

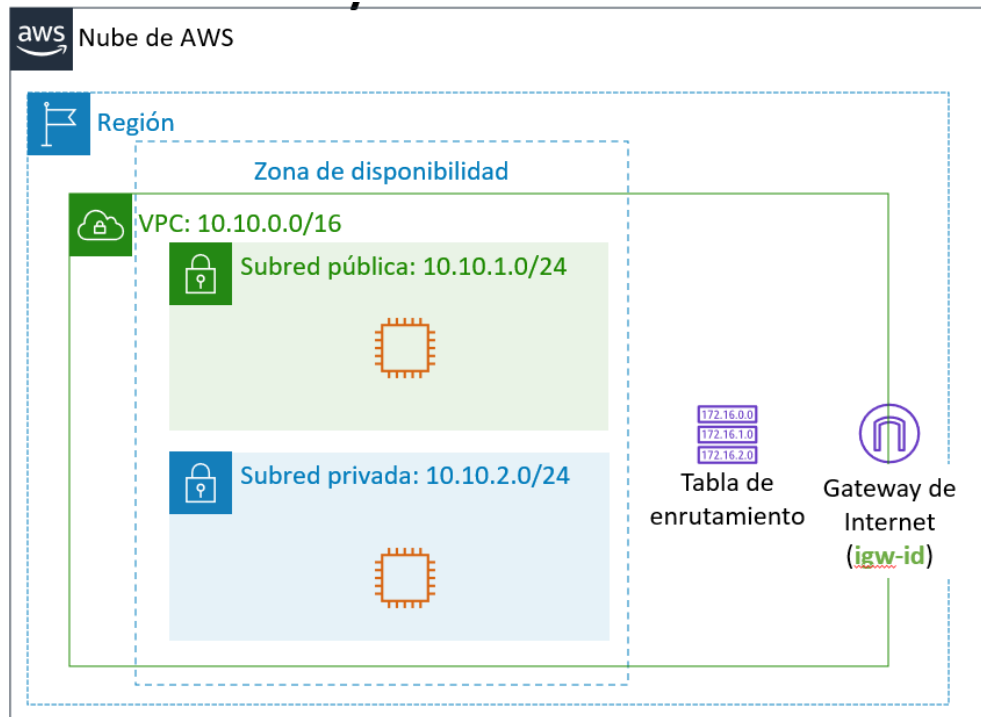
UD.1 Practica 4. VPC y servidor Libre



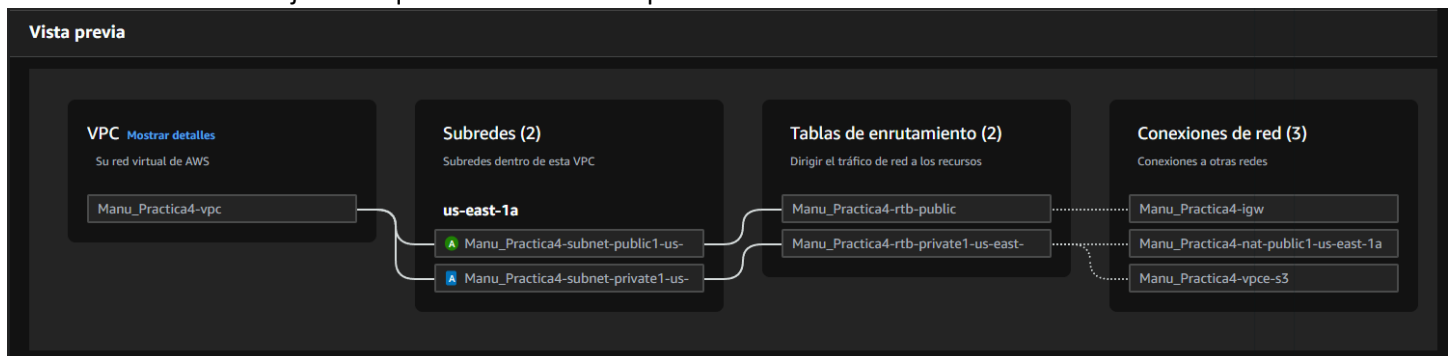
1.	Crear VPC	3
2.	Crear el grupo de seguridad para internet.....	4
3.	Creamos instancia EC2 en la subred pública. Lanzada desde la consola.....	5
4.	Probar que el servidor funciona, probar ACLs y conectividades	6
5.	Buscar diferentes configuraciones de lanzamiento en datos de usuario: crear un fichero	7
6.	Emplea la herramienta Reachability analyzer para ver que todo está bien	9
7.	Gateway NAT.....	9
8.	Deshabilitar Gateway NAT	10

1. Crear VPC

- Creamos VPC con nuestro nombre. En us-east-1 Usamos CIDR IPv4, no el IPv6. Rango de direcciones privadas: 10.10.0.0/16.
- Creamos 2 subredes (1 privada y 1 públicas) en una única AZ, con el asistente. Nombre_privada1 ; Nombre_publica1. Debemos tener 1 NAT gateway en la AZ



Adjunto esquema de red creado por el VPC Wizard



Creo la VPC con rango 10.10.0.0/16. Activo la opción de DNS en acciones, que me vendrá bien para luego configurar los servicios.

Compruebo los rangos y asigno la mitad de las direcciones a cada subred

	Name	ID de subred	Estado	VPC	CIDR IPv4
	Manu_Practica4-subnet-public1-us-east...	subnet-0238075e2fbc623db	✓ Available.	vpc-0a7e50bd1b378b118 Ma...	10.10.0.0/20
	Manu_Practica4-subnet-private1-us-eas...	subnet-0894d6ddfb670ce0f	✓ Available.	vpc-0a7e50bd1b378b118 Ma...	10.10.128.0/20

- De momento no creo un internet Gateway NAT pero lo crearle manualmente después)

Doy a crear la VPC

2. Crear el grupo de seguridad para internet

- Creamos un grupo de seguridad "Web Security Group" que de a acceso HTTP y HTTPS

Reglas de entrada:

Crear grupo de seguridad Información

Un grupo de seguridad actúa como un firewall virtual para que la instancia controle el tráfico de entrada y salida. Para crear un nuevo grupo de seguridad, complete los campos siguientes.

Detalles básicos

Nombre del grupo de seguridad Información

El nombre no se puede editar después de su creación.

Descripción Información

VPC Información

Reglas de entrada Información

Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>	Descripción: opcional <small>Información</small>	
HTTP	TCP	80	Anywhere...	0.0.0.0/0	Permitir solicitudes web Eliminar
HTTPS	TCP	443	Anywhere...	0.0.0.0/0	Permitir solicitudes web Eliminar

Agregar regla

Source (Origen): Anywhere (Cualquiera)

Description (Descripción): Permitir solicitudes web

3. Creamos instancia EC2 en la subred pública. Lanzada desde la consola

- Nombre: Tunombre_Server_I_P4
Ej: Ruth_Server_I_P4
- tipo t2.micro
- AMI: mira en el catálogo de la comunidad, y en modelo de precios, filtra por “free”
- Para esta ocasión finalmente vamos a lanzar un Ubuntu Server
- Red y Subred: asegúrate de que está en la red/sub red adecuadas
- Auto-assign Public IP (Asignar automáticamente IP pública): Enable
- Selecciona el grupo de Web Security Group para lanzarlo
- Emplea las claves de vockey para acceder al servidor

▼ Configuraciones de red [Información](#)

VPC: obligatorio [Información](#)

vpc-0a7e50bd1b378b118 (Manu_Practica4-vpc)
10.10.0.0/16

Subred [Información](#)

subnet-0238075e2fbc623db Manu_Practica4-subnet-public1-us-east-1a
VPC: vpc-0a7e50bd1b378b118 Propietario: 852235009910
Zona de disponibilidad: us-east-1a Tipo de zona: Zona de disponibilidad
Direcciones IP disponibles: 4090 CIDR: 10.10.0.0/20

Asignar automáticamente la IP pública [Información](#)

Habilitar

Se aplican [cargos adicionales](#) cuando no se cumplen los límites del [nivel gratuito](#)

Firewall (grupos de seguridad) [Información](#)
Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

● Crear grupo de seguridad ● Seleccionar un grupo de seguridad existente

Grupos de seguridad comunes [Información](#)

Seleccionar grupos de seguridad

Web Security Group sg-05ee0256e738f5e5b X
VPC: vpc-0a7e50bd1b378b118

Compare reglas de grupo de seguridad

Los grupos de seguridad que agrega o elimine aquí se agregarán a todas las interfaces de red o se eliminarán de ellas.

► Configuración de red avanzada

- En detalles avanzados pegamos lo siguiente en los datos de Usuario. (Yo he cogido Script para instalar Nginx):

```
#!/bin/bash
yum update -y
yum install -y nginx
systemctl start nginx
```

```
echo "<h1>¡Bienvenido a mi servidor Nginx!</h1>" > /usr/share/nginx/html/index.html
```

4. Probar que el servidor funciona, probar ACLs y conectividades

Por defecto al crear la red se ha creado una ACL asociada a nuestras dos subredes. Pero nota: una ACL puede reutilizarse para muchas subredes.

acl-027e2e4eb8ce8d670

Detalles

Reglas de entrada

Reglas de salida

Asociaciones de subredes

Etiquetas

Asociaciones de subredes (2)

Q

Filter subnet associations

Nombre	ID de subred	Asociada a	Zona de disponibilidad	CIDR IPv4
Manu_Practica4-subnet-private1...	subnet-0894d6ddfb670ce0f	acl-027e2e4eb8ce8d670	us-east-1a	10.10.128.0/20
Manu_Practica4-subnet-public1...	subnet-0238075e2fbc623db	acl-027e2e4eb8ce8d670	us-east-1a	10.10.0.0/20

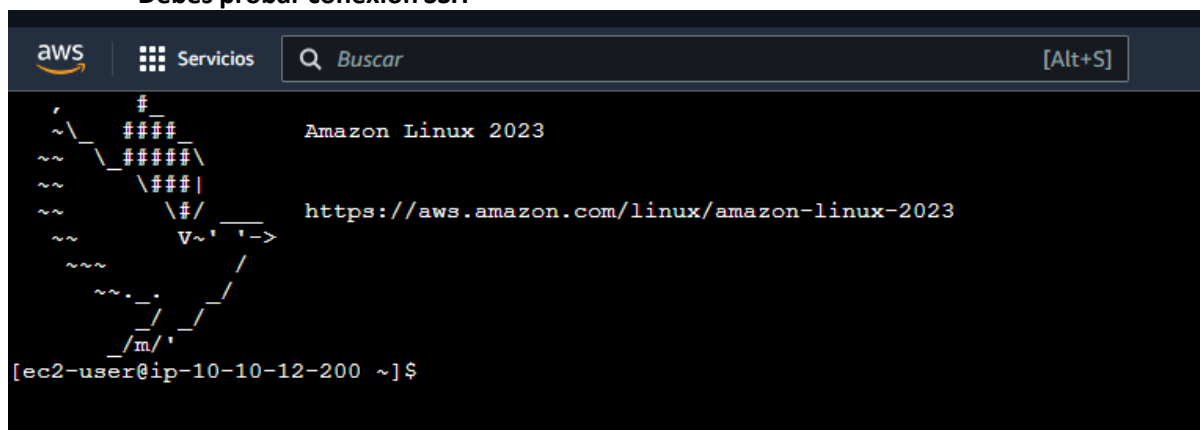
Ahora que hemos lanzado la instancia nos aplica:

- ACL de la red
- Grupo de seguridad que hemos elegido

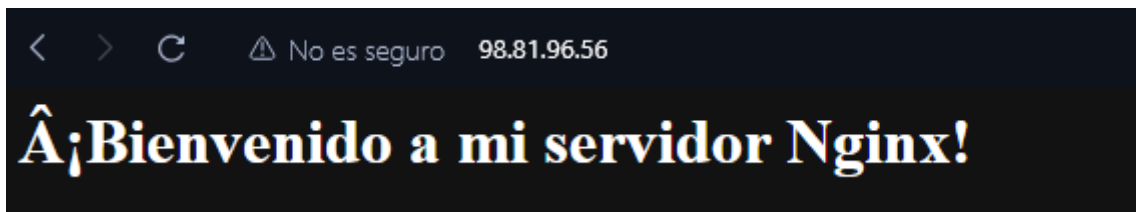
Probablemente tengas algún problema ... averigua cual es. Comprueba que la ACL y el web security group no entran en conflicto.

¿Qué problema ha sido y como lo has arreglado (si alguno). Se debía a que la ACL tiene permitido todos los tipos de conexiones, y la Web Security Group no.

Debes probar conexión SSH



También debes probar conexión HTTP



Consulta los metadatos de la instancia

Los metadatos de la instancia son datos sobre la instancia. Mientras esté conectado a la instancia los puedes ver así:

En un navegador: **[http:// 44.223.66.67/latest/meta-data/](http://44.223.66.67/latest/meta-data/)**

En una ventana de terminal: **`curl http://44.223.66.67/latest/meta-data/`**

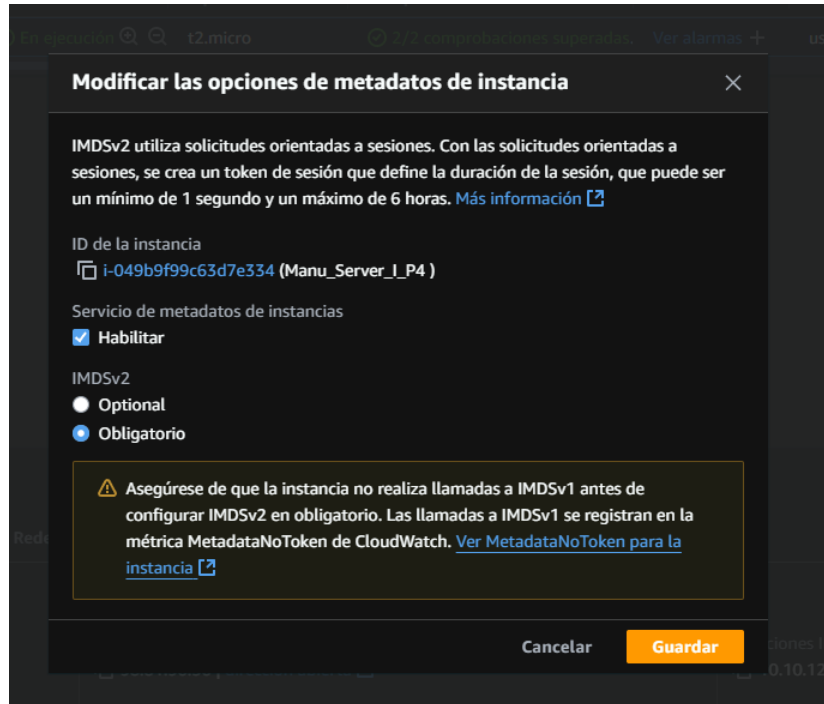
```
eee_w_3595259@runweb138769:~$
eee_w_3595259@runweb138769:~$ curl http://98.81.96.56/latest/meta-data/
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
  <head>
    <title>The page is not found</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <style type="text/css">
      /**/
      body {
        background-color: #fff;
        color: #000;
        font-size: 0.9em;
        font-family: sans-serif, helvetica;</pre>
</div>
<div data-bbox="398 641 587 775" data-label="Image">
<img alt="A close-up photo of a white cat's face."/>
  A close-up photograph of a white cat's face. The cat has dark eyes and a pink nose. It is looking directly at the camera. The background is dark and out of focus.
</div>
<div data-bbox="477 775 510 790" data-label="Text">
<p>Eh?</p>
</div>
<div data-bbox="484 923 500 939" data-label="Page-Footer">7</div>
```

Revisa las opciones metadatos de una instancia existente mediante la consola

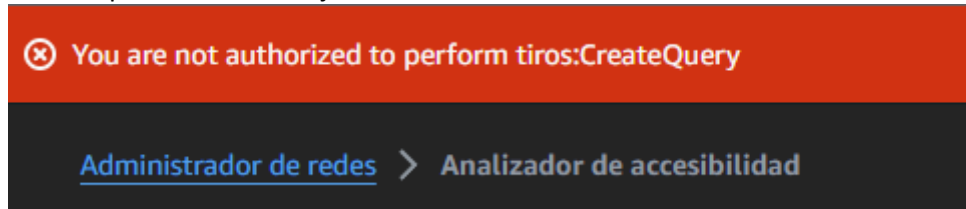
En la consola de Amazon EC2, selecciona la instancia-> Elija **Acciones, Configuración de la instancia y Modificar opciones de metadatos de instancia.**

Revise las opciones de metadatos de la instancia actuales en el cuadro de diálogo **Modificar las opciones de metadatos de la instancia.**



5. Intenta usar la herramienta Reachability analyzer para ver que todo está bien

Puedes crearla pero no te va a dejar...



6. Gateway NAT

Si lo que queremos es salida a internet pero no entrada... necesitamos un NAT Gateway. Así que lo creamos. Al crearlo nos pone las subredes disponibles a las que podemos asociarlo.

Muy importante: UN NAT Gateway debe asociarse siempre a una subred publica. Un NAT Gateway necesita salir a internet desde una subred publica, porque solo la subred publica está conectada a internet.

Lo asociamos a la subred publica. En conectividad ponemos publica y luego le asociamos una Elastic IP. Si no tenemos una, la generamos. Una Elastic IP es una IP que nos da AWS para conectarnos a internet, sin esto no tenemos conexión a internet.

Crear gateway NAT Información

Servicio administrado de traducción de direcciones de red (NAT) de alta disponibilidad que las instancias de subredes privadas pueden utilizar para conectarse a servicios de otras VPC, redes locales o Internet.

Configuración de gateway NAT

Nombre - *opcional*
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

El nombre puede tener un máximo de 256 caracteres.

Subred
Seleccione una subred en la que va a crear la gateway NAT.

Tipo de conectividad
Seleccione un tipo de conectividad para la gateway NAT.

☒ Pública
 ☐ Privada

ID de asignación de IP elástica Información
Asigne una dirección IP elástica a la gateway NAT.

► Configuraciones adicionales Información

Ya tenemos nuestro NAT Gateway disponible. Ahora tenemos que hacer que nuestra red privada acceda a internet, pero que desde internet no se pueda acceder a ella. Editamos la ruta de la tabla de enrutamiento privado. Tenemos que añadir la ruta para el caso de internet:

Todo lo que vaya a internet tiene que ir al NAT Gateway. Seleccionamos el NAT Gateway que acabamos de crear (Y que además se encuentra en la subred publica 1):

The screenshot shows the 'Editar rutas' (Edit routes) interface in the AWS Management Console. It is for a private subnet with ID 'pl-63a5400a'. The destination is '10.10.0.0/16'. The target is set to 'nat-077a63eb225924393' (NAT GW Practica 3). The interface includes a search bar for the destination, a dropdown for the target, and a button to 'Agregar ruta' (Add route).

Ahora, de la privada si es de la VPC permanece interno, y si es de internet, va al NAT Gateway que se encuentra en una subred publica. Desde internet no pueden ser accedidos. Prueba el servicio con la IP elástica. Para ello, sal del laboratorio y vuelve a entrar, verás que la IP es la misma.

7. Deshabilitar Gateway NAT

Ojo! Los NAT Gateway cuestan 0,048 por hora=1,15 dolares al dia ... unos 30 euros al mes. Asegurate de que no tienes ninguna IP elástica contratada y de que no hay ningún Gateway NAT