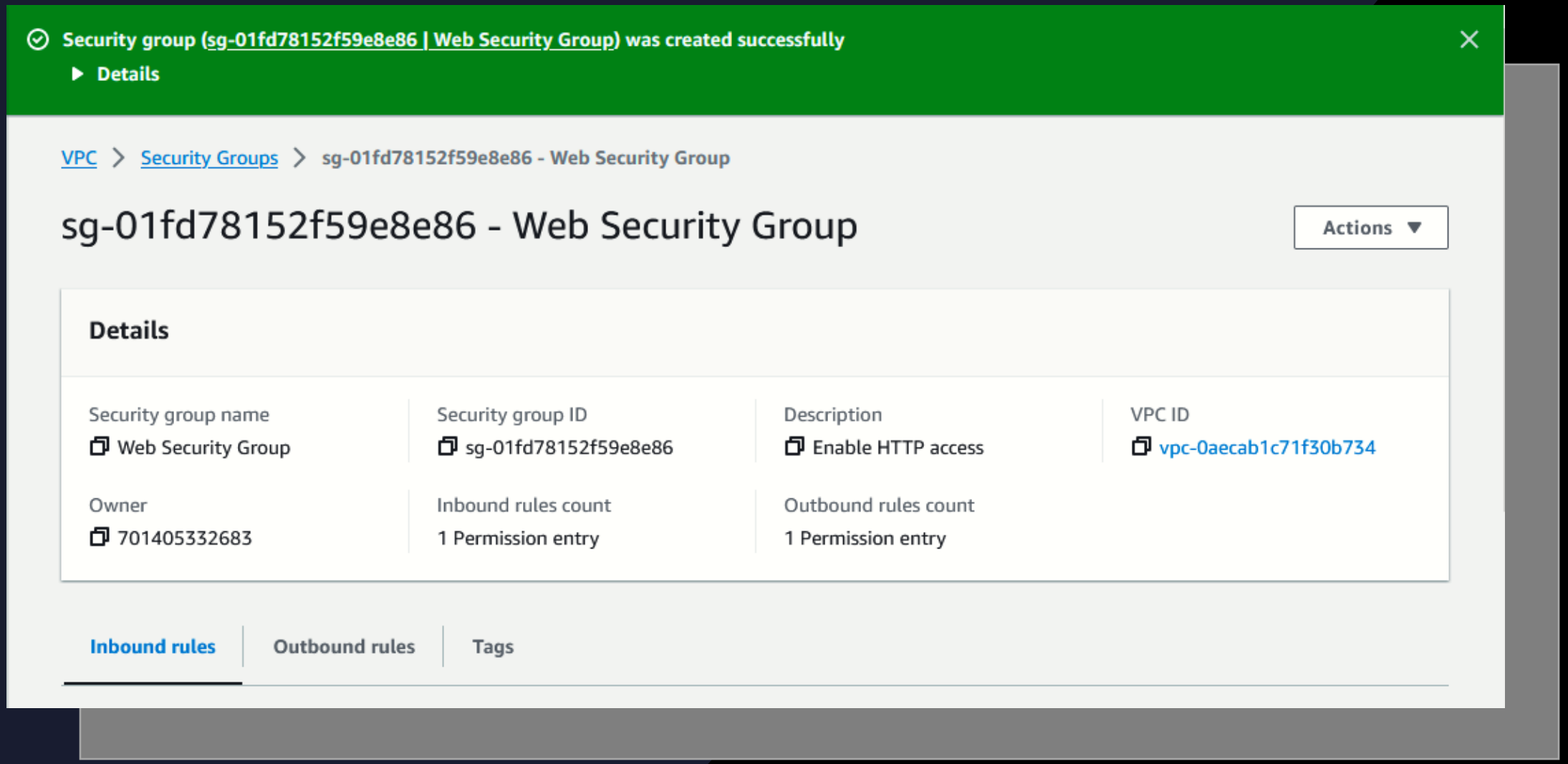


TAREA 5:

En esta tarea, debíamos crear un grupo de seguridad para la VPC, para que actuara como firewall de la instancia. Lo configuramos para que permita solicitudes web entrantes.



El grupo de seguridad una vez creado exitosamente:



TAREA 6:

En esta tarea, debíamos crear una instancia EC2 que estuviera en la VPC dentro de la AZ (b) en la subred pública. Esta instancia está configurada para que actúe como un servidor web. Para ello realizamos los siguientes pasos:

1-Elegimos **Amazon Linux 2 AMI (HVM): kernel 5.10, tipo de volumen SSD** para la imagen de la instancia.

2-En tipo de instancia seleccionamos t2.micro.

3-En configuraciones de red elegimos nuestra VPC y la subred publica 2 (que se encuentra en la AZ b)

4-Copiamos un código en datos de usuario para que se creara automáticamente la página en la EC2.

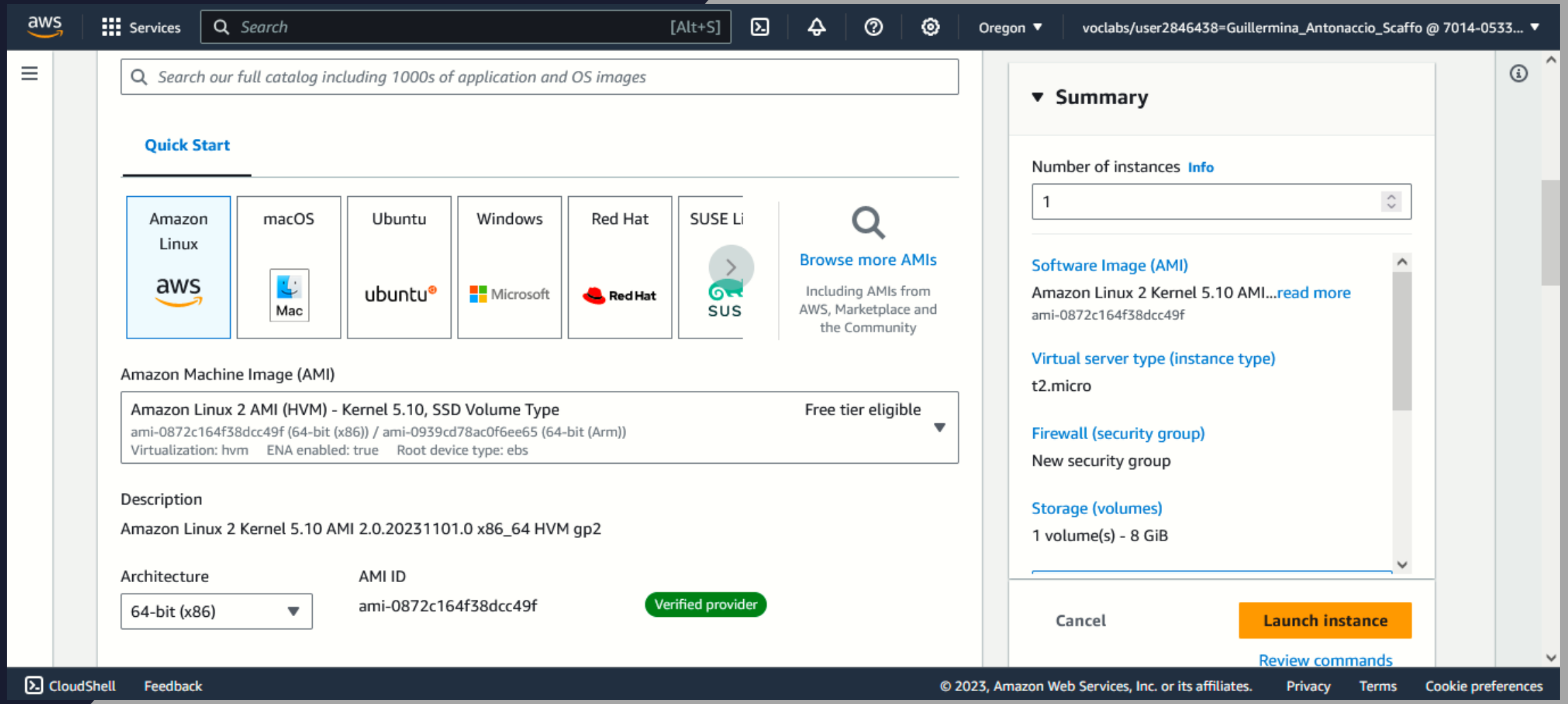
5-Asignamos el grupo de seguridad que habíamos creado anteriormente

6-Dejamos la configuración predeterminada en almacenamiento

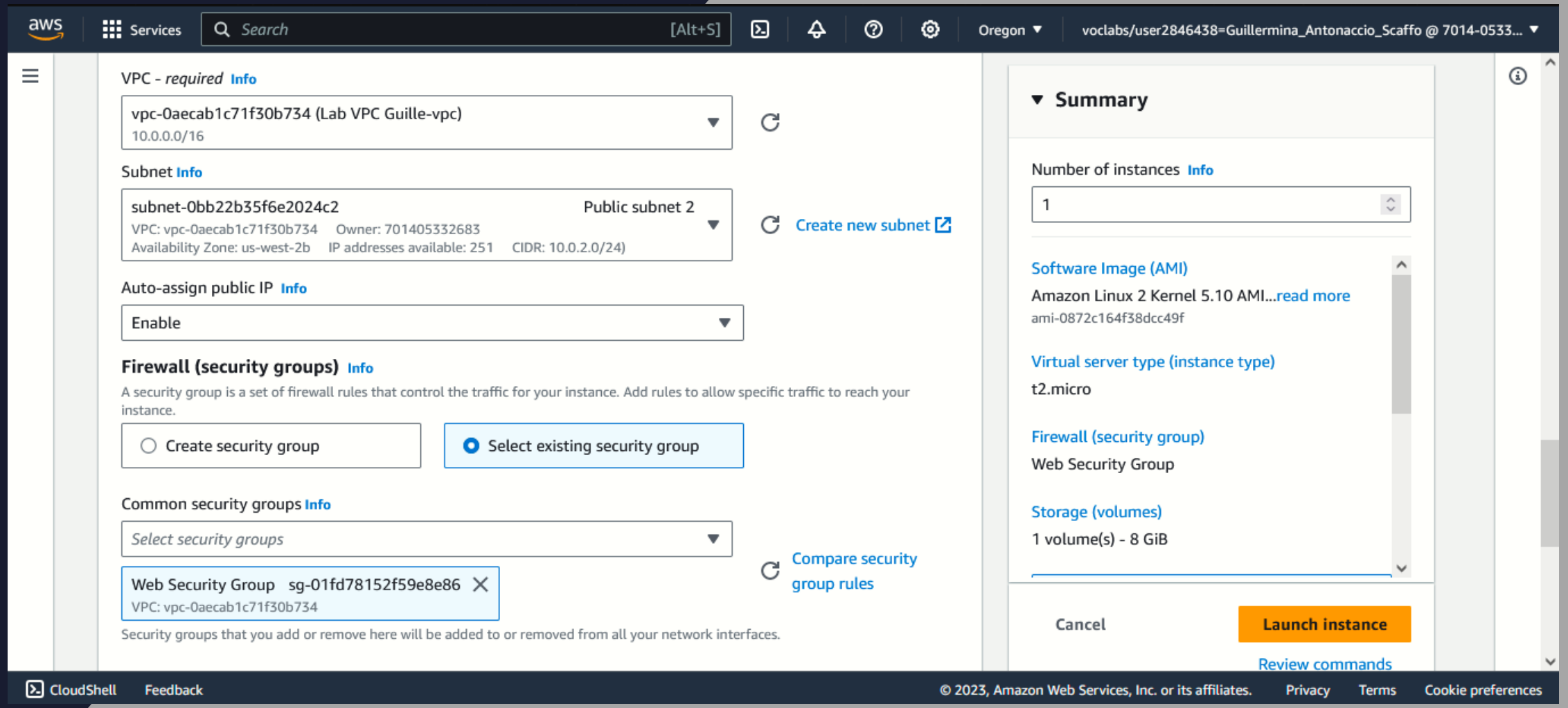
7-Agregamos una etiqueta con clave-valor.

8-En llave seleccionamos vockey RSA

En este apartado elegimos la imágen de la instancia

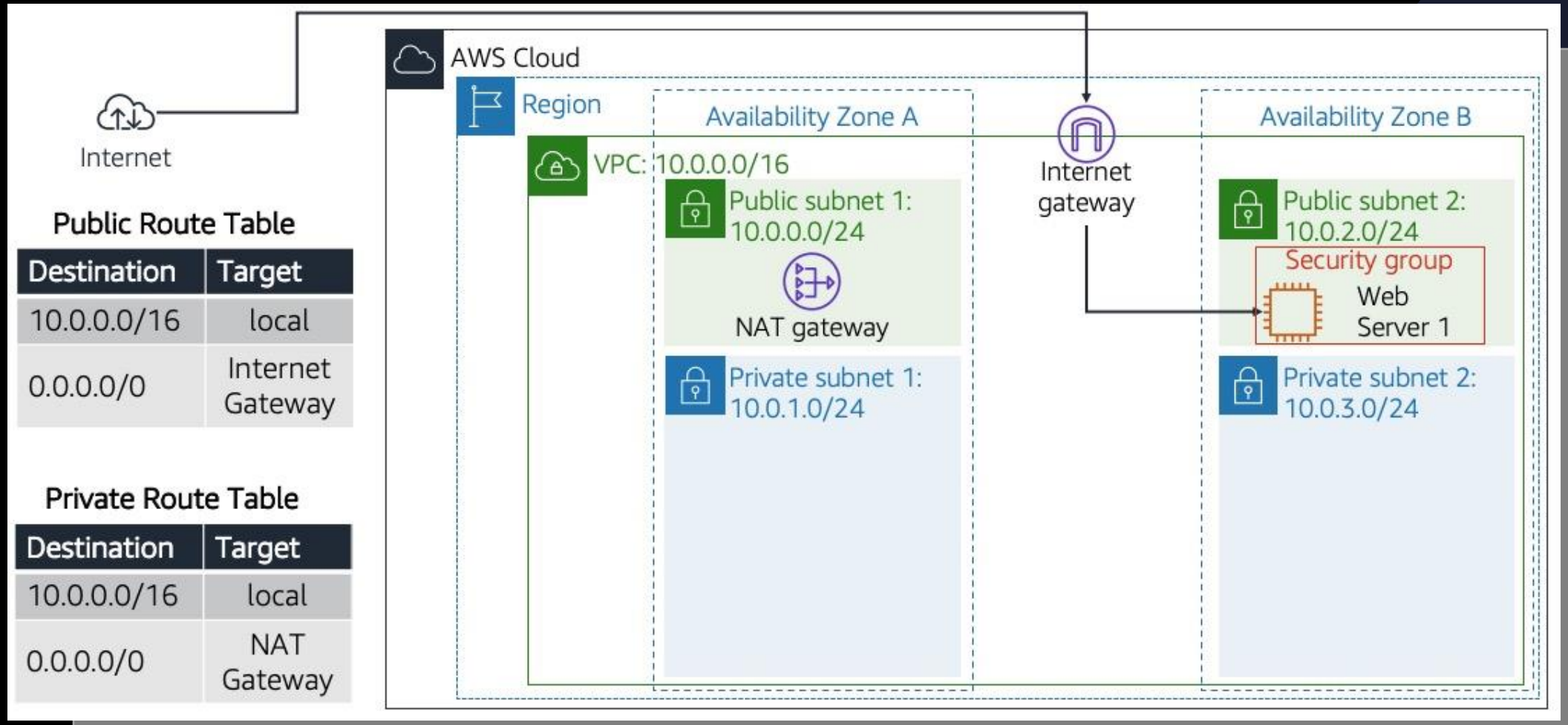


Aquí seleccionamos la VPC que habíamos creado para la instancia, la subnet publica 2 y el grupo de seguridad:



Una vez iniciada la instancia con éxito, copiamos la IP publica de la misma, la pegamos en el navegador y aquí podemos ver la página funcionando con éxito, esto significa que logramos configurar todo correctamente:

Así se ve el producto final, el cual es una VPC completamente funcional con sus recursos (red y seguridad) y un servidor web activado.



Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT Gateway

Aquí termina el laboratorio, muchas gracias