

# Actividad 7. AWS. Creación VPC

1. Creamos VPC. Indicando nombre y CIDR. Para ello usamos el buscador de servicios y buscamos VPC. Después pulsamos en el botón

The screenshot shows the AWS VPC creation interface and the resulting VPC details page.

**Create VPC Information:**

- Configuración de VPC:**
  - Recursos para crear:** Solo VPC (selected)
  - Etiqueta con nombre - opcional:** VPC\_IAMP
  - Bloque CIDR IPv4:** Entrada manual de CIDR IPv4 (selected)
  - CIDR IPv4:** 10.0.0.0/16
  - Bloque CIDR IPv6:** Sin bloque CIDR IPv6 (selected)

**VPC Details:**

You successfully created **vpc-06a1598f3b0cd3dfb / VPC\_IAMP**

Details	
<b>VPC ID</b>	vpc-06a1598f3b0cd3dfb
<b>DNS resolution</b>	Enabled
<b>Main network ACL</b>	acl-0f7458cec41a35f9b
<b>IPv6 CIDR (Network border group)</b>	-
<b>Encryption control ID</b>	-
<b>State</b>	Available
<b>Tenancy</b>	default
<b>Default VPC</b>	No
<b>Network Address Usage metrics</b>	Disabled
<b>Encryption control mode</b>	-
<b>Block Public Access</b>	Off
<b>DHCP option set</b>	dopt-06bf597af7c14544a
<b>IPv4 CIDR</b>	10.0.0.0/16
<b>Route 53 Resolver DNS Firewall rule groups</b>	-
<b>DNS hostnames</b>	Disabled
<b>Main route table</b>	rtb-0af26129809b65ab6
<b>IPv6 pool</b>	-
<b>Owner ID</b>	992382856097

2. Paso 2. Creación de subredes (pública y privada). En el menú lateral izquierdo seleccionamos la opción subredes y después Crear subred.

The screenshot shows the AWS VPC console with the following details:

- Panel de control de VPC:** Shows a list of options like 'Vista global de AWS', 'Filtrar por VPC', 'Nube privada virtual', 'Sus VPC', and 'Subredes'. 'Subredes' is highlighted with a red box.
- Vista de subredes:** Shows a table of subnets with columns: Name, Subnet ID, State, VPC, Block Public., and IPv4 CIDR. One row is selected: 'subnet-03d0cb44fb07ae5c1' (State: Available, VPC: 'vpc-06a1598f3b0cd3dfb', Block Public.: Off, IPv4 CIDR: 172.31.16.0/2).
- Create subnet:** A yellow box highlights the 'Create subnet' button at the top right of the subnet table.

### 3. Seleccionamos el VPC creado en el paso anterior.

Create subnet [Info](#)

The screenshot shows the 'Create subnet' wizard with the following steps:

- VPC:** A dropdown menu labeled 'Select a VPC' with a search bar. The result 'vpc-0ae59af5e69af299a' is listed with '(default)' next to it. Below it, 'vpc-06a1598f3b0cd3dfb (VPC\_IAMP)' is also listed and highlighted with a red box.
- Select a VPC first to create new subnets.** A note below the dropdown.
- Add new subnet:** A button at the bottom of the form.

### 4. Completamos nombre, zona de disponibilidad y el bloque CIDR, del VPC y de la subred. Subredes creadas:

The screenshot shows the AWS VPC Subnets creation interface. The top section is titled "Create subnet". It includes fields for "IPv4 VPC CIDR block" (set to 10.0.0.0/16), "Tags - optional" (with a key-value pair of "Name123456:subred1"), and a "Create subnet" button. Below this, a success message states "You have successfully created 1 subnet: subnet-0b7e50e78298c31f2". The main pane displays a table of existing subnets, including the newly created one.

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-03d0cb44fb07ae5c1	Available	vpc-0ae59af5e69af299a	Off	172.31.16.0/20
-	subnet-0dc1a8ea0c6be02a7	Available	vpc-0ae59af5e69af299a	Off	172.31.48.0/20
-	subnet-06cc0453f5b3e0243	Available	vpc-0ae59af5e69af299a	Off	172.31.0.0/20
-	subnet-0d9cbe0717c826a0f	Available	vpc-0ae59af5e69af299a	Off	172.31.64.0/20
-	subnet-0339268ac95efc5f	Available	vpc-0ae59af5e69af299a	Off	172.31.32.0/20
-	subnet-0edd069d2c7c810ba	Available	vpc-0ae59af5e69af299a	Off	172.31.80.0/20
-	subnet-0b7e50e78298c31f2	Available	vpc-06a1598f3b0cd3fdb   VPC...	Off	10.0.0.0/17

## 5. Editamos ambas subredes para habilitar la asignación automática de IP.

**Configuración de la asignación automática de IP** Información  
Permita que AWS asigne automáticamente una dirección IPv4 o IPv6 pública a una nueva interfaz de red principal para una instancia de esta subred.

Habilitar la asignación automática de la dirección IPv4 pública Información

Habilitar la asignación automática de direcciones IPv4 propiedad del cliente Información  
Opción desactivada porque no se encontraron grupos propiedad del cliente.

## 6. Paso 3. Creamos la puerta de enlace que posteriormente nos hará falta en la configuración de la tabla de enrutamiento:

igw-086d004d45eea8854 / gateway1

The screenshot shows the AWS Gateway Endpoints creation interface. It includes sections for "Detalles" (with ID "igw-086d004d45eea8854" and state "Detached") and "Etiquetas" (with a single tag "Name: gateway1"). A "Propietario" section shows the owner ID "992382856097".

## 7. Paso 4. Tablas de enrutamiento.

**Crear tabla de enrutamiento** Información

Una tabla de enrutamiento especifica cómo se envían los paquetes entre las subredes de la VPC, Internet y la conexión de la VPN.

**Configuración de la tabla de enrutamiento**

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

**VPC**  
La VPC que se debe usar para esta tabla de enrutamiento.

**Etiquetas**  
Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

Clave	Valor - opcional
<input type="text" value="Name"/>	<input type="text" value="tablaruta2"/> <span>X</span>

[Agregar nueva etiqueta](#)

Puede agregar 49 más etiquetas.

Cancelar Crear tabla de enrutamiento

Después de crear la tabla vamos a editar rutas:

**rtb-05f7b783cc21e024c / tablaruta2**

**Detalles** Información

ID de tabla de enrutamiento

Principal  
 No

ID de propietario

**Asociaciones de subredes explícitas**  
-

**Rutas** | Asociaciones de subredes | Asociaciones de borde | Propagación de rutas | Etiquetas

**Rutas (1)**

Destino	Destino	Estado	Propagada	Origen de la ruta
10.0.0.0/16	local	<span style="color: green;">Activo</span>	No	<a href="#">Crear tabla de enrutamiento</a>

Ambos Edit routes < 1 > | |

**Acciones**

- Configurar tabla de enrutamiento principal
- Editar asociaciones de subredes
- Editar asociaciones de borde
- Editar la propagación de rutas
- Edit routes
- Administrar etiquetas
- Eliminar

Seleccionamos la puerta de enlace creada anteriormente:

**Rutas para rtb-05f7b783cc21e024c / tablaruta2 actualizadas correctamente**

**rtb-05f7b783cc21e024c / tablaruta2**

**Detalles** Información

ID de tabla de enrutamiento <a href="#">rtb-05f7b783cc21e024c</a>	Principal <input checked="" type="checkbox"/> No	Asociaciones de subredes explícitas -	Asociaciones de borde -
VPC <a href="#">vpc-06a1598f3b0cd3dfb   VPC_IAMP</a>	ID de propietario <a href="#">992382856097</a>		

**Rutas** [Asociaciones de subredes](#) [Asociaciones de borde](#) [Propagación de rutas](#) [Etiquetas](#)

**Rutas (2)**

Filtrar rutas						
Destino	Destino	Estado	Propagada	Origen de la ruta		
0.0.0.0/0	<a href="#">igw-086d004d45eea8854</a>	<input checked="" type="checkbox"/> Activ	No	Crear ruta		
10.0.0.0/16	local	<input checked="" type="checkbox"/> Activ	No	Crear tabla de enrutamiento		

## 8. Antes de las comprobaciones nos queda asignar la tabla de enrutamiento a la subred pública, que es la que queremos que salga al exterior:

**rtb-05f7b783cc21e024c / tablaruta2**

**Detalles** Información

ID de tabla de enrutamiento <a href="#">rtb-05f7b783cc21e024c</a>	Principal <input checked="" type="checkbox"/> No	Asociaciones de subredes explícitas <a href="#">subnet-044bd3534734c997b / pública</a>	Asociaciones de borde -
VPC <a href="#">vpc-06a1598f3b0cd3dfb   VPC_IAMP</a>	ID de propietario <a href="#">992382856097</a>		

**Rutas** [Asociaciones de subredes](#) [Asociaciones de borde](#) [Propagación de rutas](#) [Etiquetas](#)

**Rutas (2)**

Filtrar rutas						
Destino	Destino	Estado	Propagada	Origen de la ruta		
0.0.0.0/0	<a href="#">igw-086d004d45eea8854</a>	<input checked="" type="checkbox"/> Activ	No	Crear ruta		
10.0.0.0/16	local	<input checked="" type="checkbox"/> Activ	No	Crear tabla de enrutamiento		

## 9. Paso 5. Comprobaciones.

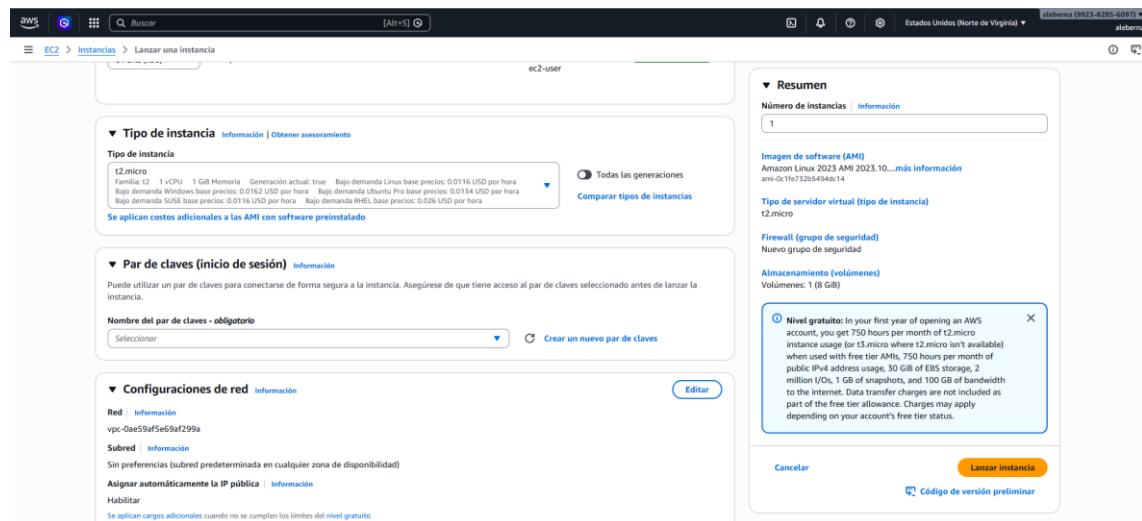
## 10. Para ello tendremos que crear una instancia. Usamos el buscador para acceder al menú de EC2. En el menú lateral pulsamos en instancias. Luego en Lanzar Instancia.

The screenshots show the AWS EC2 Instances page. In the left sidebar, 'Instancias' is selected. The main area displays resource statistics and a 'Lanzar la instancia' (Launch instance) button. The bottom screenshot shows the 'Lanzar instancias' (Launch instances) button highlighted with a red box.

## 11. Damos nombre y elegimos SSOO. Seleccionamos el tipo de instancia.

The screenshot shows the 'Lanzar una instancia' (Launch instance) wizard. The 'Nombre' (Name) field is filled with 'SSOO'. The 'Imagen de software (AMI)' section shows 'Amazon Linux 2023 AMI 2023.10... más información'. The 'Tipo de servidor virtual (tipo de instancia)' section shows 't3.micro'. A tooltip for 'Nivel gratuito' is visible on the right, stating: 'In your first year of opening an AWS account, you get 750 hours per month of t2.micro instances, 125 hours per month of t3.micro instances, and 125 hours per month of t3.1xlarge instances (when used with free tier AMIs). 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance. Charges may apply depending on your account's free tier status.'

**Importante editar la configuración de red para seleccionar nuestro VPC y la sub red en la que queremos que se cree la instancia. Dejamos la opción vockey para conectarnos por ssh. La instancia está corriendo y vemos cómo se le ha asignado una ip privada del rango**



**Tenemos que crear las claves manualmente. Es importante poner .ppk para utilizar después con PuTTY**

## Crear par de claves

### Nombre del par de claves

Con los pares de claves es posible conectarse a la instancia de forma segura.

vockey

El nombre puede incluir hasta 255 caracteres ASCII. No puede incluir espacios al principio ni al final.

### Tipo de par de claves



RSA

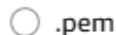
Par de claves pública y privada cifradas mediante RSA



ED25519

Par de claves privadas y públicas cifradas ED25519

### Formato de archivo de clave privada



.pem

Para usar con OpenSSH



.ppk

Para usar con PuTTY



Cuando se le solicite, almacene la clave privada en un lugar seguro y accesible del equipo. Lo necesitará más adelante para conectarse a la instancia. [Más información ↗](#)

[Cancelar](#)

[Crear par de claves](#)

**12. establecido y una pública a través de la que vamos a conectarnos.**

## Configuración de Red (Paso Crítico)

Baja hasta el apartado que dice **Configuraciones de red** y haz clic en el botón blanco **Editar** (a la derecha).

- **VPC:** En el desplegable, NO dejes la que viene por defecto. Busca y selecciona tu VPC\_IAMP.
- **Subred:** Selecciona la subred que creaste como publica\_vpc (debería tener el rango 10.0.1.0/24).
- **Asignar automáticamente la IP pública:** Asegúrate de que esté marcado como Habilitar. (Si no haces esto, no podrás conectarte desde Putty).



## Configurar el Firewall (Security Group)

Justo debajo, en Grupo de seguridad:

- **Selecciona Crear grupo de seguridad.**
- **Nombre del grupo:** Ponle permitir-ssh.
- **Regla de seguridad (SSH):** Asegúrate de que el tipo sea SSH, el puerto 22, y en Origen, selecciona Cualquier lugar (0.0.0.0/0).

Se aplicarán 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

Nombre del grupo de seguridad - **obligatorio**  
permitir-ssh

Este grupo de seguridad se agrega a todas las interfaces de red. El nombre no se puede editar después de crear el grupo de seguridad. La longitud máxima es de 255 caracteres. Caracteres válidos: a-z, A-Z, 0-9, espacios y \_-/.@#=;&!\$\*

**Descripción - obligatorio | Información**  
launch-wizard-2 created 2026-02-17T09:07:41.630Z

**Reglas de grupos de seguridad de entrada**

▼ Regla del grupo de seguridad 1 (TCP, 22, 0.0.0.0/0)    [Eliminar](#)

Tipo   Información	Protocolo   Información	Intervalo de puertos   Información
ssh	TCP	22
Tipo de origen   Información	Origen   Información	Descripción - opcional   Información
Cualquier lugar	<input type="text"/> Agregue CIDR, lista de prefijos o grupo de seg. 0.0.0.0/0	por ejemplo, SSH para Admin Desktop

⚠ Las reglas con origen 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia. Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas. [X](#)

[Agregar regla del grupo de seguridad](#)

► Configuración de red avanzada

## Lanzar y esperar

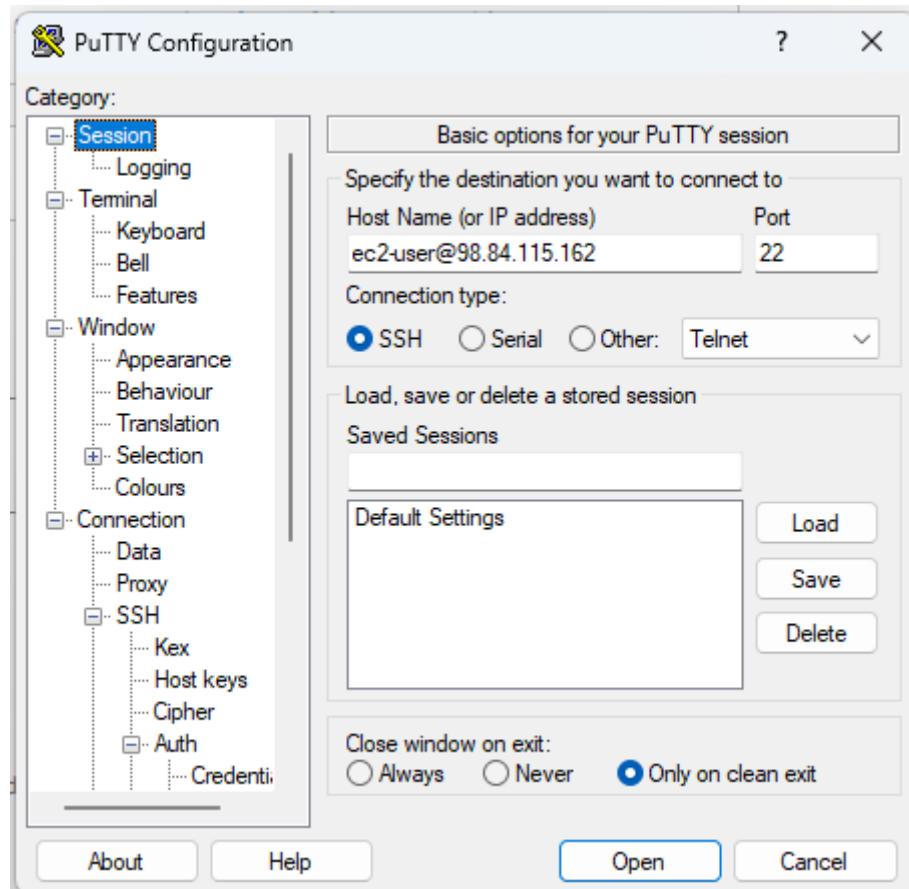
The screenshot shows the AWS EC2 console with the 'Launch instance' wizard open. The current step is 'Starting instance' (Inicio del lanzamiento), which is 80% complete. The progress bar is blue. Below the bar, it says 'Espere a que lancemos la instancia. No cierre el navegador mientras se realiza la carga.' (Wait for the instance to launch. Do not close the browser while the load is in progress.). At the bottom, there's a summary table with columns for 'Servidor de pr...', 'i-042847f7e2728c018', 'En ejecución', 't2.micro', 'us-east-1a', and '98.84.115.162'. The IP address 98.84.115.162 is highlighted in blue.

98.84.115.162

### 13. Desde Putty vamos a importar el archivo de clave privada que hemos descargado previamente:

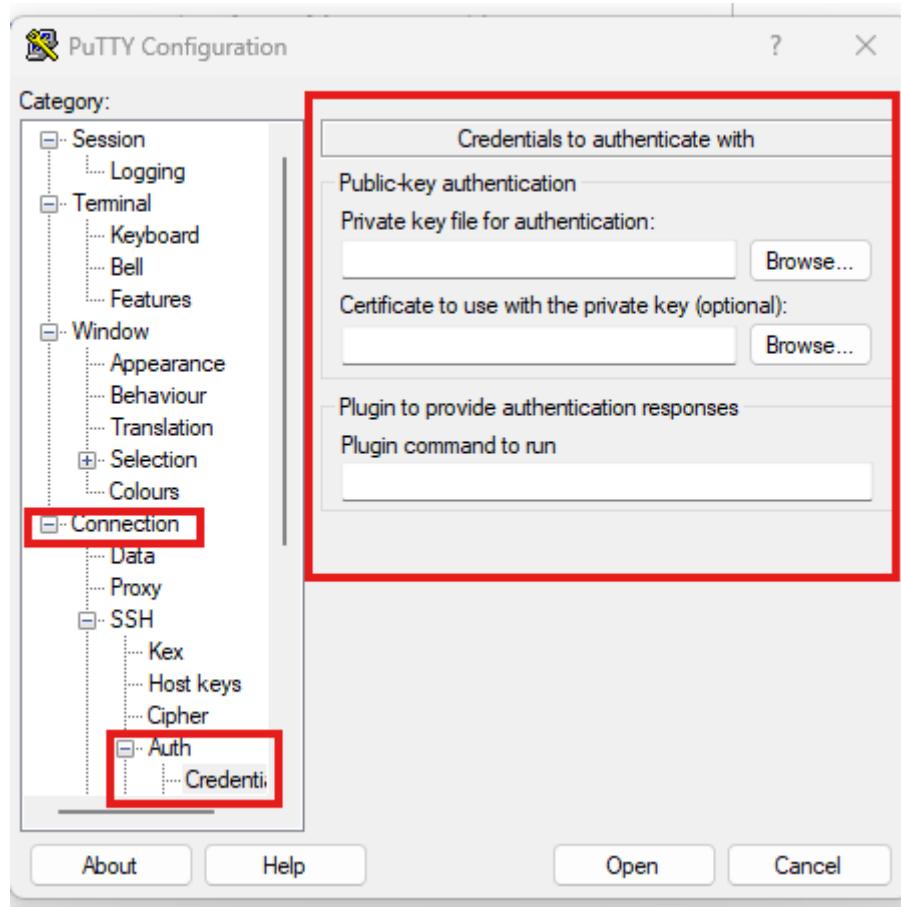
#### 1. Configurar la Sesión en PuTTY

1. Abre el programa PuTTY en tu ordenador.
2. En el campo Host Name (or IP address), escribe el usuario seguido de tu IP: ec2-user@TU\_IP\_PÚBLICA (por ejemplo: ec2-user@3.85.12.140).
3. Asegúrate de que el Port sea 22 y el Connection type sea SSH.



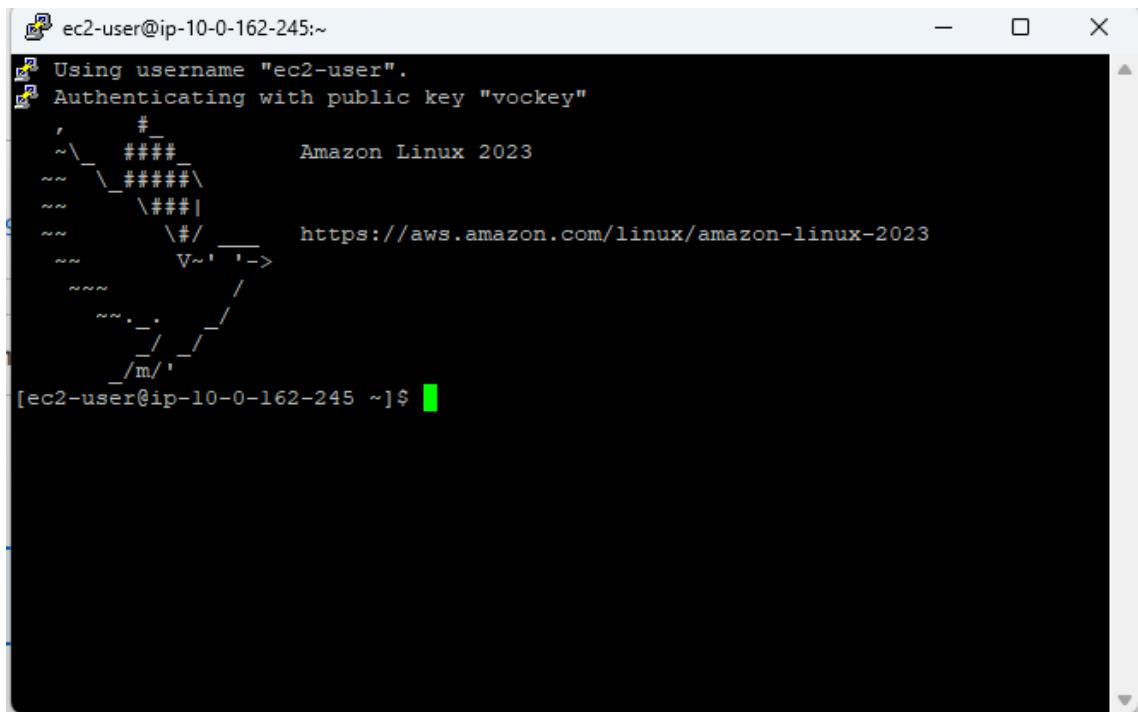
## 2. Cargar la Llave Privada (.ppk)

1. En el menú de la izquierda, busca la categoría Connection y despliégalas haciendo clic en el +.
2. Despliega SSH y luego Auth.
3. Haz clic en Credentials.
4. En el apartado "Private key file for authentication", pulsa el botón Browse....
5. Busca y selecciona el archivo vockey.ppk que descargaste antes.



### 3. Iniciar la Conexión

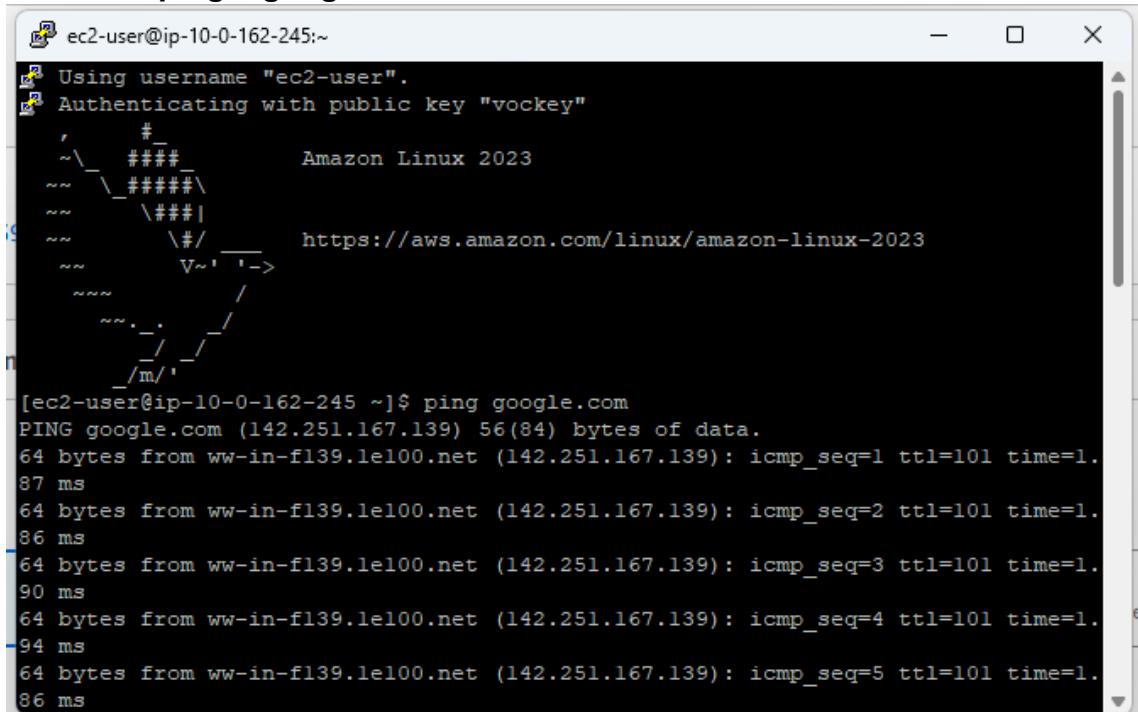
1. Vuelve a la categoría Session (arriba a la izquierda en el menú).
2. (Opcional) En "Saved Sessions", escribe Mi-VPC-AWS y dale a Save para no tener que repetir esto la próxima vez.
3. Haz clic en el botón Open abajo del todo.
4. Aviso de seguridad: Si te sale una ventana de "PuTTY Security Alert", haz clic en Accept o Yes.



```
ec2-user@ip-10-0-162-245:~  
Using username "ec2-user".  
Authenticating with public key "vockey"  
Amazon Linux 2023  
https://aws.amazon.com/linux/amazon-linux-2023  
[ec2-user@ip-10-0-162-245 ~]$
```

14. Nos conectamos con el usuario ec2-user (diferente para cada ssoo)

15. Hacemos ping a google:



```
ec2-user@ip-10-0-162-245:~  
Using username "ec2-user".  
Authenticating with public key "vockey"  
Amazon Linux 2023  
https://aws.amazon.com/linux/amazon-linux-2023  
[ec2-user@ip-10-0-162-245 ~]$ ping google.com  
PING google.com (142.251.167.139) 56(84) bytes of data.  
64 bytes from ww-in-f139.le100.net (142.251.167.139): icmp_seq=1 ttl=101 time=1.  
87 ms  
64 bytes from ww-in-f139.le100.net (142.251.167.139): icmp_seq=2 ttl=101 time=1.  
86 ms  
64 bytes from ww-in-f139.le100.net (142.251.167.139): icmp_seq=3 ttl=101 time=1.  
90 ms  
64 bytes from ww-in-f139.le100.net (142.251.167.139): icmp_seq=4 ttl=101 time=1.  
94 ms  
64 bytes from ww-in-f139.le100.net (142.251.167.139): icmp_seq=5 ttl=101 time=1.  
86 ms
```