

LABORATORIO 8

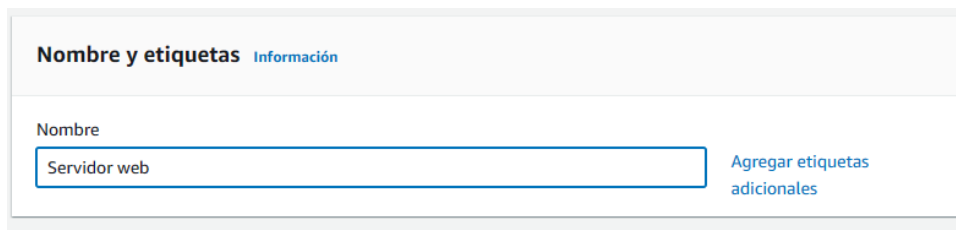
Para realizar esta práctica:

3.1 Lanzar y manejar una instancia EC2 de AWS

1. Lanzar la instancia de Amazon EC2.

Para poder lanzar una instancia de Amazon EC2, con protección de terminación y desplegar la instancia con un script de datos de usuario permitiendo así poder desplegar un servidor web sencillo, los pasos realizados son:

- Asignar a la instancia el nombre de “Servidor web” como se puede observar en la **imagen 1**.



Nombre y etiquetas Información

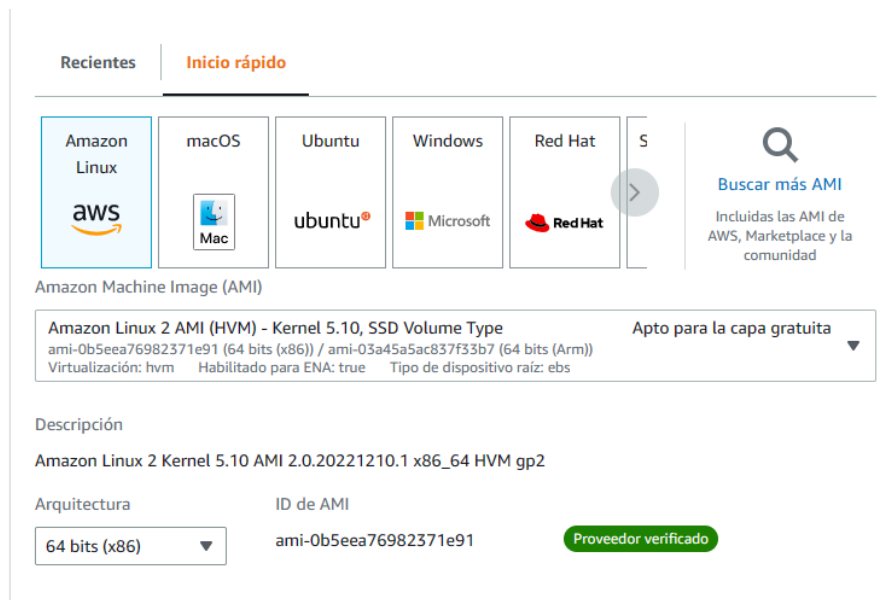
Nombre

Servidor web

Agregar etiquetas adicionales

Imagen 1: Asignación de nombre a la instancia

- Selección de la AMI de Amazon Linux, y después se la AMI predeterminada de Amazon Linux 2 (HVM), como se observa en la **imagen 2**.



Recientes Inicio rápido

Amazon Linux macOS Ubuntu Windows Red Hat S

Buscar más AMI

Incluidas las AMI de AWS, Marketplace y la comunidad

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type Apto para la capa gratuita

ami-0b5eea76982371e91 (64 bits (x86)) / ami-03a45a5ac837f33b7 (64 bits (Arm))

Virtualización: hvm Habilitado para ENA: true Tipo de dispositivo raíz: ebs

Descripción

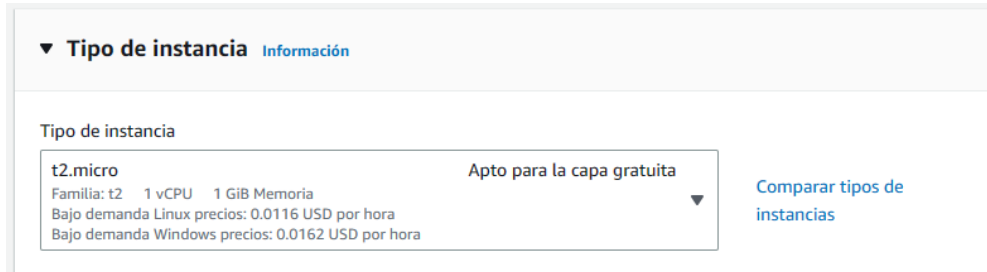
Amazon Linux 2 Kernel 5.10 AMI 2.0.20221210.1 x86_64 HVM gp2

Arquitectura ID de AMI

64 bits (x86) ami-0b5eea76982371e91 Proveedor verificado

Imagen 2: Selección de la AMI de Amazon Linux

- c) Selección del tipo de instancia (**imagen 3**), manteniendo el tipo predeterminado que es el t2.micro. Este tiene 1 CPU virtual y 1 GiB de memoria.



▼ **Tipo de instancia** [Información](#)

Tipo de instancia

t2.micro Apto para la capa gratuita

Familia: t2 1 vCPU 1 GiB Memoria

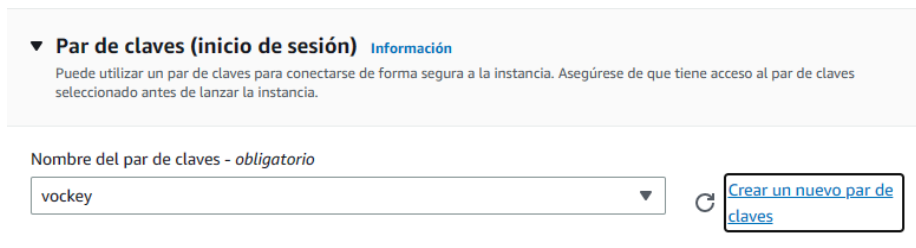
Bajo demanda Linux precios: 0.0116 USD por hora

Bajo demanda Windows precios: 0.0162 USD por hora

[Comparar tipos de instancias](#)

Imagen 3: Selección del tipo de instancia

- d) Establecer el par de claves para poder conectarte a la instancia creada, como se puede observar en la **imagen 4 y 5**.



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

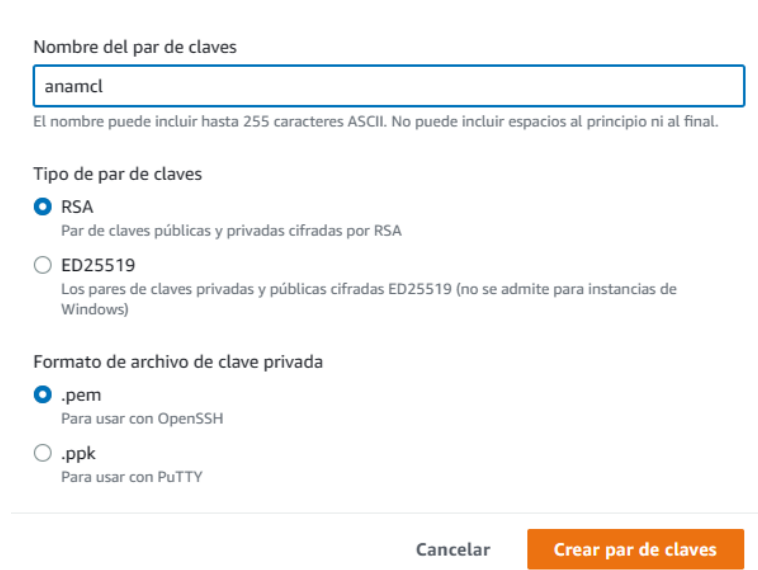
Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - *obligatorio*

vockey

[Crear un nuevo par de claves](#)

Imagen 4: Selección de vockey



Nombre del par de claves

anamcl

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 públicas y privadas cifradas por RSA

☐ ED25519
Los pares de claves privadas y públicas cifradas ED25519 (no se admite para instancias de Windows)

Formato de archivo de clave privada

☒ .pem
Para usar con OpenSSH

☐ .ppk
Para usar con PuTTY

[Cancelar](#) [Crear par de claves](#)

Imagen 5: Introducción del nombre del par de claves

- e) Para la configuración de red, primero se ha seguido el paso mostrado en la **imagen 6**. A continuación, se procede a seleccionar la casilla de “Crear grupo de seguridad” (**imagen 7**). Después, se establece un nombre para la casilla marcada en rojo en la **imagen 7**. Además, se introduce una descripción en la casilla marcada en verde en la **imagen 7**. Por último, se procede a eliminar la regla del grupo de seguridad seleccionando la casilla eliminar, marcada en azul en la **imagen 7**.

▼ **Configuraciones de red** Información

VPC - obligatorio Información

vpc-00c71aaa3022c91ec (Lab VPC) 10.0.0.0/16

Subred Información

Imagen 6: Selección de Lab VPC para VPC.

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

Grupo de seguridad del servidor web

Este grupo de seguridad se agregará 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

Grupo de seguridad para mi servidor web

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 - optional Información

Cualquier lugar Q Agregue CIDR, lista de prefijos por ejemplo, SSH para Admin Desk

Imagen 7: Parte Firewall de la configuración de la red.

- f) Para poder configurar el almacenamiento, se dejará la configuración predeterminada (volumen de disco predeterminado de 8 GiB, que será el volumen raíz), como se observa en la **imagen 8**.

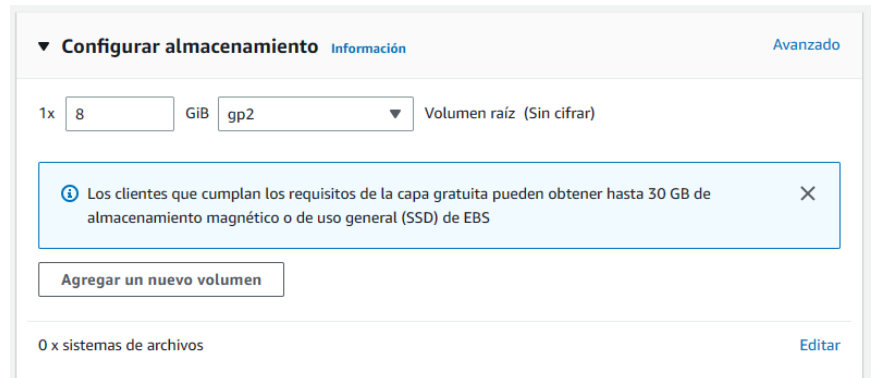


Imagen 8: Configuración de almacenamiento.

- g) En la parte de detalles avanzados, seleccionaremos la parte de “Habilitar” en la Protección de terminación (**imagen 9**).



Imagen 9: Detalles avanzados

- h) En la parte inferior de la página, se introduce el código que se observa en la **imagen 10**. Con este código, se meten los datos de usuario para que cuando se lance la instancia se usen para realizar tareas de instalación y configuración de una manera automática una vez iniciada esta.

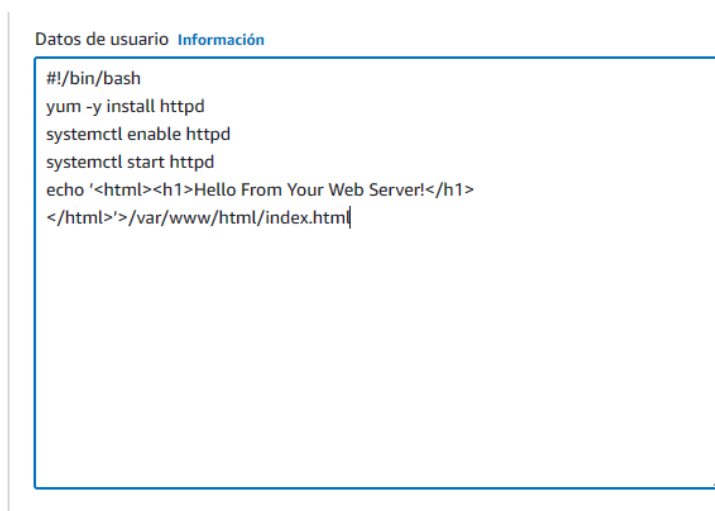


Imagen 10: Datos de usuario

- i) Para lanzar la instancia, se selecciona “Iniciar instancia” y aparece el mensaje de éxito que se observa en la **imagen 11**.

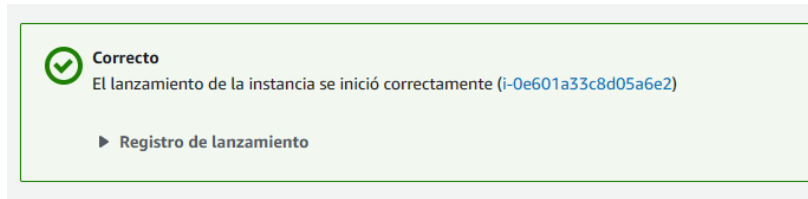


Imagen 11: Mensaje de éxito.

- j) Al lanzar la instancia, primero aparecerá estado “Pendiente”. Después, aparecerá el estado “Inicializando”, como se observar en la **imagen 12** marcado en rojo. Por último, una vez completado el proceso, aparecerá el estado “2/2 comprobaciones aprobadas” (marcado en rojo en la **imagen 13**), indicándonos esto que hemos lanzado la instancia con éxito.



Imagen 12: Muestra el estado de la instancia.



Imagen 13: Muestra el estado de la instancia.

2. Supervisa la instancia.

- a) Observar la salida de la consola de la instancia en el registro del sistema y comprobar que el paquete HTTP se ha instalado, a partir de los datos de usuario que se han introducido en los pasos previos. Este paso se observa en la **imagen 14**. En el repositorio de GitHub se ha subido la salida de la consola completa.

```
[ 22.599718] cloud-init[3240]: --> Running transaction check
[ 22.603984] cloud-init[3240]: --> Package httpd.x86_64 0:2.4.54-1.amzn2 will be installed
[ 22.653256] cloud-init[3240]: --> Processing Dependency: httpd-tools = 2.4.54-1.amzn2 for package: httpd-2.4.54-1.amzn2.x86_64
[ 22.922357] cloud-init[3240]: --> Processing Dependency: httpd filesystem = 2.4.54-1.amzn2 for package: httpd-2.4.54-1.amzn2.x86_64
[ 22.937037] cloud-init[3240]: --> Processing Dependency: system-logos-httpd for package: httpd-2.4.54-1.amzn2.x86_64
[ 22.949130] cloud-init[3240]: --> Processing Dependency: mod_http2 for package: httpd-2.4.54-1.amzn2.x86_64
[ 22.978615] cloud-init[3240]: --> Processing Dependency: httpd filesystem for package: httpd-2.4.54-1.amzn2.x86_64
[ 22.995285] cloud-init[3240]: --> Processing Dependency: /etc/mime.types for package: httpd-2.4.54-1.amzn2.x86_64
[ 23.001459] cloud-init[3240]: --> Processing Dependency: libaprutil-1.so.0()(64bit) for package: httpd-2.4.54-1.amzn2.x86_64
[ 23.018610] cloud-init[3240]: --> Processing Dependency: libapr-1.so.0()(64bit) for package: httpd-2.4.54-1.amzn2.x86_64
[ 23.038619] cloud-init[3240]: --> Running transaction check
[ 23.058635] cloud-init[3240]: --> Package apr.x86_64 0:1.7.0-9.amzn2 will be installed
[ 23.062640] cloud-init[3240]: --> Package apr-util.x86_64 0:1.6.1-5.amzn2.0.2 will be installed
[ 23.074640] cloud-init[3240]: --> Processing Dependency: apr-util-bdb(x86-64) = 1.6.1-5.amzn2.0.2 for package: apr-util-1.6.1-5.amzn2.0.2.x86_64
[ 23.098348] cloud-init[3240]: --> Package generic-logos-httpd.noarch 0:18.0.0-4.amzn2 will be installed
```

Imagen 14: Salida de la consola de la instancia.

- b) En la **imagen 15** se observa la captura de pantalla de la instancia, para poder observar cómo se vería la consola de la instancia de Amazon EC2 si se le añadiera una pantalla.

```
Amazon Linux 2
Kernel 5.10.157-139.675.amzn2.x86_64 on an x86_64

ip-10-0-1-23 login: [ 27.507354] xfs filesystem being remounted at /tmp support
ts timestamps until 2038 (0x7fffffff)
[ 27.546993] xfs filesystem being remounted at /var/tmp supports timestamps un
til 2038 (0x7fffffff)
```

Imagen 15: Consola de la instancia de Amazon EC2.

3.2 Usando más a fondo AWS

1. Actualiza tu grupo de seguridad y accede al servidor web.

En la **imagen 16**, se observa la pestaña “Detalles” donde, marcado en rojo, está la dirección IPv4 pública de la instancia que hay que copiar en una pagina nueva del navegador web y comprobar que efectivamente, como se observa en la **imagen 17**, no te deja acceder al servidor web que se había instalado cuando se creo la instancia EC2 en los pasos previos.



Imagen 16: Pestaña Detalles.

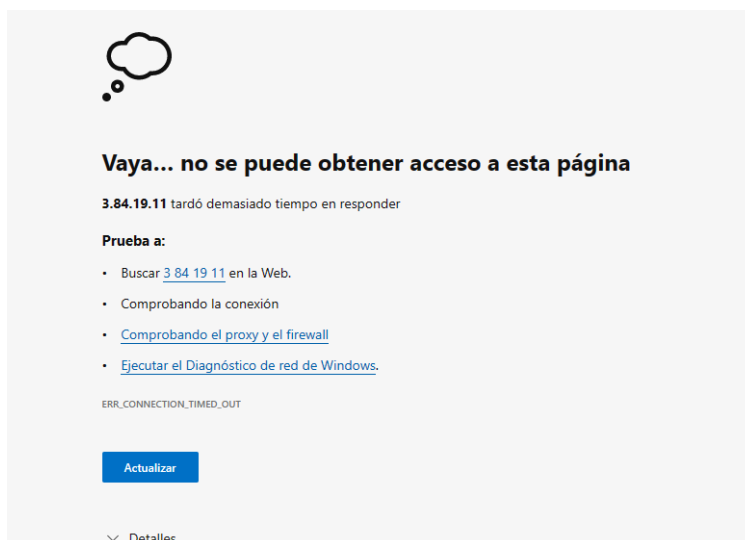


Imagen 17: Mensaje de error al intentar acceder al servidor web.

Para poder acceder a dicho servidor, se modificará las reglas de entrada, tal y como se observa en la **imagen 18**, marcadas en color rojo.

Imagen 18: Pestaña editar reglas de entrada del grupo de seguridad del servidor web.

Al guardar los cambios y actualizar la página del navegador, que se había abierto anteriormente, se observa que ya te deja acceder al servidor web (**imagen 19**). Marcado en verde, se observa que en el mensaje de la página pone que tiene un funcionamiento correcto.

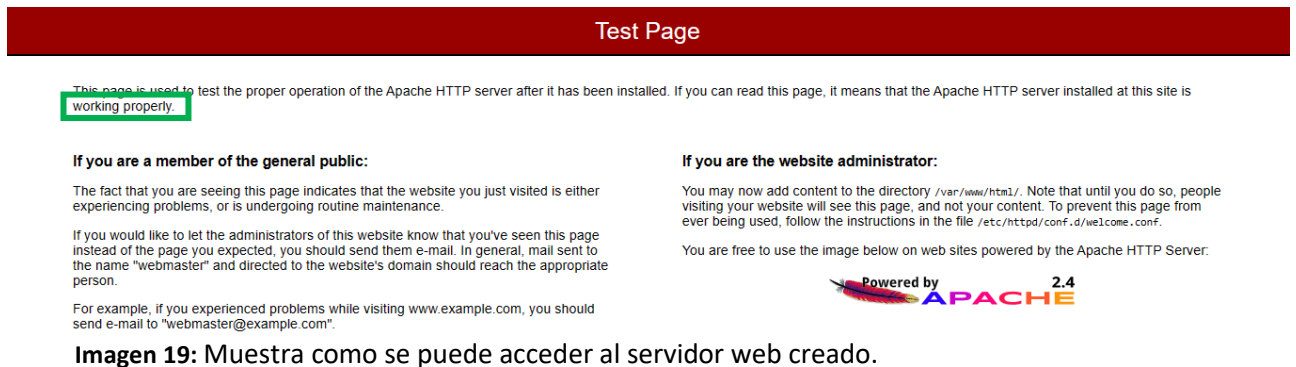


Imagen 19: Muestra como se puede acceder al servidor web creado.

2. Cambia el tamaño de su instancia.

Para cambiar el tipo de instancia, se detendrá primero esta y después en la “Configuración de instancia”, se selecciona la pestaña “Cambiar tipo de instancia” y en esta cambiaremos el tipo a t2.small, marcado en rojo en la **imagen 20**.

Imagen 20: Pestaña Cambiar tipo de instancia.

Para cambiar el tamaño del volumen de EBS en la pestaña “Almacenamiento”, se selecciona el nombre de la ID del volumen y después la casilla de verificación junto al volumen. A continuación, en “Acciones” se selecciona “Modificar Volumen” y se cambia el tamaño de esta tal y como se observa en la **imagen 21**.

Detalles del volumen

ID de volumen
vol-0e161bc9fa6edf7dc

Tipo de volumen [Información](#)
SSD de uso general (gp2)

Tamaño (GiB) [Información](#)
10
Min.: 1 GiB, máx.: 16384 GiB. El valor debe ser un número entero.

IOPS [Información](#)
100/3000
Referencia de 3 IOPS por GiB con un mínimo de 100 IOPS, ampliable a 3000 IOPS

Cancelar Modificar

Imagen 21: Pestaña detalles del volumen.

Una vez realizados estos cambios, se procede a reiniciar la instancia. Al ejecutar este paso se puede observar como se han implementado las modificaciones de tipo y volumen en nuestra instancia, haciendo que está ahora tenga más memoria y más espacio en disco(**imagen22**).

Servidor web i-0e601a33c8d05a6e2 Detenida t2.small Sin alarmas us-east-1a

Instancia: i-0e601a33c8d05a6e2 (Servidor web)

Filtrar dispositivos de bloques

ID de volumen	Nombre del di...	Tamaño del volu...	Estado de la cone...	Hora de conexión
vol-0e161bc9fa6edf7dc	/dev/xvda	10	Asociado	Fri Jan 06 2023 20:32:21 GM...

Imagen 22: Se observan marcados en rojo los cambios introducidos de tipo y volumen en la instancia.

3. Eliminar la instancia.

Para eliminar la instancia se procede a desmarcar la casilla “Habilitar” de la pestaña “Cambiar protección de terminación” (**imagen 23**).

Cambiar protección de terminación

Habilite la protección de terminación de la instancia para evitar que esta se termine accidentalmente. [Más información](#)

ID de la instancia
i-0e601a33c8d05a6e2 (Servidor web)

Protección de terminación
☐ Habilitar

Protección de terminación desactivada.
La instancia ya no está protegida contra la terminación accidental. Si la instancia se termina, se pierden los datos almacenados en almacenamiento efímero.

Cancelar Guardar

Imagen 23: Pestaña Cambiar protección de terminación

Una vez realizado esto, ya se podrá terminar la instancia (**imagen 24**)



Imagen 24: Marcado en rojo el estado de la instancia.

Comentario de la práctica

Con esta práctica se ha podido manejar y observar el funcionamiento de una instancia de Amazon EC2. Una instancia de Amazon EC2 es un servidor virtual en Elastic Compute Cloud (EC2) para ejecutar aplicaciones en la infraestructura de Amazon Web Services (AWS). Esta última es una plataforma de computación en la nube integral, mientras que EC2 es un servicio que permite a los suscriptores comerciales ejecutar programas de aplicación en el entorno informático.

Las instancias se crean a partir de imágenes de máquinas de Amazon (AMI). Están configuradas con un sistema operativo y otro software, que determinan el entorno operativo del usuario. Amazon proporciona varios tipos de instancias con diferentes configuraciones de CPU, memoria, almacenamiento y recursos de red para satisfacer las necesidades del usuario. Cada tipo está disponible en varios tamaños para abordar los requisitos de carga de trabajo específicos.

Por último, en la práctica además de aprender a lanzar, detener, relanzar y eliminar instancias, se ha podido realizar personalizaciones de las funciones de estas, como puede ser: el almacenamiento, la memoria disponible para la instancia, el sistema operativo y la AMI en la que se basa la instancia.