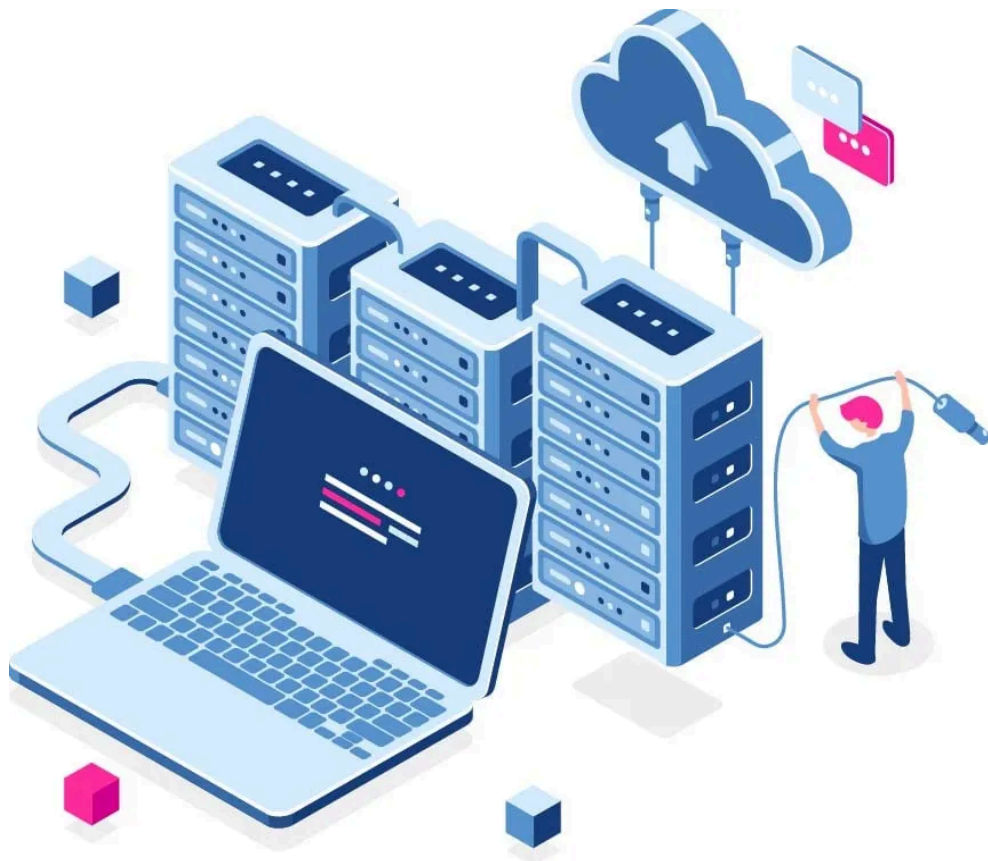


# Inicio de un Laboratorio en AWS



Marcos García Rodríguez  
25 de septiembre de 2025  
2º DAW

# ÍNDICE

Acceso al curso	2
Inicio del Laboratorio	2
Configuración del Laboratorio	3
Configuración de una instancia	3
Creación de las claves	5
Configuración de los Grupos de seguridad	7
Acceso al servidor mediante SSH	8

# Acceso al curso

Para comenzar, accedemos al curso proporcionado y entramos en él. Su nombre es el siguiente:

[AWS Academy Learner Lab \[139270\]](#)

AWS Academy Learner Lab [139270]

Una vez dentro, nos vamos al apartado de contenidos y buscamos la opción “Lanzamiento del Laboratorio para el alumnado de AWS Academy”

[Página de inicio](#)

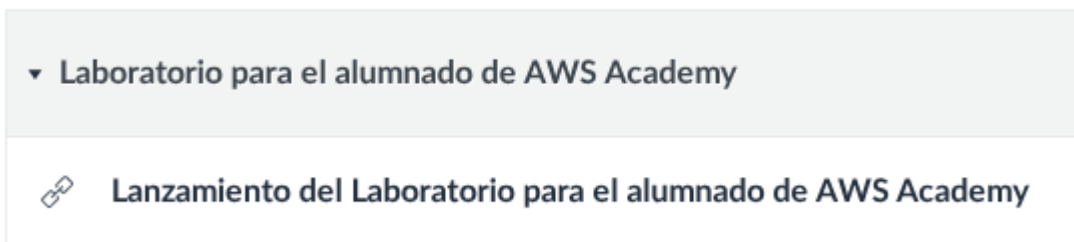
**Contenidos**

[Foros de discusión](#)

[Notas](#)

[Lucid \(pizarra\)](#)

Accedemos y esperamos que cargue.



## Inicio del Laboratorio

Una vez dentro, si nos fijamos en la parte superior veremos que tenemos el servidor apagado, para iniciarlo hacemos clic en “**Start Lab**”.

[AWS](#) ● ▶ Start Lab

Esperamos a que se inicie y mientras debería verse de la siguiente forma:

[AWS](#) ●

[AWS](#) ●

Hacemos clic sobre el icono de AWS para acceder a su configuración.

# Configuración del Laboratorio

Una vez estamos en la pantalla de configuración, hacemos clic en el menú superior izquierdo, y nos dirigimos a **“Todos los servicios”**.



**Página de inicio de la Consola** <

myApplications

Todos los servicios

Buscamos la categoría “Informática” y seleccionamos EC2, que sería lo más parecido a una máquina virtual.

## Servicios por categoría



**Informática**

EC2

Lanzamos la instancia y procedemos a su configuración.

## Lanzar la instancia

Para comenzar, lance una instancia de Amazon EC2, que es un servidor virtual en la nube.

Lanzar la instancia



Migrar un servidor

## Configuración de una instancia

### Nombre y etiquetas [Información](#)

Nombre

sshUbuntu2|

Seleccionamos ubuntu como S.O. y además comprobamos una versión apta para la capa gratuita. En este caso utilizaré la versión “**Ubuntu Server 24.04 LTS**”.

▼ **Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon)** [Información](#)

Una AMI posee el sistema operativo, el servidor de aplicaciones y las aplicaciones de la instancia. Si a continuación no ve una AMI adecuada, utilice el campo de búsqueda o elija [Buscar más AMI](#).

Q *Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones*

Recientes | **Inicio rápido**

		<b>Ubuntu</b> 				
--	--	-------------------	--	--	--	--

**Imágenes de máquina de Amazon (AMI)**

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type ami-0360c520857e3138f (64 bits (x86)) / ami-026fccd88446aa0bf (64 bits (Arm)) Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs	Apto para la capa gratuita
--	----------------------------

Volvemos a hacer lo mismo con el tipo de instancia, en este caso será la versión “**t3.micro**”.

▼ **Tipo de instancia** [Información](#) | [Obtener asesoramiento](#)

**Tipo de instancia**

<b>t3.micro</b> Familia: t3 2 vCPU 1 GiB Memoria Generación actual: true Bajo demanda Ubuntu Pro base precios: 0.0139 USD por hora Bajo demanda SUSE base precios: 0.0104 USD por hora Bajo demanda Linux base precios: 0.0104 USD por hora Bajo demanda RHEL base precios: 0.0392 USD por hora Bajo demanda Windows base precios: 0.0196 USD por hora	Apto para la capa gratuita
--	----------------------------

**Se aplican costos adicionales a las AMI con software preinstalado**

Hacemos clic en “**Crear un nuevo par de claves**” para crear las claves de acceso al servidor.

▼ **Par de claves (inicio de sesión)** [Información](#)

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

**Nombre del par de claves - obligatorio**

Continuar sin un par de claves (no recomendado) Valor predeterminado ▼ [Crear un nuevo par de claves](#)

## Creación de las claves

Indicamos el nombre con el que identificaremos posteriormente las claves, el tipo de clave será **"RSA"** y el formato de archivo será el `.pem`. También podríamos utilizar el `.ppk` pero tendríamos que utilizar un servicio PuTTY, en lugar del SSH que vamos a utilizar.

### Crear par de claves



#### Nombre del par de claves

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

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

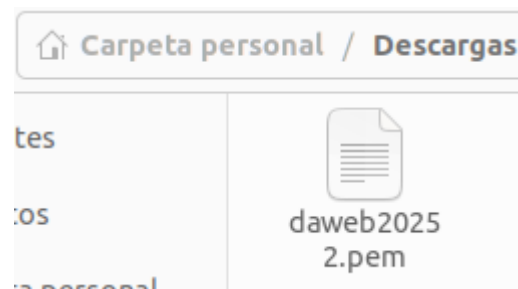
**.ppk**  
Para usar con PuTTY

 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

Localizamos la ruta donde se han guardado las claves, ya que nos hará falta posteriormente.



En la configuración de red, procedemos a crear un grupo de seguridad, ya que aún no tenemos ninguno.

También permitiremos el tráfico SSH, ya que de primeras será más cómodo para la configuración inicial del servidor.

▼ **Configuraciones de red** [Información](#) Editar

**Red** | [Información](#)  
vpc-0dc498a2e88a67e44

**Subred** | [Información](#)  
Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

**Asignar automáticamente la IP pública** | [Información](#)  
Habilitar

**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

Crearemos un nuevo grupo de seguridad denominado **"launch-wizard-2"** con las siguientes reglas:

- Permitir el tráfico de SSH desde Cualquier lugar  
0.0.0.0/0  
Ayuda a establecer conexión con la instancia
- Permitir el tráfico de HTTPS desde Internet  
Para configurar un punto de enlace, por ejemplo, al crear un servidor web
- Permitir el tráfico de HTTP desde Internet  
Para configurar un punto de enlace, por ejemplo, al crear un servidor web

⚠ 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. ✕

Hacemos clic en **"Lanzar instancia"** y esperamos a que se inicie.

▼ **Resumen**

**Número de instancias** | [Información](#)

---

**Imagen de software (AMI)**  
Canonical, Ubuntu, 24.04, amd6...[más información](#)  
ami-0360c520857e3138f


**Tipo de servidor virtual (tipo de instancia)**  
t3.micro

**Firewall (grupo de seguridad)**  
Nuevo grupo de seguridad

**Almacenamiento (volúmenes)**  
Volúmenes: 1 (8 GiB)

---

[Cancelar](#) Lanzar instancia

 [Código de versión preliminar](#)

✔ **Correcto**  
El lanzamiento de la instancia se inició correctamente ([i-09676b774317d3c4f](#))

Si volvemos a la pantalla anterior de instancias, podremos ver las que hemos creado. La del ejemplo es la “sshUbuntu2” que como vemos está en ejecución e inicializando algunos parámetros aún. Esperaremos a que se ejecute por completo.

Instancias (3) [Información](#) Última actualización Hace 3 minutos

Buscar instancia por atributo o etiqueta (case-sensitive) Todos los ... ▾

<input type="checkbox"/>	Name <a href="#">↗</a> ▾	ID de la instancia	Estado de la i... ▾	Tipo de inst... ▾	Comprobación de	Estado de la al:	Zona de dispon... ▾
<input type="checkbox"/>	sshUbuntu	i-0e61440ba9050368d	<span style="color: green;">✔</span> En ejecución <a href="#">🔗</a> <a href="#">🔍</a>	t3.micro	<span style="color: green;">✔</span> 3/3 comprobaci	<a href="#">Ver alarmas +</a>	us-east-1d
<input type="checkbox"/>	sshUbuntu2	i-01d8ba42b60a6af94	<span style="color: green;">✔</span> En ejecución <a href="#">🔗</a> <a href="#">🔍</a>	t3.micro	<span style="color: gray;">⌚</span> Inicializando	<a href="#">Ver alarmas +</a>	us-east-1d

## Configuración de los Grupos de seguridad

En caso de querer cambiar el puerto de escucha de SSH, podremos acceder a los “Grupos de seguridad” y aquí cambiar el servicio y/o puerto. En mi caso lo dejaré por defecto.

Detalles Estado y alarmas Monitoreo **Seguridad** Redes Almacenamiento Etiquetas

▼ Detalles de seguridad

Rol de IAM: - ID del propietario: 975049884934 Hora de lanzamiento: Thu Sep 25 2025 13:00:11 GMT+0200 (hora de verano de Europa central)

Grupos de seguridad: sg-056abfe8bec295796 (launch-wizard-3)

▼ Reglas de entrada

Buscar reglas < 1 >

Nombre	ID de la regla del grupo ...	Intervalo de p...	Protocolo	Origen	Grupos de seguridad	Descripción
-	sgr-001fdd081ce3d1a21	22	TCP	0.0.0.0/0	launch-wizard-3 <a href="#">🔗</a>	-

Reglas de entrada (1) [Administrar etiquetas](#) [Editar reglas de entrada](#)

Buscar < 1 > ⚙️

<input type="checkbox"/>	Name ▾	ID de la regla del gr... ▾	Versión de IP ▾	Tipo ▾	Protocolo ▾	Intervalo de puertos ▾	Origen ▾	Descripción
<input type="checkbox"/>	-	sgr-001fdd081ce3d1a21	IPv4	SSH	TCP	22	0.0.0.0/0	-

Reglas de entrada [Información](#)

ID de la regla del grupo de seguridad: sgr-001fdd081ce3d1a21

Tipo: [Información](#) SSH

Protocolo: [Información](#) TCP

Intervalo de puertos: [Información](#) 22

Origen: [Información](#) Persona...  [Eliminar](#)

[Agregar regla](#)

Volvemos a la página de las instancias y hacemos clic sobre el ID de la nuestra. Posteriormente, nos conectamos a la instancia.

[Conectar](#) [Estado de la instancia ▾](#) [Acciones ▾](#)



# Acceso al servidor mediante SSH

Ahora, iremos a “**Ciente SSH**”, donde nos aparecerán los pasos a seguir para poder acceder al servidor.


Conexión de la instancia EC2 | Administrador de sesiones | **Ciente SSH** | Consola de serie de EC2

## ID de la instancia

 [i-01d8ba42b60a6af94](#) (sshUbuntu2)

1. Abra un cliente SSH.
2. Localice el archivo de clave privada. La clave utilizada para lanzar esta instancia es `daweb20252.pem`
3. Ejecute este comando, si es necesario, para garantizar que la clave no se pueda ver públicamente.  
 `chmod 400 "daweb20252.pem"`
4. Conéctese a la instancia mediante su DNS público:  
 `ec2-3-90-86-192.compute-1.amazonaws.com`

Ejemplo:

 `ssh -i "daweb20252.pem" ubuntu@ec2-3-90-86-192.compute-1.amazonaws.com`

Ahora, desde el terminal del equipo anfitrión, entramos en la ruta donde guardamos antes las claves y comenzamos a ejecutar los comandos.

En mi caso, en lugar de entrar con el nombre DNS, accederé con la clave pública

```
alumnado@iespsur:~/Descargas$ chmod 400 daweb2025.pem
alumnado@iespsur:~/Descargas$ ssh -i "daweb2025.pem" ubuntu@18.215.146.19
The authenticity of host '18.215.146.19 (18.215.146.19)' can't be established.
ED25519 key fingerprint is SHA256:CznGieKjLmX8bUQwCRcpOL8ilG13IRePl01fCB9MqzE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Finalmente, ejecutamos el comando “**sudo service ssh status**” para comprobar que el servicio funciona correctamente y está activo.

Importante que no entremos como sudo, sino que ejecutemos los comandos como este únicamente cuando sea estrictamente necesario, para evitar posibles grandes problemas.

```
ubuntu@ip-172-31-27-174:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Drop-In: /usr/lib/systemd/system/ssh.service.d
            └─ec2-instance-connect.conf
   Active: active (running) since Thu 2025-09-25 10:08:09 UTC; 11min ago
   TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
         man:sshd_config(5)
   Process: 1078 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1080 (sshd)
     Tasks: 1 (limit: 1008)
    Memory: 4.2M (peak: 6.9M)
       CPU: 95ms
```