

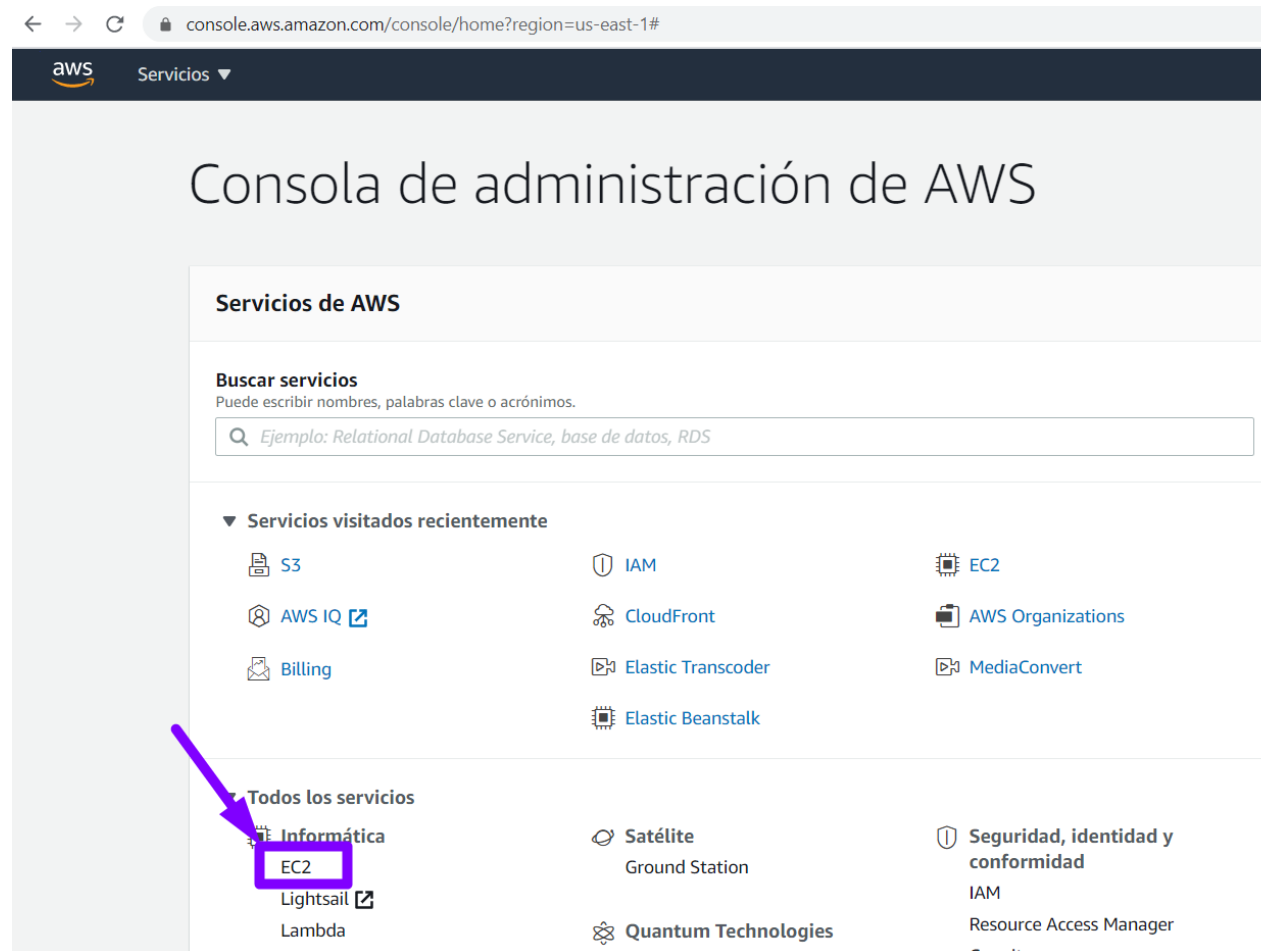
# Lanzar instancia en EC2

---

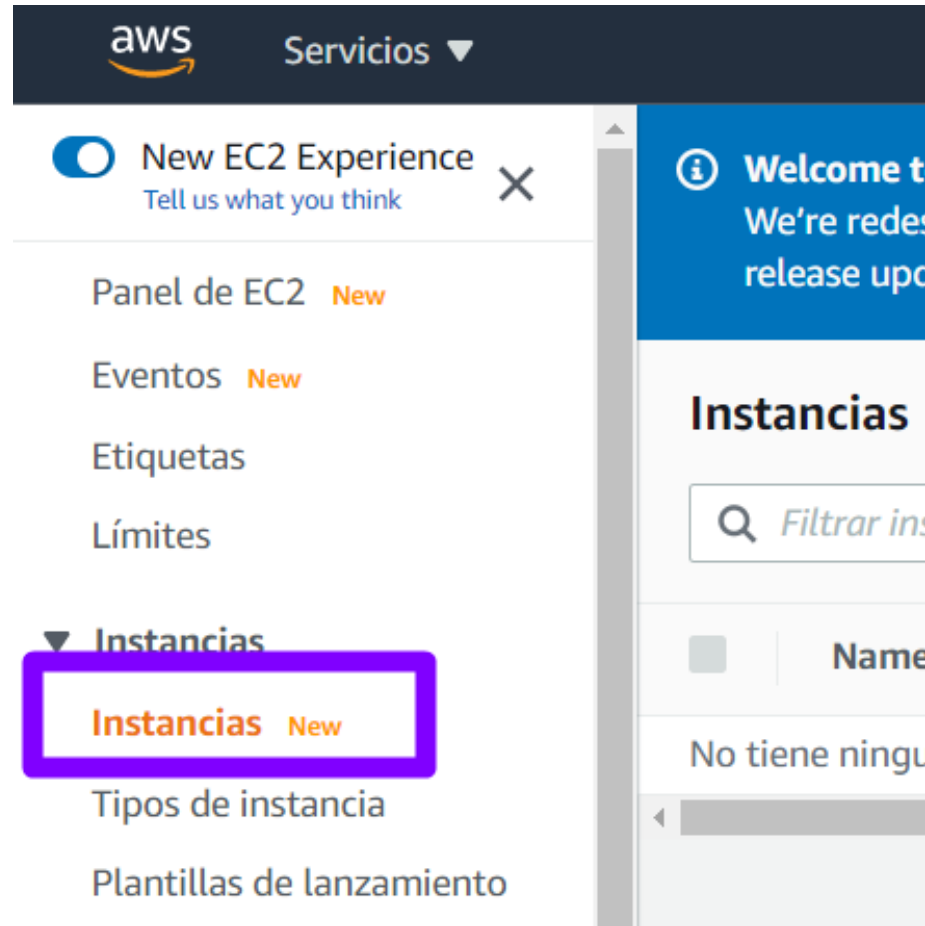


Ingresa a tu cuenta de AWS

Después ingresa a la Consola de Administración de Amazon y selecciona la opción de servicios y busca la opción EC2:

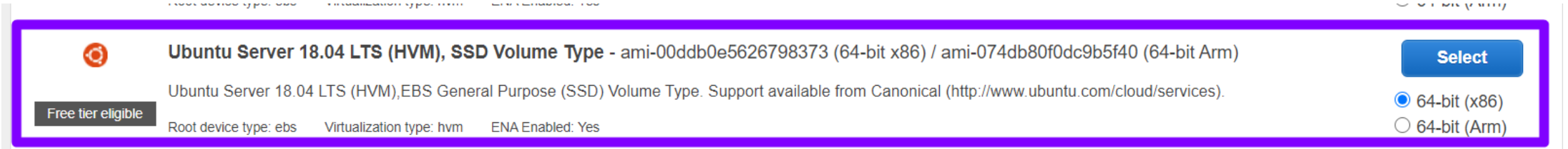


Dentro de la consola de EC2, ingresa al apartado de instancias:



Después ingresa a la opción de **Lanzar instancias**

En nuestro caso vamos a seleccionar la instancia **Ubuntu Server 18.04 LTS (HVM)**



The screenshot shows the AWS console interface for selecting an Amazon Machine Image (AMI). The selected AMI is **Ubuntu Server 18.04 LTS (HVM), SSD Volume Type** with IDs `ami-00ddb0e5626798373` (64-bit x86) and `ami-074db80f0dc9b5f40` (64-bit Arm). A blue **Select** button is visible. Below the title, it states: "Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).". A "Free tier eligible" badge is on the left. At the bottom, it lists "Root device type: ebs", "Virtualization type: hvm", and "ENA Enabled: Yes". On the right, there are radio buttons for "64-bit (x86)" (selected) and "64-bit (Arm)".

Ahora vamos a elegir el tipo de instancia, para los propósitos de este curso la instancia `t2.micro` es suficiente, sin embargo para aplicaciones de producción, considera emplear una instancia `t2.medium` para arriba dependiendo de las necesidades de la aplicación.



Después da clic en el botón de **Next: Configure instance details**. En este apartado dejaremos todo como está por defecto.

Damos **Next: Add Storage**. En este apartado vamos a colocar 30 GB los cuales están incluidos dentro de la capa gratuita.

Storage options for instance type

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/sda1	snap-0b071e09e1285af85	30	General Purpose SSD (gp2) ▼	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted ▼
Add New Volume								

Después damos clic en Next: Add Tags. En este apartado no es necesario añadir nada

A continuación damos clic en Next: Configure Security Group. En este apartado vamos a definir las reglas o protocolos para poder conectarse.



Lo primero que vamos a hacer es modificar la conexión SSH para que solo acepte conexiones desde mi IP

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH ▾	TCP	22	My IP ▾ 187.190.157.13/32	e.g. SSH for Admin Desktop ✕

Add Rule

Y vamos a añadir dos protocolos de conexión HTTP y HTTPS  
Así nos deben de quedar:

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH ▾	TCP	22	My IP ▾ 187.190.157.13/32	e.g. SSH for Admin Desktop ✕
HTTP ▾	TCP	80	Anywhere ▾ 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop ✕
HTTPS ▾	TCP	443	Anywhere ▾ 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop ✕

Add Rule



Finalmente vamos a dar clic en **Review and Launch** y después le vas a dar clic en **Launch**  
Ahora debemos crear nuestro KeyPair

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair

Key pair name

awsdemo

Download Key Pair

You have to download the **private key file** (\*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

Es muy importante que guardes tu archivo .pem en un lugar seguro y accesible ya que no lo podrás descargar nuevamente.

Después damos clic en **Launch Instances**

Esperamos un poco en lo que AWS lanza nuestra instancia.