

© Germán Moltó, 2013-2025. Se prohíbe la divulgación, utilización, transmisión, distribución, reproducción y modificación total o parcial de este documento y de cualquier otro material educativo del Curso Online de Cloud Computing con Amazon Web Services por cualquier medio sin el previo y expreso consentimiento del autor, ni siquiera para ámbito académico y/o educativo. Este material es de uso estricta y exclusivamente personal.

22/04/2025

---

---

# Práctica

*Despliegue de Instancias de Máquinas Virtuales con Amazon EC2  
Usando la AWS Management Console*

---

---

# Práctica

*Despliegue de Instancias de Máquinas Virtuales con Amazon EC2 Usando la AWS Management Console*

## Contenido

|      |  |    |
|------|--|----|
| 1.   | Introducción .....   | 2  |
| 2.   | Resultados de Aprendizaje.....   | 2  |
| 3.   | Advertencias Previas .....   | 3  |
| 4.   | Conexión a la AWS Management Console.....                              | 3  |
| 4.1. | Listado de Regiones.....   | 5  |
| 5.   | Despliegue de Máquinas Virtuales en AWS.....                           | 6  |
| 5.1. | Creación del Par de Claves, Grupo de Seguridad y Elección de AMI ..... | 7  |
| 5.2. | Despliegue de Instancias de Máquinas Virtuales .....                   | 18 |
| 5.3. | Sobre las Características de las Instancias basadas en EBS .....       | 29 |
| 6.   | Despliegue de Instancias Basadas en Windows .....                      | 32 |
| 6.1. | Creación del Grupo de Seguridad y Selección de la AMI.....             | 32 |
| 6.2. | Despliegue, Datos de Acceso y Conexión a la Instancia .....            | 33 |
| 7.   | Conclusiones.....  | 39 |
|      | Información Adicional .....  | 39 |
|      | Referencias.....   | 39 |
|      | ANEXO .....  | 41 |

## 1. Introducción

Amazon Web Services (AWS) [1] es un proveedor de Cloud público pionero en el campo de las tecnologías Cloud (ofreciendo servicio desde 2006). De entre todos los servicios que ofrece, en esta práctica se utilizarán principalmente los siguientes:

- Amazon Elastic Compute Cloud (EC2).

Esta práctica permite que el alumno realice el despliegue de máquinas virtuales sobre la infraestructura de Cloud público de Amazon, usando EC2. Esto permitirá ofrecer una visión de la forma de trabajar desde el punto de vista del IaaS (*Infrastructure as a Service*), donde se realiza un aprovisionamiento de máquinas virtuales, que posteriormente debe gestionar de forma conveniente el usuario. Existen múltiples cuentas de usuario para los alumnos creadas mediante el servicio IAM (*Identity and Access Management*) bajo una cuenta de usuario de AWS con cargo a la tarjeta de crédito VISA del profesor. Esto permite agrupar el coste de todos los usuarios bajo una misma cuenta.

En esta práctica se utilizará fundamentalmente la AWS Management Console, que permite la realización de la mayor parte de la funcionalidad aquí explicada de forma gráfica a través de un navegador web. No obstante, AWS también ofrece la interfaz de línea de comandos (AWS CLI [18]) para interactuar con los principales servicios de AWS. El uso de línea de comandos facilita el *scripting* o la posibilidad de integrar la funcionalidad de AWS en aplicaciones propias del usuario.

Se recomienda que realices esta práctica si no te encuentras demasiado cómodo usando la línea de comandos en un entorno GNU/Linux. En cualquier caso, en esta versión de la práctica también tendrás que utilizar un poco la línea de comandos para algunas situaciones.

## 2. Resultados de Aprendizaje

---

Se espera que, una vez finalizada la práctica, el alumno sea capaz de:

- Conocer el esquema de funcionamiento a nivel de usuario de Amazon EC2.
- Entender el concepto de máquina virtual y su mecanismo de despliegue a través EC2.



1. Tu profesor te habrá asignado un número. Los comandos que aparecen en el boletín hacen referencia al usuario alucloudo. Por favor, **sustituye en los comandos que veas oo por tu número** (por ejemplo, si tu número es 06, entonces el usuario que has de utilizar es alucloudo6). Recuerda esta regla para facilitar tanto tu trabajo como el del resto de compañeros. Para facilitar tu trabajo, en los comandos se utiliza una variable de entorno llamada ID que se debe resolver a tu número.
2. En esta práctica haremos ejecuciones reales sobre un proveedor de Cloud público, que generan un coste económico. Asegúrate de **liberar apropiadamente los recursos** (terminar instancias si ya no las vas a gastar, etc.) para **no incurrir en costes adicionales**. Si tienes alguna duda al respecto consulta con tu profesor.
3. Cualquier recurso creado en AWS que no cumpla con la nomenclatura indicada en este boletín podrá ser automáticamente eliminado por parte del instructor.
4. Trabajarás exclusivamente en la región us-east-1 (N. Virginia) de AWS. El acceso al resto de regiones de AWS ha sido restringido por el instructor.
5. Recuerda que hay un sistema de recompensas, definido en la Guía de Prácticas, por el que podrás aumentar la duración del curso reportando las discrepancias que encuentres en este boletín frente a posibles cambios introducidos por AWS. Cuento con tu colaboración.

### 3. Advertencias Previas

En primer lugar, tienes a tu disposición en PoliformaT una guía para la realización de las prácticas que explica el uso de un cliente SSH para conectarse al entorno de realización de prácticas, así como la forma de acceder a la AWS Management Console mediante un navegador web.

En segundo lugar, a lo largo de este boletín verás comandos que hay que ejecutar en una ventana de terminal conectada por SSH a una máquina (virtual) Linux remota. Para facilitarte el trabajo, puedes copiar y pegar los comandos de este boletín en la ventana de terminal. No obstante, deberás tener cuidado con aquellos comandos que utilicen comillas simples (o dobles). A veces, al copiar el comando del boletín y pegarlo en la ventana de terminal, el carácter asociado a las comillas no es el apropiado, por lo que deberás modificar el comando en la ventana de terminal para que lleve las comillas apropiadas.

A lo largo del boletín verás que se utiliza \$ID para referirse a tu identificador de alumno. Si tu nombre de usuario es alucloud25 entonces \$ID debe sustituirse por 25 en todos los nombres que veas. Respeta la nomenclatura de los recursos indicada en la práctica para facilitar tanto tu trabajo como el de tus compañeros e instructor.



Este boletín está diseñado para responder a la problemática común que te puedes encontrar durante la resolución de la práctica. Si te surge algún problema, lo más probable es que el boletín te explique a continuación una posible solución al respecto. Revisa la propuesta antes de contactar con el instructor. Si encuentras un problema que no está explicado en el boletín contacta con el instructor explicándolo con detalle para así aislarlo y resolverlo.

Ten en cuenta que EC2 introduce cambios frecuentes en su interfaz. Este boletín está adaptándose progresivamente a la nueva interfaz de la consola de EC2, teniendo en cuenta que se introducen cambios bastante frecuentes en la misma. En cualquier caso, los cambios no te impedirán realizar la práctica, pero no dudes en avisarme si detectas alguna discrepancia importante.

### 4. Conexión a la AWS Management Console

En primer lugar, conéctate con las credenciales de IAM que te suministró tu instructor a la siguiente dirección.

<https://grycap-aws.signin.aws.amazon.com/console>

The screenshot shows two side-by-side web pages. On the left is the 'Inicio de sesión de usuario de IAM' (IAM User Sign-in) page. It has fields for 'ID de cuenta (12 dígitos) o alias de cuenta' (Account ID (12 digits) or user alias) containing 'grycap-aws', 'Nombre de usuario de IAM' (IAM User Name) highlighted in yellow containing 'alucloud00', 'Contraseña' (Password) masked, and a checkbox for 'Mostrar contraseña' (Show password). Below these are links for 'Iniciar sesión' (Sign In), 'Iniciar sesión con el correo electrónico del usuario raíz' (Sign in with root user email), 'Crear una cuenta de AWS' (Create a new AWS account), and 'Recordar esta cuenta' (Remember this account). At the bottom, there's a small note about accepting the AWS Customer Agreement and privacy policy, followed by a link to 'Acerca de cookies' (About cookies). On the right is the 'Amazon Lightsail' landing page, featuring a cartoon robot, the text 'Lightsail is the easiest way to get started on AWS', a 'Learn more' button, and a 'Get Started' button.

El servicio IAM (Identity and Access Management) [21] permite la creación de múltiples cuentas vinculadas a usuario de AWS, de manera que múltiples personas pueden acceder a AWS usando las credenciales de su usuario IAM con cargo a la tarjeta de crédito del usuario AWS para el que han sido creadas.

Por ejemplo, en una empresa puede haber una única cuenta de AWS y luego crear múltiples usuarios para diferentes departamentos.

Una vez autenticado, obtendrás acceso a la consola de administración de AWS (AWS Management Console), tal y como se muestra en la siguiente figura.

The screenshot shows the AWS Management Console homepage. At the top, there are sections for recently visited services (Visitados recientemente) and applications (Aplicaciones). Below these are sections for AWS Health, Cost and Usage, and a welcome message (Le damos la bienvenida a AWS) with links to AWS introduction, certification, and news. The 'Costo y uso' section displays current costs, expected final costs, and cost-saving opportunities. A bottom navigation bar includes links to AWS Health and Billing and Cost Management.

Esta herramienta web permite la administración de los principales servicios de AWS. Si pulsas sobre *Servicios* (en la parte superior izquierda de la barra) aparecerán todos los servicios que pueden ser gestionados desde la AWS Management Console:

## 4.1. Listado de Regiones

La mayoría de los servicios de AWS pueden operar en diferentes regiones, que representan zonas geográficas. Es posible obtener un listado de las regiones que actualmente están disponibles pulsando sobre el botón desplegable de la barra superior al lado de la cuenta de usuario.

Podrás ver las regiones que actualmente están disponibles para ser utilizadas. Para las prácticas utilizaremos la región por defecto que utiliza Amazon: us-east-1. Esta región está localizada en la costa este de Estados Unidos, en Virginia (EE.UU.) y te aparecerá en la interfaz web como N. Virginia. En caso de tener seleccionada otra región, asegúrate de que eliges la región de N. Virginia. Cada región tiene diferentes zonas de disponibilidad (*availability zones*), que son diferentes centros de datos dentro de la misma región, con el objetivo de ofrecer alta disponibilidad dentro una región. Los fallos de una zona de disponibilidad no deben afectar a otra puesto que involucran máquinas y redes diferentes.

## 5. Despliegue de Máquinas Virtuales en AWS

En esta sección se plantea el despliegue de una máquina virtual de la forma más sencilla posible, a partir de una AMI (*Amazon Machine Image*) [19] ya existente. Para ello, será necesario elegir el servicio EC2 en el listado principal de servicios y entrar dentro de la consola de administración de EC2.

The screenshot shows the AWS EC2 console interface. On the left, there's a sidebar with navigation links for various EC2 services like Instances, Images, and Block Store. The main content area is divided into several sections:

- Recursos:** Shows a summary of resources in the US East (N. Virginia) region, including 1 instance in execution, 1 elastic IP address, 1 snapshot, 5 snapshots, 0 load balancers, 0 auto-scaling groups, 0 security groups, 0 reservations, 0 dedicated hosts, 4 instances, 2 volumes, and 117 key pairs.
- Lanzar la instancia:** A button to launch a new instance.
- Estado del servicio:** A section showing a red error message: "Se produjo un error" (An error occurred) with a link to "Diagnose with Amazon Q".
- Zonas:** A table listing availability zones with their IDs: us-east-1a (use1-az1), us-east-1b (use1-az2), us-east-1c (use1-az3), us-east-1d (use1-az4), us-east-1e (use1-az5), and us-east-1f (use1-az6).
- Alertas de instancia:** Shows 0 alerts.
- Eventos programados:** Shows no scheduled events.
- Migrar un servidor:** Information about using AWS Application Migration Service.
- Atributos de la cuenta:** Shows VPC predeterminada (none), Configuration (Protection and data security, Zones, EC2 console series, Credit limit specification, EC2 console preferences), and Información adicional (Introduction guide, Documentation, All resources, Forums, Prices, Contact us).

Posteriormente, se seguirá el proceso descrito en la Figura 1.



**Figura 1. Acciones a realizar para el despliegue de instancias en Amazon EC2.**

## 5.1. Creación del Par de Claves, Grupo de Seguridad y Elección de AMI

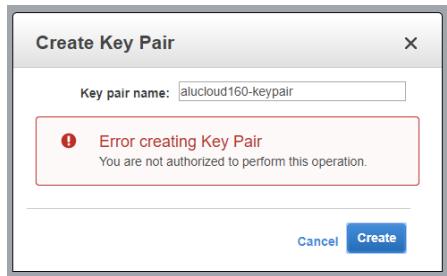
### 1. Construcción del par de claves.

En primer lugar, asegúrate de que estás conectado a la consola de administración del servicio EC2 y no a la consola de administración del servicio IAM (Identity & Access Management). Inicialmente será necesario construir un par de claves (*keypair*). Se trata de un par (clave pública, clave privada) utilizado para que puedas conectarte a la máquina virtual mediante SSH sin tener que especificar la contraseña. La clave privada la almacenará el usuario en su equipo (en nuestro caso, en el entorno de prácticas). La clave pública se guarda automáticamente en Amazon y se injectará en la máquina virtual en el momento del arranque. También es posible importar un par de claves que el usuario ya tuviera, para usarlas en EC2. Ten en cuenta que los pares de clave creados van ligados a una región concreta y no pueden ser compartidos entre diferentes regiones. El par de claves podrá ser compartido para acceder a otras instancias. Por lo tanto, puede crearse una única vez.

Elige la opción Pares de Claves (*Key Pairs*) del menú lateral, pulsa sobre el botón “Crear par de claves” e indica el nombre del par de claves que deberá ser alucloudXX-keypair (sustituye XX por tu identificador de usuario, de manera que si eres alucloud40 el par de claves se debe llamar alucloud40-keypair). Recuerda utilizar exactamente el nombre propuesto en este boletín de prácticas. De lo contrario, tu par de claves será eventualmente eliminado. Además, asegúrate de elegir el formato de fichero de claves PEM y el tipo RSA tal y como se muestra en la figura siguiente.

The screenshot shows the 'Create key pair' step in the AWS EC2 console. The top navigation bar shows 'EC2 > Pares de claves > Crear par de claves'. The main title is 'Crear par de claves' with a 'Información' link. Below it, a section titled 'Par de claves' defines what a key pair is: 'Un par de claves, compuesto por una clave privada y una clave pública, es un conjunto de credenciales de seguridad que se utilizan para demostrar su identidad cuando se conecta a una instancia.' The 'Nombre' field is filled with 'alucloud40-keypair'. A note says 'El nombre puede incluir hasta 255 caracteres ASCII. No puede incluir espacios al principio ni al final.' The 'Tipo de par de claves' section has 'RSA' selected. The 'Formato de archivo de clave privada' section has '.pem' selected, with a note 'Para usar con OpenSSH'. The 'Etiquetas' section is labeled 'opcional' and notes 'No hay etiquetas asociadas a este recurso.' A button 'Agregar nueva etiqueta' is present. At the bottom, there are 'Cancelar' and 'Crear par de claves' buttons.

Si obtienes el siguiente mensaje de error:



Asegúrate de que estás conectado a la región del N. Virginia. No tienes permisos para usar otras regiones:

Una vez creado el par de claves, se descargará automáticamente el fichero que contiene la clave privada, cuyo nombre será alucloud40-keypair.pem (para el caso del alumno con dicho identificador).

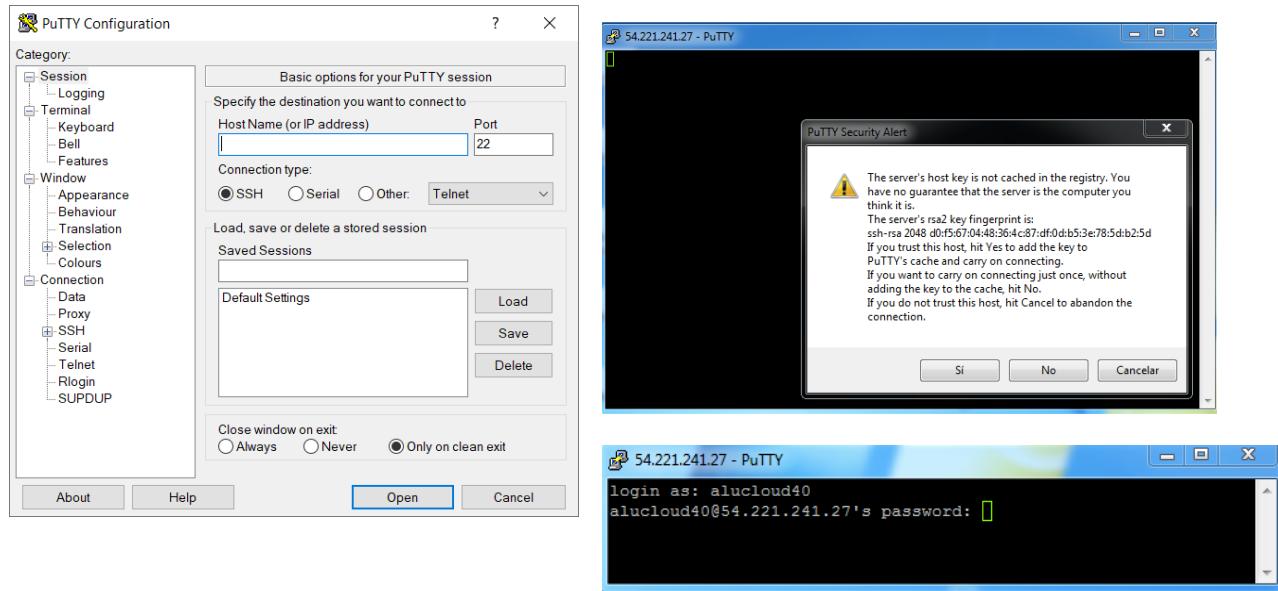
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAYx5Pldyk4DmNy/QU5k80XNi0s7wJiJViChZl82cm3KOUqTDB0QMUjxyK/1Xo
JLoysbL/8ICmywdh0fKzB5/bGsuYRe34FwzjeTQPuuqcLg481gjE2q+wfv1uG1j1Ho3mtwKVAE
KT+05T1sc0T-DmuVd5Hza3P9qj583vhauA2zBMvUc6LzpSA1QGCCdxsYGzfEzLbvR04AytfGveQ0
UJu2++-isVxsaltTM-F+mtpRqVrrmwirAy6LiRmsSTVXYnkeF4jd1kx3ln9uc7MInE/uWvC2L
Ya+j6R0mEM6nrojCuaLdgipXAt+iuNUXukrjDWYvgAs8H2auflhNRlsEBT07/LgefibiByLN03AwPd
zs4B+uNhbPdai/wxkbrJ7rbpbRHBTjpdpF5izASLw9KJnhF-xF22CMFr+Up2DsP8KGrg5CLK
VblgKJ55jL+8mGoEd0Eu6b5u/v/e4uAKFQ+x3iBMQK2tHjVveCKVqdZ5RZNVTz0Ph/C1+g/AKcqL
AoGBAP1XwT80iTBRLJMSNh59h/yZK+leIzytURLHf1PF7pLXLY4af5nxuuA063Gq3EWf42RS01p
oZhRdm20/MN010rGMat2rWNMVduVupTZIYjxPWO09u5RwS7kURmXamb1mNBgsA0LA2VMyhtfjP
rK77tVmrkWkghamTAJVEvhgtAoGAR4+PAqPrzUQjPN00y2C+PiFN0j62v4Dg90ZR9o37fzheU3
dfxNzkrh9Po33x6TA8i+XL9jM1y0ZWN8fx7vhaxq4702md2aucNDNVuY6507HK80PfMcw3Np2o5
Vqr4Gj5PAikS/vPlKJ3Uenk3YlqzofRA3uTSU1cJ0hx2ECgYEAxGRNifJh7swCz1hdad12HIf
Tbd1sh1HcGAr2AsdR43oR6MIo6C97gSwmlygcicuI57ETLdIH+4a6H72/3pq4G0i4u/lB0xuogw
9hX4Nqqm1/gAQ3El0R/ENXwzbmg/C0geoIGqny7+r1o+0t4dtioslpMNzEipffzHD1Mg=
-----END RSA PRIVATE KEY-----
```

dicho fichero más adelante para conectarnos mediante SSH sin contraseña a las instancias desplegadas usando Amazon EC2.

Asumiremos que la máquina del entorno de prácticas está en **lab.cursocloudaws.net** pero **recuerda utilizar la dirección del entorno de prácticas que te haya indicado tu instructor**<sup>1</sup>. Si trabajas desde un entorno GNU/Linux o macOS tendrás que abrir un terminal y ejecutar el siguiente comando (asegúrate de cambiar XX por tu identificador de alumno):

<sup>1</sup> Ten en cuenta que es posible que tu instructor te haya asignado la máquina lab2.cursocloudaws.net, por lo que **no te equivoques en este punto**. En el correo de bienvenida tienes indicada la máquina asignada.

Por el contrario, si utilizas Windows, puedes utilizar un cliente SSH como Putty [22] (tal y como indica la guía de realización de prácticas) para conectarte vía SSH al entorno de realización de prácticas. Para ello deberás indicar el nombre DNS o la dirección IP del entorno de prácticas (que el instructor te haya indicado otro nombre en el correo de bienvenida, en cuyo caso tendrás que utilizar dicho nombre) y abrir una conexión SSH remota con dicha máquina (pulsando el botón Open). Tras aceptar (pulsar Si) sobre la advertencia de seguridad, obtendrás una ventana de login en el que deberás introducir tu nombre de usuario (alucloudXX) y contraseña que te haya indicado tu instructor.



Superado el proceso de autenticación estarás conectado al entorno remoto de prácticas. Procedemos a copiar dicho fichero. Para ello, lo más fácil es copiar el contenido del fichero mediante el propio terminal. En primer lugar, abre el fichero con un editor como *vim*. Puedes ejecutar el comando anterior directamente en el entorno de prácticas sin cambiar el valor de \$ID por tu número. Existe una variable de entorno en la máquina del entorno de prácticas que sustituye \$ID automáticamente por dicho número.

```
:~$ vim alucloud$ID-priv.pem
```

Luego copia todo el contenido del fichero que contiene la clave privada (ábrelo para ello con el bloc de notas o cualquier otro editor de textos), asegurándote de que eliges desde la línea (incluida)

-----BEGIN RSA PRIVATE KEY-----

hasta la línea

-----END RSA PRIVATE KEY----- (incluida).

En la ventana de terminal, pulsa la tecla *i* para pasar al modo inserción en vim y luego pega el contenido pulsando sobre el botón derecho del ratón. A continuación pulsa *ESC* y luego :wq seguido de *ENTER* para guardar el contenido del fichero. Es importante que el contenido de la clave privada no tenga líneas en blanco entre medias (dependiendo del programa que hayas utilizado para abrir y copiar la clave privada esto puede ocurrir). En definitiva, la clave privada debe tener el siguiente aspecto (el contenido será diferente):

```
:~$ cat alucloud$ID-priv.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAjNCEDdTzpyVstHX1u9c1DkdvIaZaDGtPTyCR6gDFzfwtUgdx9FUCH/uju
+ps3UUfiE2SKGkSs+pzT/f2E9M4OMeNR11f14nlQ9iHqFG36Ywmvgc8ILawLCCcdEOOBETLWZSctj
E6N+65cQephWMpMI7WxarSp7gdrnv0zDznT311DDkk6urOsDR6o54VcEwyHvT6Ay8nnnNcuTssK
Eme
...
1KXmFaT6ErgOpt4TwsmJiW2QUpikKISyk6o+Q8FdIGy2qAlkPS5db1s6IspIFjHBnsMDPt2FKa
```

```
EX5ITX21f6Qzb10mb7LFXJrm0nvB7qSqwiEDa1Z2De+2vTiaA/kVJ0nJJ1wXyVBO+a8=
-----END RSA PRIVATE KEY-----
```

Fíjate por tanto que la clave pública se habrá guardado automáticamente en Amazon EC2, mientras que la clave privada la acabas de guardar en el fichero alucloud\$ID-priv.pem (donde \$ID se sustituye por tu código de usuario). Es importante que el fichero donde se almacena la clave privada solo tenga permisos de lectura y escritura para el usuario. Para ello, se puede cambiar los permisos con la siguiente operación:

```
:~$ chmod 0600 alucloud$ID-priv.pem
```

No pierdas la clave privada. No hay forma de recuperarla, ni siquiera desde la AWS Management Console. Afortunadamente, siempre es posible borrar un par de claves y volver a crearlo nuevamente. Antes de continuar, asegúrate que el contenido del fichero alucloud\$ID-priv.pem contiene efectivamente una clave privada (con el formato que se muestra en el ejemplo anterior).

Si has creado correctamente par de claves puedes obviar lo que se explica a continuación. Por el contrario, si en el momento de la creación del par de claves obtienes un mensaje indicando que el par de claves ya existe, lo más probable es que algún otro alumno se haya confundido y haya creado el par de claves usando tu identificador (por ejemplo, que el alumno con identificador 06 haya creado el par de claves alucloud03-keypair). No podrás acceder a las instancias desplegadas con dicho par de claves al no disponer de la clave privada. Por ello, en ese caso, y tras asegurarte de que estás utilizando tu identificador de alumno correcto, puedes proceder a borrar tú mismo el par de claves desde la AWS Management Console a través de la barra lateral eligiendo “Key Pairs” y luego seleccionado el par de claves y con el botón derecho pulsando sobre “Delete”:

The screenshot shows the AWS EC2 Key Pairs page. On the left, there's a sidebar with 'New EC2 Experience' and a 'Tell us what you think' link. Below that are links for 'EC2 Dashboard', 'Events', 'Tags', 'Limits', and 'Instances'. Under 'Instances', there's a link to 'Instances'. The main area is titled 'Key pairs (1/144)' with a 'Actions' button and a 'Create key pair' button. There's a search bar labeled 'Filter key pairs'. The table lists four key pairs:

| Name               | Fingerprint                                | ID                     |
|--------------------|--|------------------------|
| alocloud295-keypar | 93:2d:d9:78:43:b5:41:5b:66:f4:e0:3c:6...   | key-017ddaa104ded366b3 |
| alucloud00-keypair | 3a:95:b3:bd:5a:41:1f:bf:b7:40:fc:cb:70:... | key-084c9c9def531f59   |
| alucloud02-keypair | 3e:bc:81:8f:d6:d6:a3:1e:e2:dd:55:0...      | key-0d4af7c40db89b464  |
| alucloud04-keypair | 92:2b:9e:6d:eb:bf:c6:42:81:27:01:5e:0...   | key-0df0ce6ce9a629bc6  |

Luego ya podrías proceder a la creación de un nuevo par de claves. Es posible que el instructor haya restringido la eliminación de los pares de claves para limitar que unos alumnos interfieran con otros. Por ello, si recibes un mensaje de error indicando que no es posible eliminarlo deberás avisar al instructor para que proceda a la eliminación del par de claves.

Recuerda que la clave pública del par de claves se injectará en la instancia únicamente en el momento del despliegue de la misma. Por ello, si eliminas el par de claves y vuelves a crear uno nuevo con el mismo nombre, esto no provoca que se actualice la clave pública de las instancias desplegadas con dicho par de claves.

## 2. Construcción del grupo de seguridad

A continuación, es preciso definir el grupo de seguridad (*security group*) al que la instancia (máquina virtual) pertenecerá. Un grupo de seguridad define un conjunto de reglas de cortafuegos y permisos de conexión especificando qué tipo de conexiones y hacia qué puertos de la instancia se permiten las conexiones. Múltiples instancias pueden utilizar el mismo grupo de seguridad. Por ejemplo, si se

pretende desplegar un servidor web que pretende ser administrado de forma remota vía SSH habrá que incluir la instancia en un grupo de seguridad que permita el acceso a los puertos 22 (SSH) y 80 (HTTP) desde Internet. El grupo de seguridad podrá ser compartido por parte de otras instancias. Por lo tanto, puede crearse una única vez.

En primer lugar, asegúrate de que no existe ya un grupo de seguridad con el nombre gs-aws-XX (donde XX es tu identificador de usuario). Si ya existe, bórralo para proseguir con la creación del mismo (podrías reaprovechar el grupo de seguridad siempre que tuviera las reglas bien configuradas).

Creamos un grupo de seguridad llamado gs-aws-XX que permita acceso a los puertos TCP 80 (HTTP) y 22 (SSH) desde el exterior. Para ello, desde la opción “Security Groups” pulsamos sobre el botón “Crear grupo de seguridad”.

The screenshot shows the AWS EC2 console with the "Security Groups" section selected. The main area displays a table of existing security groups, each with columns for Name, ID, VPC, Description, Owner, and Count. The table includes rows for various groups like "gs-aws-147-win", "gs-aws-174-win", and "gs-aws-183". At the top right of the table, there is a "Crear grupo de seguridad" (Create security group) button.

| Name                  | ID del grupo de segu... | Nombre del grupo ... | ID de la VPC             | Descripción  | Propietario | Númer... |
|-----------------------|-------------------------|----------------------|--------------------------|--------------|-------------|----------|
| sg-08bb8c4993158a6d03 | gs-aws-147-win          | vpc-83a213fb         | GS Alumno 147 (Wind...   | 974349055189 | 1 Ent       |          |
| sg-09025bea3567a99b09 | gs-aws-174-win          | vpc-83a213fb         | GS Alumno 174 (Wind...   | 974349055189 | 1 Ent       |          |
| sg-01ff20fc00a9a2e1f  | gs-aws-105              | vpc-83a213fb         | GS del alumno 105        | 974349055189 | 2 Ent       |          |
| sg-0b50f398fe9db63bd  | gs-aws-173-win          | vpc-83a213fb         | GS Alumno 173            | 974349055189 | 1 Ent       |          |
| sg-01c25b48fb50130f2  | gs-aws-183              | vpc-83a213fb         | GS del alumno 183        | 974349055189 | 2 Ent       |          |
| sg-0ed58de4be4e2eece  | gs-aws-48               | vpc-83a213fb         | aluctoud48               | 974349055189 | 2 Ent       |          |
| sg-025c48ef21318eb9d  | gs-aws-180              | vpc-83a213fb         | GS alumno 180            | 974349055189 | 3 Ent       |          |
| sg-07b02874ec04d252c  | gs-aws-69-win           | vpc-83a213fb         | GS Alumno 69 (Windo...   | 974349055189 | 1 Ent       |          |
| sg-0b7ca04292d5e1af1  | gs-aws-127              | vpc-83a213fb         | GS de aluctoud 127. P... | 974349055189 | 2 Ent       |          |

Debes indicar tanto el nombre (Name), que debe ser gs-aws-\$ID, como la descripción (Description) que queremos y el VPC (Virtual Private Cloud) [35], que debe ser el de nombre “default”. Más adelante aprenderás con detalle el concepto de VPC. Por ahora, es suficiente que sepas que un VPC es una subsección aislada de AWS compuesta por diferentes subredes, cada una de ellas en una zona de disponibilidad diferente, sobre la que se despliegan instancias de EC2. Recuerda respetar el esquema de nombres propuesto y sustituir \$ID por tu identificador de alumno. Comprueba nuevamente que has elegido el VPC correcto (de nombre *default* y de identificador *vpc-83a213fb*) antes de continuar.

The screenshot shows the "Crear grupo de seguridad" (Create security group) wizard. The first step, "Detalles básicos" (Basic details), is displayed. It contains three input fields: "Nombre del grupo de seguridad" (Security group name) with value "gs-aws-00", "Descripción" (Description) with value "GS del alumno 00", and "VPC" (VPC) with value "vpc-83a213fb". Below the VPC field is a note stating "El nombre no se puede editar después de su creación." (The name cannot be edited after creation).

Seguidamente, definimos los rangos de direcciones que pueden tener acceso a determinados puertos de la instancia. En este caso se autorizará el acceso al puerto TCP 80 (donde suele escuchar un servidor web) desde cualquier máquina de Internet y al puerto 22 (donde suele escuchar el servicio SSH) únicamente desde la IP del entorno de prácticas (la máquina lab.cursocloudaws.net o lab2.cursocloudaws.net, en función de lo que te haya indicado tu instructor en el correo de bienvenida). Para averiguar dicha IP debes ejecutar el siguiente comando desde dicha máquina o

desde cualquier otra máquina Linux o macOS (asegúrate de indicar el nombre de máquina que te haya indicado el instructor en el correo de bienvenida<sup>2</sup>; usaremos lab.cursocloudaws.net a continuación a modo de ejemplo):

```
:~$ nslookup lab.cursocloudaws.net

Server:      10.0.0.2
Address:     10.0.0.2#53

Non-authoritative answer:
Name:  lab.cursocloudaws.net
Address: 3.217.191.49 ← Esta es la IP pública de la máquina lab.cursocloudaws.net
```

Para ello, una vez seleccionado el grupo de seguridad, **desde el panel Reglas de entrada (Inbound rules)** debes crear una nueva regla pulsando sobre el botón “Agregar regla” (Add Rule) con “Intervalo de puertos” (Port range) 80 y “Origen” (Source) 0.0.0.0/0, así como otra regla análoga para el puerto 22. Esta información se resume en la siguiente tabla y se muestra también desde la interfaz web (aunque con otra dirección IP).

| Tipo | Protocolo | Intervalo de puertos | Origen                  |
|------|-----------|----------------------|-------------------------|
| HTTP | TCP       | 80                   | Anywhere-IPv4 0.0.0.0/0 |
| SSH  | TCP       | 22                   | 3.217.191.49/32         |

**Editar reglas de entrada** Información

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

| Reglas de entrada                     |      |             |           |                      |   |   |
|---------------------------------------|------|-------------|-----------|----------------------|---|---|
| ID de la regla del grupo de seguridad | Tipo | Información | Protocolo | Intervalo de puertos | Origen                                    | Descripción: opcional   |
| <small>Información</small>            |      |             |           |                      |   |   |
| sgr-02bee419c6dea69e3                 | HTTP | ▼           | TCP       | 80                   | Person... ▼                               | <input type="text" value="0.0.0.0/0"/> Eliminar   |
| sgr-0b435dd3e9874b2f5                 | SSH  | ▼           | TCP       | 22                   | Person... ▼                               | <input type="text" value="54.157.106.156/32"/> Eliminar   |
| <a href="#">Agregar regla</a>         |      |             |           |                      |   |   |
|                                       |      |             |           | Cancelar             | <a href="#">Previsualizar los cambios</a> | <a href="#" style="background-color: orange; color: white; border: none; padding: 2px 10px;">Guardar reglas</a> |

<sup>2</sup> Ten en cuenta que es posible que tu instructor te haya asignado la máquina lab2.cursocloudaws.net, por lo que no te equivoques en este punto. En el correo de bienvenida tienes indicada la máquina asignada.

Asegúrate de que has introducido las reglas en el panel de “Reglas de entrada” y no “Reglas de salida”.

Fíjate en el uso de CIDR (*Classless Inter-Domain Routing*) para definir los rangos de direcciones que pueden tener acceso a la instancia. Una vez creadas las dos reglas será necesario pulsar sobre “Create security group” para confirmar la creación y aplicación de las reglas. Fíjate que, al final, un grupo de seguridad de EC2 no es más que una configuración de cortafuegos sobre un grupo de instancias (todas las instancias que se desplieguen con dicho grupo de seguridad). Si quieras conectarte a tus instancias de SSH desde tu equipo local (o desde cualquier punto de Internet) entonces puedes añadir una nueva regla donde el *source* sea 0.0.0.0/0. La desventaja de esta aproximación es que la instancia queda más expuesta a posibles amenazas.

Con respecto a las “Reglas de salida” (*Outbound*), por defecto ya hay una regla que permite todo el tráfico de salida hacia Internet. No elimines la regla de la pestaña Outbound. Déja la configuración por defecto.

The screenshot shows the AWS CloudFormation console interface. At the top, there's a search bar and a 'Create new stack' button. Below that, a table lists existing stacks. One stack, 'stack-aws-00', is highlighted. The 'Outputs' tab is selected, showing a single output named 'MyNewStack' with the value 'stack-aws-00'. Below the stack list, the 'AWS Lambda' service is shown with a single function named 'lambda-aws-00'.

Ten en cuenta que te aparecerán listados los grupos de seguridad creados tanto por ti como por el resto de alumnos del curso, debido al mecanismo de gestión de usuarios empleados.

En realidad, no hubiera sido necesario que cada alumno cree su propio grupo de seguridad, ya que, al representar un conjunto de reglas, puede reutilizarse para diferentes usuarios. Sin embargo, esto permite conocer el proceso completo de despliegue de una instancia.

### 3. Selección de la Imagen de Máquina Virtual

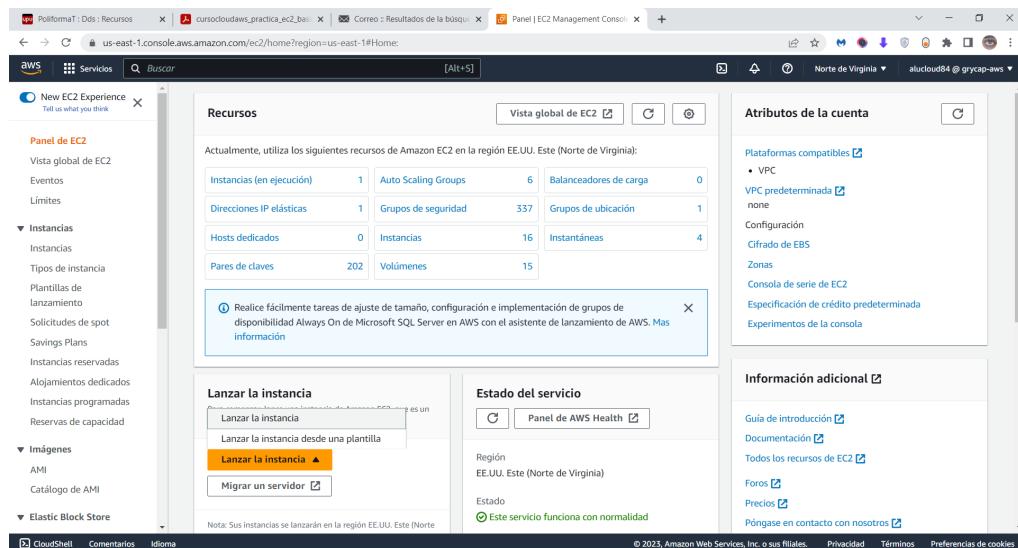
Una imagen de máquina virtual incluye toda la configuración para desplegar una instancia en Amazon EC2. En el contexto de Amazon, éstas se denominan *Amazon Machine Image* (AMI), definidas como un tipo especial de sistema operativo pre-configurado y software de aplicación usado para crear una máquina virtual (instancia) en Amazon EC2. Sirve como una unidad básica de despliegue para los servicios desplegados en EC2. Existen muchas AMIs de acceso público, y el usuario puede crear una

AMI específica, bien desde cero o a partir de otra AMI existente. Existen AMIs con diferentes variantes de Linux y Windows. Existen dos tipos de AMIs en AWS:

- AMIs basadas en S3 (denominadas *Instance-Store Images*). En las instancias de EC2 desplegadas a partir de estas AMIs, cualquier fichero nuevo creado o modificación de los existentes, desaparecerá cuando la instancia termine. En realidad, cuando se arranca la instancia es como si se clonase la imagen temporalmente, por lo que, al desplegar una nueva instancia de la misma imagen, ésta siempre mantiene la misma configuración base. Este tipo de instancias no pueden detenerse (stop) e iniciarse (start). Por el contrario, tan solo pueden ser reiniciadas o terminadas. Si se reinicia no se pierde ningún dato.
- AMIs basadas en EBS (denominadas *EBS Images*). En las instancias de EC2 desplegadas a partir de estas AMIs, se crea un volumen EBS que mantiene los datos de la misma y que se destruye cuando se termina la instancia pero que se mantiene al detenerla. Por tanto, los cambios realizados en estas instancias sí que se mantienen si ésta se detiene (stop) y luego se inicia (start).

Las AMIs basadas en EBS son las más modernas y tienen muchas ventajas con respecto a las de tipo *instance-store* (tamaño de partición más grande, posibilidad de detenerlas y volverlas a iniciar, etc.).

Es posible obtener un listado actualizado de las AMIs disponibles en AWS desde la consola de EC2 pulsando sobre el botón “Lanzar la instancia”:



Por ejemplo, en dicho catálogo busca una AMI que incluya una configuración de LAMP (Linux, Apache, MySQL y PHP) [16] para disponer de un servidor web ya preinstalado. Para ello introduce en la barra de búsqueda texto “Bitnami LAMP”<sup>3</sup> (sin las comillas dobles) y pulsa Enter.

The screenshot shows the 'Launch instance' wizard in the AWS Management Console. The user has entered 'bitnami lamp' into the search bar. Below the search bar, there are three tabs: 'Recientes' (Recent), 'Mis AMI' (My AMIs), and 'Inicio rápido' (Quick Start). Under 'Mis AMI', several AMI icons are listed, including Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and others. A specific AMI entry for 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type' is highlighted with a red box. This entry includes details like 'ami-0f56004c63e32376 (64 bits (x86)) / ami-0f53141013ebdc12 (64 bits (Arm))', 'Virtualización: hvm', 'Habilitado para ENA: true', and 'Tipo de dispositivo raíz: ebs'. Below this, a note says 'Apto para la capa gratuita' (Free tier eligible).

The screenshot shows the search results for 'bitnami lamp' in the AWS AMI search interface. On the left, there is a sidebar with filters for 'Pulir los resultados' (Refine results), 'Categorías' (Categories), 'Editor' (Editor), and 'Modelo de precios' (Price model). The main area shows a search bar with 'bitnami lamp' and a result list titled 'bitnami lamp (5 resultados)'. The first result is 'Bitnami package for LAMP' by Bitnami, which is described as 'Por Bitnami by VMware | Ver 8.1.26-0-r05 on Debian 11'. It has a rating of ★★★☆☆ 39 revisiones de AWS. A yellow 'Seleccionar' (Select) button is visible next to the result. The interface also includes a 'Ordenar por: Relevancia' (Sort by: Relevance) dropdown and navigation controls.

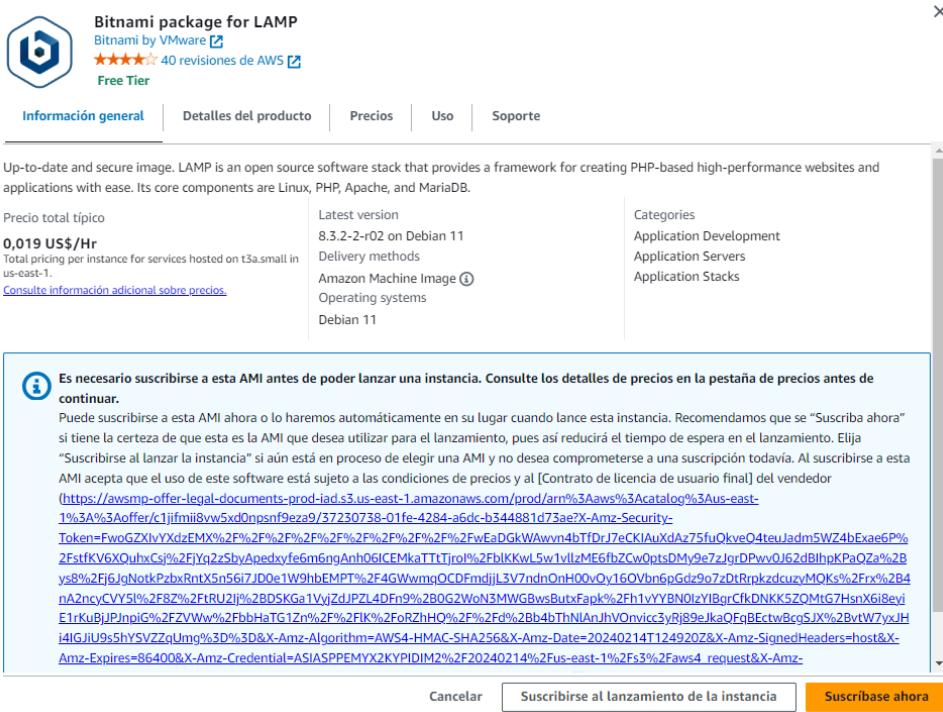
<sup>3</sup> Bitnami es una empresa que, entre otras funciones, produce AMIs para AWS: <https://bitnami.com/>

Por ejemplo “Bitnami package for LAMP” es una AMI de 64 bits creada por Bitnami [17] basada en Debian que viene con un servidor Apache configurado. Al elegir dicha imagen es posible acceder a información detallada sobre la misma, como el sistema operativo sobre el que está basada, la arquitectura para la que ha sido diseñada (64 bits), si está basada en EBS (en “AWS Services required” indica que es necesario Amazon EBS), una descripción del producto, la valoración que los usuarios de dicha AMI realizan de ella y los precios en los que el usuario incurrirá al utilizar dicha AMI en cada una de las regiones en las que esté disponible y dependiendo del tipo de instancia (t3.micro, m3.large, etc.). La AMI que hemos elegido incluye el soporte de virtualización de tipo HVM (Hardware Virtualization Machine) mientras que otras AMIS pueden soportar el tipo de virtualización PV (Paravirtual). Tienes una descripción de los distintos tipos de virtualización soportados por AWS en [29].

Por lo general, las AMIs suelen ser gratuitas y el usuario únicamente incurre en los costes por segundo de la instancia EC2 desplegada, dependiendo tanto de la región elegida como del tipo de instancia. Las AMIs van ligadas a regiones concretas, aunque se pueden transferir fácilmente de una región a otra. Por ello, según la región elegida, el identificador de AMI que finalmente obtendrás será diferente (serán AMIs diferentes, con identificadores diferentes, pero con idéntico contenido). También existen las Paid AMIs [23] donde una empresa puede cobrar por el uso de una AMI que previamente ha pre-configurado con un determinado software (típicamente de su propiedad). Esto permite pasar de un modelo basado en venta de licencias a un modelo donde el usuario paga por el uso que realiza de dicho software (segundos de ejecución de la instancia que ejecuta dicho software).

The screenshot shows the AWS Marketplace product page for the "Bitnami package for LAMP". At the top, there's a button labeled "Lanzar una instancia". Below it, the product name "Bitnami package for LAMP" is displayed, along with the logo for "Bitnami by VMware" and a rating of 3.5 stars from 39 reviews. A "Free Tier" badge is also present. Below this, there are tabs for "Información general" (selected), "Detalles del producto", "Precios", "Uso", and "Soporte". The main content area contains a brief description: "Up-to-date and secure image. LAMP is an open source software stack that provides a framework for creating PHP-based high-performance websites and applications with ease. Its core components are Linux, PHP, Apache, and MariaDB." To the left, a box displays the "Precio total típico" as "0,019 US\$/Hr" (Total pricing per instance for services hosted on t3a.small in us-east-1). It also includes a link to "Consulte información adicional sobre precios.". To the right, there are sections for "Latest version" (8.1.26-0-r03 on Debian 11), "Delivery methods" (Amazon Machine Image), "Operating systems" (Debian 11), and "Categories" (Application Development, Application Servers, Application Stacks). At the bottom right of the page is a large orange "Continuar" button.

Por ejemplo, en el panel anterior verás el coste horario de la instancia derivado del uso de EC2 puesto que no hay ningún cargo extra por el uso del software. Pulsa en “Continuar”. Es posible que obtengas un mensaje diciendo que es necesario suscribirse a la AMI. En ese caso pulsa en “Suscríbete ahora”.



A continuación, en los siguientes paneles deberás especificar (ahora se te proporciona un resumen, pero en la siguiente sección se te guía paso a paso para que veas dónde hay que especificar esta información):

- **El tipo de instancia** de EC2.
  - Elige el tipo t3.micro, que proporciona 1 GiB de RAM.
- **Configuración de VPC** (Virtual Private Cloud).
  - Network: vpc-83a213fb | default (**es posible que se haya seleccionado automáticamente otro VPC por lo que siempre asegúrate de usar el correcto**)
  - Subnet: subnet-2bfb6c4f | subnet-default-1a-public (o cualquier otra subred disponible)
- **Grupo de seguridad**.
  - Elige del desplegable tu grupo de seguridad gs-aws-\$ID. Ten en cuenta que el desplegable puede contener muchos grupos de seguridad (todos los de tus compañeros más algunos más, por lo que deberías navegar entre las diferentes páginas de resultados para encontrarlo). Puedes usar la herramienta de búsqueda de texto del navegador para encontrarlo más fácilmente.
- **Par de claves**.
  - Deberás elegir tu par de claves alucloud\$ID-keypair

Veamos paso a paso cómo realizar el despliegue.

## 5.2. Despliegue de Instancias de Máquinas Virtuales

### 1. Despliegue de la instancia en EC2

Una vez elegida la AMI de “LAMP packaged by Bitnami”, indica como nombre alucloudXX-linux, donde XX es tu identificador de usuario para identificar luego fácilmente tu instancia,

A continuación debes elegir el tipo de instancia, que será **t3.micro** (asegúrate que no lo confundes con otros tipos similares como t3a.micro). El uso de tipos de instancia superiores ha sido restringido por el instructor para evitar sobreconsumos innecesarios. Aprovecha para explorar los diferentes tipos de instancia y las características de cada uno de ellos.

The screenshot shows the 'Type' section of the AWS Lambda configuration interface. The 't3.micro' instance type is selected and highlighted with a blue border. The 't3.micro' row contains the following details: Familia: t3, 2 vCPU, 1 GiB Memoria. To the right of the list, there is a 'Comparar tipos de instancias' button and a note about the optimal price-to-performance ratio. Below the list, there is a search bar, a 'Crear un nuevo par de claves' button, and an 'Editar' button.

| Tipo de instancia |             |                          |
|-------------------|-------------|--------------------------|
| <b>t3.micro</b>   | Familia: t3 | 2 vCPU 1 GiB Memoria     |
| t1.micro          | Familia: t1 | 1 vCPU 0.612 GiB Memoria |
| t2.nano           | Familia: t2 | 1 vCPU 0.5 GiB Memoria   |
| <b>t2.micro</b>   | Familia: t2 | 1 vCPU 1 GiB Memoria     |
| <b>t2.small</b>   | Familia: t2 | 1 vCPU 2 GiB Memoria     |
| <b>t2.medium</b>  | Familia: t2 | 2 vCPU 4 GiB Memoria     |
| <b>t2.large</b>   | Familia: t2 | 2 vCPU 8 GiB Memoria     |
| <b>t2.xlarge</b>  | Familia: t2 | 4 vCPU 16 GiB Memoria    |
| <b>t2.2xlarge</b> | Familia: t2 | 8 vCPU 32 GiB Memoria    |
| <b>t3.nano</b>    | Familia: t3 | 2 vCPU 0.5 GiB Memoria   |
| <b>t3.micro</b>   | Familia: t3 | 2 vCPU 1 GiB Memoria     |

A continuación, elige tu par de claves:

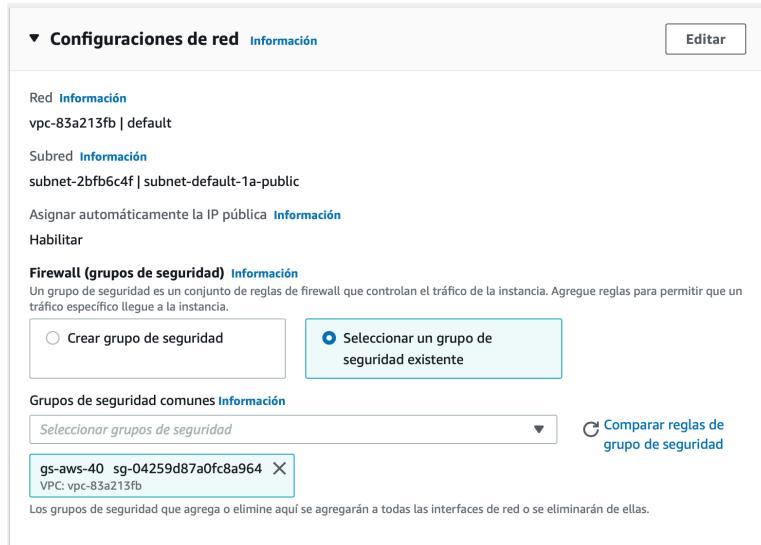
The screenshot shows the 'Key Pair' section of the AWS Lambda configuration interface. The 'alucloud40' key pair is selected and highlighted with a blue border. The 'alucloud40' row contains the following details: Continúe sin un par de claves (no recomendado) and Valor predeterminado. To the right of the list, there is a 'Crear un nuevo par de claves' button and an 'Editar' button.

| Nombre del par de claves - <i>obligatorio</i>  |                      |   |
|--|----------------------|---|
| Seleccionar                                    | alucloud40           | X |
| Continúe sin un par de claves (no recomendado) | Valor predeterminado |   |
| <b>alucloud40-keypair</b>                      | Tipo: rsa            |   |

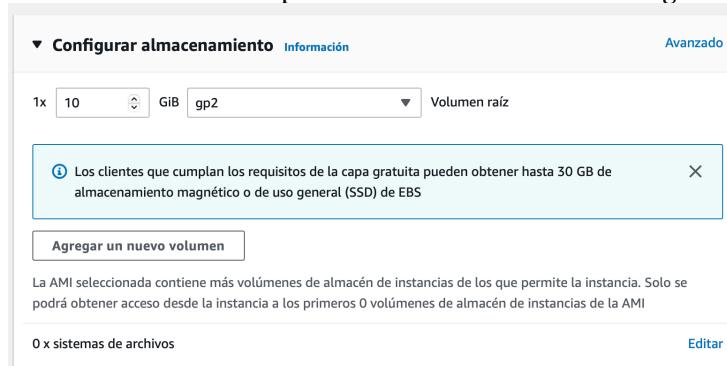
Puedes teclear el nombre de este para facilitar la búsqueda. Si no eliges tu par de claves no podrás conectarte posteriormente por SSH a la instancia.

Ahora deberás indicar dónde quieras desplegar dicha instancia. Lo haremos en el VPC llamado "default" con identificador vpc-83a213fb (asegúrate de no equivocarte y elegir otro VPC de los que

puedan haber creados). Elige como subred cualquiera de las que sean públicas, por ejemplo, subnet-2bfb6c4f | subnet-default-1a-public. En su momento, aprenderás la implicación de los VPC y crearás uno. Por el momento, solo es necesario que sepas que desplegaremos las instancias sobre una subred pública de un VPC por defecto. Es importante que compruebes que está activa la opción de auto-asignar IP pública. Aunque la subred pública está configurada para asignar por defecto una IP pública, he detectado que contadas ocasiones puede que no se asigne una IP pública si no está activa esta opción por lo que la activaremos como medida de precaución. También deberás elegir tu grupo de seguridad:

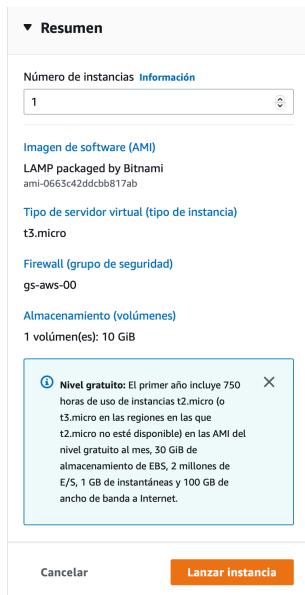


En el siguiente panel se puede cambiar el tamaño del volumen raíz (la cantidad de almacenamiento que estará disponible en “/”), así como añadir volúmenes adicionales para tener espacio de almacenamiento adicional dentro de la máquina virtual. No introduzcas ningún cambio.

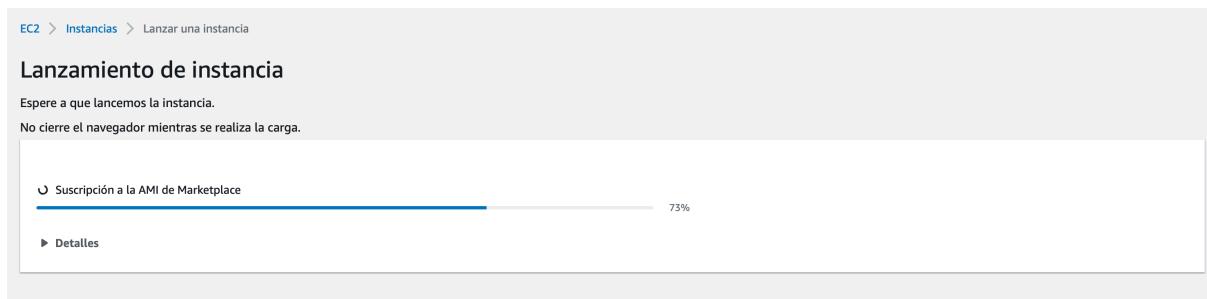


No introduciremos ningún cambio más en los paneles posteriores. Verás que, en “Detalles avanzados”, puedes especificar configuración adicional para una instancia, como la posibilidad de usar monitorización detallada de la instancia mediante CloudWatch [31], entre otras muchas opciones.

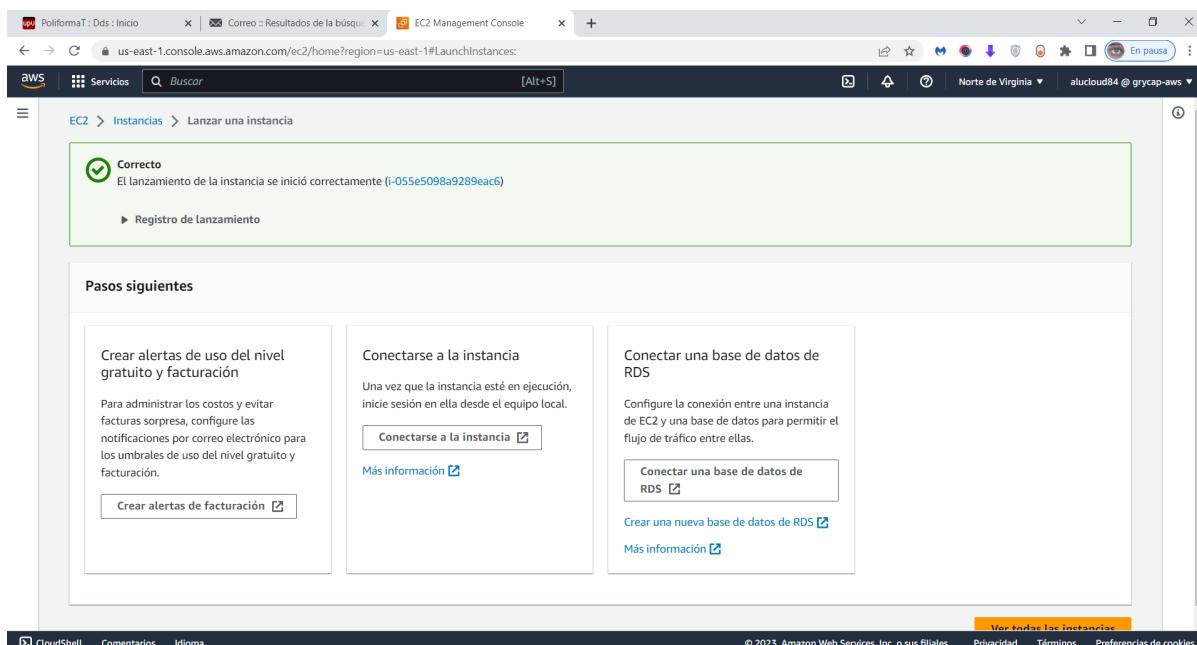
Finalmente, pulsa sobre el botón “Lanzar instancia”, que te aparece en el panel lateral de resumen:



Obtendrás un breve informe de progreso:



Y finalmente una confirmación de que ha sido desplegada la máquina virtual correctamente:



Si pulsas sobre el identificador de la instancia (i-0b2c2c4f328a5f9e6 en nuestro caso) irás directamente a la consola de administración de EC2 para ver el estado de esa instancia. Acuérdate de anotar el identificador de la instancia, ya que te hará falta más adelante.

| Name | ID de la instancia  | Estado de la i... | Tipo de inst... | Comprobación ... | Estado de la ... | Zona de dispon... | DNS de IPv4 públ... |
|------|---------------------|-------------------|-----------------|------------------|------------------|-------------------|---------------------|
| -    | i-0b2c2c4f328a5f9e6 | En ejecución      | t3.micro        | 2/2 comprobador  | Sin alarmas      | us-east-1a        | ec2-3-237-81-229    |

Si obtienes el siguiente mensaje de error (como el que se muestra en la figura siguiente) “*Your recent LAMP Stack powered by Bitnami launch failed. The requested Availability Zone is currently constrained and we are no longer accepting new customer requests for t1/m1/c1/m2/m3 instance types. Please retry your request by not specifying an Availability Zone or choosing us-east-1c, us-east-1d, us-east-1e*”, es porque la instancia estaba tratando de ser desplegada en una zona de disponibilidad que actualmente está restringida (por algún tipo de trabajo de mantenimiento). Podrás especificar la zona de disponibilidad eligiendo la subred correspondiente del VPC (si recuerdas, elegimos la primera subred que aparecía en la lista, creada para la zona de disponibilidad us-east-1a).

**Launch Failed**  
The requested Availability Zone is currently constrained and we are no longer accepting new customer requests for t1/m1/c1/m2/m3 instance types. Please retry your request by not specifying an Availability Zone or choosing us-east-1c, us-east-1d, us-east-1e.  
[Hide launch log](#)

Initiating launches: Failure Retry

Cancel Back to Review Screen Retry Failed Tasks

A continuación, procede conectarte a la AWS Management Console para comprobar el estado de la instancia en ejecución. Pulsando directamente sobre el enlace del mensaje se acude directamente a dicha consola web de administración. Alternativamente, deberás pulsar sobre el apartado “Instances” dentro de la consola de administración de EC2. Es posible que en dicha consola aparezcan mensajes de aviso (como el mostrado en el recuadro de color naranja) pero no están relacionados con el despliegue de tu instancia.

| Instances (running)    | 7  | Dedicated Hosts | 0   | Elastic IPs    | 4 |
|------------------------|----|-----------------|-----|----------------|---|
| Instances (all states) | 19 | Key pairs       | 127 | Load balancers | 0 |
| Placement groups       | 1  | Security groups | 199 | Snapshots      | 6 |
| Volumes                | 18 |                 |     |                |   |

En el panel de control de Amazon EC2 verás un listado con todas las instancias desplegadas actualmente por todos los usuarios IAM vinculados a la cuenta AWS del instructor del curso. Por tanto, no verás únicamente las instancias desplegadas por ti sino también las de tus compañeros y las del instructor.

| Name                    | ID de la instancia  | Estado de la i... | Tipo de inst... | Comprobación ... | Estado de la ... | Zona de dispon... | DNS de IPv4 públ... |
|-------------------------|---------------------|-------------------|-----------------|------------------|------------------|-------------------|---------------------|
| vpc-nat00               | i-066fd20c61cc095ba | Detenida          | t1.micro        | –                | Sin alarmas +    | us-east-1a        | –                   |
| rCUDA-server-nat        | i-0a14070c02b5e63ba | Detenida          | p2.xlarge       | –                | Sin alarmas +    | us-east-1a        | –                   |
| test-oscar-k3s-srisc    | i-045c353c9854ec4e6 | Detenida          | t4g.medium      | –                | Sin alarmas +    | us-east-1a        | –                   |
| lambda-vpc-nat-instance | i-0efdf8d0fe18da11d | Detenida          | t2.micro        | –                | Sin alarmas +    | us-east-1b        | –                   |
| rCUDA-server            | i-08e434c65164aa487 | Detenida          | p2.xlarge       | –                | Sin alarmas +    | us-east-1e        | –                   |
| cursocloudaws-lab       | i-0209084e6db346725 | En ejecución      | t3.micro        | 2/2 comprobador  | 3 alarma +       | us-east-1e        | ec2-54-157-106-15   |
| –                       | i-0b2c2c4f328a5f9e6 | En ejecución      | t3.micro        | 2/2 comprobador  | Sin alarmas +    | us-east-1a        | ec2-3-237-81-229.   |

Es relativamente sencillo averiguar qué instancia acabas de desplegar, no solo por el nombre que le has dado, sino también revisando el par de claves utilizado (columna Key Name). Esto permite averiguar el identificador de la instancia (columna Instance ID). En efecto, cada instancia lleva asociado un identificador único. Es importante que anotes los identificadores de las instancias que vas desplegando para posteriormente terminarlas cuando ya no sean necesarias. Puedes utilizar el botón de refresco de la interfaz (al lado del botón “Connect”) para ver si tu instancia ya ha pasado a estado “Running”, pues a veces la interfaz no se refresca automáticamente.

El tipo de instancia elegido (*t3.micro*) determina las características del hardware virtual y, por lo tanto, las prestaciones de la instancia. Puedes encontrar la información más actualizada sobre los precios de las instancias, así como el resto de tipos de instancias en [13], aunque una buena página para consultarlos de forma fácil es <https://ec2instances.info/>

El precio de los tipos de instancia depende de la región en la que se desplieguen. Aunque los precios se muestran por hora, la facturación se realiza por segundos.

La instancia se ha desplegado en la región us-east-1 (Virginia del Norte, USA), en la zona de disponibilidad vinculada a la subred del VPC elegida. Concretamente, esta instancia se ha desplegado en la zona de disponibilidad us-east-1d. Podrás conectarte por SSH conociendo la IP pública o el nombre DNS público.

Si lo que deseas es obtener un listado que únicamente incluya las instancias en ejecución que has desplegado tú entonces puedes especificar un filtro de búsqueda que sólo muestre aquellas instancias que han sido lanzadas con un determinado par de claves, tal y como se muestra a continuación:

| Name        | ID de la instancia  | Estado de la i... | Tipo de inst... | Comprobación de  | Estado de la al... | Zona de dispon... | DNS de  |
|-------------|---------------------|-------------------|-----------------|------------------|--------------------|-------------------|---------|
| alucloud100 | i-014dce635c76b076c | En ejecución      | t3.micro        | 3/3 comprobacion | Ver alarmas +      | us-east-1a        | ec2-44- |

Si no lo has hecho en el momento del despliegue, es posible asignarle un nombre a la instancia estableciendo una etiqueta a la misma. De esta manera, en la AWS Console se mostrará con un nombre concreto. Para ello puedes editar directamente desde el navegador el valor de la columna Name para dicha instancia:

The screenshot shows the AWS EC2 Instances page with a modal dialog open. The modal title is "Instancias (1/1) Información". It contains a search bar with placeholder text "Find instancia by attribute or tag (case-sensitive)" and a filter button "Quitar los filtros". Below these are two tabs: "Name" (selected) and "ID de la instancia". The "Name" tab has a dropdown menu with "Editar Name" and a text input field containing "alucloud40-linux". At the bottom of the modal are "Cancelar" and "Guardar" buttons.

| Name       | ID de la instancia | Estado de la i... | Tipo de inst... | Comprobación ... |
|------------|--------------------|-------------------|-----------------|------------------|
| alucloud40 | i-5f9e6            | En ejecución      | t3.micro        | 2/2 comprobacion |

Sobre la columna “Comprobación de estado” (*Status Checks*), un despliegue correcto de la instancia se marca con el símbolo verde y el mensaje “3/3 checks passed” o en español “3/3 comprobaciones superadas”. Ten en cuenta que a veces la interfaz no se actualiza automáticamente por lo que deberás refrescar periódicamente para ver el cambio de estado. Si eliges la instancia y pulsas sobre la pestaña llamada “Status Checks” tendrás más información sobre el tipo de comprobación que realiza EC2:

- *System Status Checks (Comprobaciones de estado de sistemas)*. Verifica que los sistemas usados por AWS para ejecutar la instancia funcionan correctamente. Básicamente comprueba que la instancia puede recibir paquetes de red (lo que significa que la infraestructura sobre la que se ejecuta la instancia funciona correctamente).
- *Instance Status Checks (Comprobaciones de estado de instancias)*. Verifica que el sistema operativo de la instancia está recibiendo tráfico y, por tanto, se ejecuta correctamente.
- *EBS Status Checks (Comprobaciones de estado de EBS asociado)*. Verifica que el volumen EBS creado para alojar la partición de arranque de la máquina virtual está correcto.

The screenshot shows the AWS EC2 Instances page with a single instance selected: "alucloud100". The instance ID is i-014dce635c76b076c, state is "En ejecución", type is "t3.micro", and status checks are "3/3 comprobaciones superadas". The "Estado y alarmas" tab is selected in the detailed view, showing sections for "Comprobaciones de estado" (with a note about detecting problems that could prevent the instance from running applications) and "Comprobaciones de estado de EBS asociado" (with a note about checking the EBS volume). The "Alarms" section is empty.

## 2. Conexión a la instancia

Dado que la máquina virtual dispone de servidor web preinstalado y servidor SSH, y que hemos habilitado los correspondientes puertos en el grupo de seguridad, debe ser posible acceder a la misma

tanto por SSH (puerto 22), desde un cliente SSH, como por HTTP (puerto 80) desde un navegador web. Hasta que la instancia no esté en estado *running* y haya pasado el suficiente tiempo para que arranque el SO, el servidor SSH y se copie la clave pública a la instancia, no será posible acceder a ella. En poco más de 2 minutos debería estar disponible.

Recuerda que puedes averiguar la IP pública y/o el nombre DNS de la instancia seleccionándola en la consola de administración de EC2 y viendo sus propiedades, como se muestra en la siguiente imagen. Filtra por tu identificador de usuario y elige la IP pública:

Desde el entorno de prácticas, la conexión por ssh a la instancia se realiza mediante el siguiente comando (recuerda utilizar la IP pública correspondiente o el nombre DNS. Es necesaria la clave privada para conectarte a una instancia de EC2. De hecho, si quisieras conectarte mediante usuario y contraseña deberás cambiar la configuración del servidor SSH [36]. Si no consigues conectar sigue leyendo un poco más adelante donde se explican posibles causas, antes de contactar con el instructor. Además, recuerda que el siguiente comando lo tienes que ejecutar desde la máquina de prácticas, no desde tu equipo local:

Fíjate que al desplegar la instancia en EC2, la clave pública del usuario (especificada en el *keypair*) se habrá inyectado en la cuenta de usuario *bitnami* de la instancia (máquina virtual). Por ello, le especificamos al cliente SSH que use la clave privada para conectarse como usuario *bitnami* a la instancia (fichero *alucloud\$ID-priv.pem*), sin necesidad de tener que especificar una contraseña. Otro tipo de imágenes, basadas en otras distribuciones de Linux pueden requerir otra cuenta de usuario diferente para conectarse a la instancia (a menudo *ec2-user*). En concreto, las basadas en Red Hat (Fedora, CentOS) requieren conectarse como usuario *root*, mientras que las basadas en Ubuntu suelen elegir el usuario *ubuntu*. En este caso concreto fíjate que el usuario elegido es *bitnami*. Esto es debido a la configuración específica de dicha AMI.

Generalmente, el creador de la AMI debe aportar la información de uso de la misma. Al tratar de lanzar una nueva instancia EC2, buscando por la AMI de interés verás un apartado “Uso”, donde indica el usuario a utilizar para conectarte a la instancia:

The screenshot shows the AWS Lambda console page for the 'LAMP packaged by Bitnami' AMI. At the top, there's a logo for Bitnami, the text 'LAMP packaged by Bitnami', 'Bitnami by VMware', a 4-star rating with 38 reviews from AWS, and 'Free Tier'. Below this, there are tabs: 'Información general', 'Detalles del producto', 'Precios', 'Uso' (which is highlighted in orange), and 'Soporte'. Under the 'Uso' tab, it says '64-bit (x86) Amazon Machine Image (AMI)'. It includes sections for 'Instrucciones de uso' (with a detailed text about connecting via SSH) and 'Recursos adicionales' (links to 'LAMP packaged by Bitnami', 'User Guide', and 'Changelog'). At the bottom right, there's a 'Continuar' button.

Si al conectarte vía SSH se te solicita una contraseña asegúrate de que: i) has esperado el tiempo suficiente desde que la instancia está en estado RUNNING antes de realizar la conexión SSH (no más de 2-3 minutos), dado que es necesario que se inyecte la clave pública en la instancia; ii) estás especificando el fichero *alucloud\$ID-priv.pem* como parámetro al comando ssh, dado que ese fichero contiene la clave privada necesaria para identificar al usuario y autorizar la conexión vía SSH sin contraseña a la instancia; iii) el contenido del fichero *alucloud\$ID-priv.pem* contiene efectivamente una clave privada. Si lo editas verás que comienza con la línea -----BEGIN RSA PRIVATE KEY---- y termina con la línea -----END RSA PRIVATE KEY----- (asegúrate de que no te olvidas ninguno de los cinco guiones delanteros ni traseros tanto en la primera como en la última línea y de que no hay líneas en blanco entre medias de la clave privada, ni ningún carácter adicional) y iv) estás utilizando el nombre de cuenta apropiado para dicha AMI (en nuestro caso concreto es *bitnami*) en la conexión vía SSH.

Si por el contrario obtienes el mensaje de error “*Warning: Identity file alucloud\$ID-priv.pem not accessible: No such file or directory*”, es porque el comando ssh no puede encontrar el fichero de clave

privada que le estás indicando (mediante el parámetro *-i*). Para resolverlo, asegúrate de que: i) estás indicando la ruta correcta al fichero de clave privada; ii) estás indicando el nombre correcto de la clave privada y iii) estás situado en el directorio correcto para acceder a ese fichero con la ruta que has indicado). Si obtienes el mensaje de error “WARNING: UNPROTECTED PRIVATE KEY FILE”, es porque te olvidaste de cambiar los permisos al fichero alucloud\$ID-priv.pem mediante el comando *chmod*, tal y como está explicado en la sección anterior.

Si obtienes algún error al tratar de conectar por SSH de tipo “Connection timed out”, asegúrate de que la máquina lleve en estado running al menos un par de minutos, que estés utilizando la IP pública (en lugar de la IP privada) o el nombre DNS correcto de tu instancia y que el grupo de seguridad con el que desplegaste la instancia permita la conexión al puerto 22 desde la máquina de prácticas (asegúrate de que la IP indicada es correcta y que has puesto las reglas en la pestaña “Inbound”). Por último, aunque muy poco probable, es posible que haya ocurrido algún problema al desplegarla. Para ello, deberás proceder a terminar la instancia y desplegar una nueva. Si el problema persiste puedes tratar de forzar a desplegar en una zona de disponibilidad diferente (usando la AWS CLI). Recuerda que desde la AWS Management Console es posible ver si una instancia ha superado los tests de accesibilidad (*System Status Check*, que verifica que el hardware sobre el que se ejecuta la instancia funciona correctamente e *Instance Status Check*, que verifica que el sistema operativo de la instancia está recibiendo tráfico y, por tanto, se ejecuta correctamente).

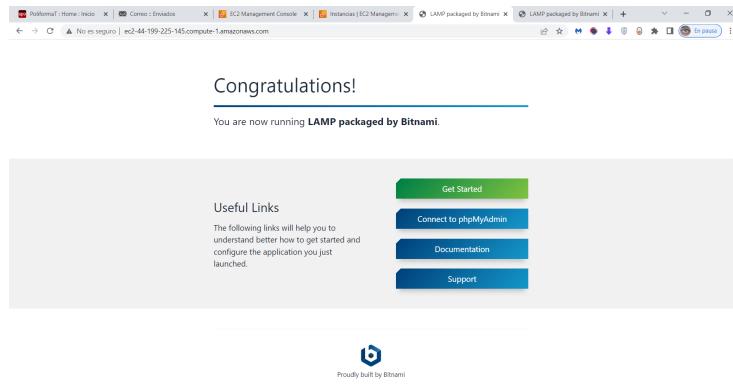
Una vez conectado a la instancia, es posible ver algunas características de la misma, como el estado del sistema de archivos, la versión del kernel de Linux o la clave pública correspondiente al par de claves con el que ha sido desplegada la instancia.

```
bitnami@ip-10-31-224-79:~$ df
Filesystem      1K-blocks    Used   Available  Use% Mounted on
udev              499296       0    499296   0% /dev
tmpfs             101440   3304     98136   4% /run
/dev/xvda1      10098468 3464732   6617352  35% /
tmpfs             507196       0    507196   0% /dev/shm
tmpfs               5120       0     5120   0% /run/lock
tmpfs             507196       0    507196   0% /sys/fs/cgroup
/dev/loop0          89088   89088        0  100% /snap/core/4917
/dev/loop1          12928   12928        0  100% /snap/amazon-ssm-agent/295
/dev/loop2          90624   90624        0  100% /snap/core/7270
/dev/loop3          18432   18432        0  100% /snap/amazon-ssm-agent/1335
tmpfs             101440       0   101440   0% /run/user/1000

bitnami@ip-10-31-224-79:~$ uname -a
Linux ip-172-31-13-212 4.4.0-1083-aws #93-Ubuntu SMP Wed May 8 16:08:41 UTC
2019 x86_64 x86_64 x86_64 GNU/Linux

bitnami@ip-10-31-224-79:~$ cat $HOME/.ssh/authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQQCQhJPBWKwpFWaTp2kAtnJSmFZWhpLeX6ewZy5S0ZkaOIu
C1WahjqHhNXsifyczHXh0RLe4/jkvTSTGPP1gLVESG6RZendhpmsog1UKI2GPemt9BFejy+hdO
e35M9Zd6Wv4AoWPtjhvP2IwuxDGu81xdf4yBCwlWC/nxWBEsAfsnfsguX1EcMRO0ULoLE6GeRKk
eP5saQnD8MEFTOyIAz1bPv9ORfOrC9975wMnEvABxY7jhfrnn3D72eb7yGYYAY+PmDXrSQmRr1I
+f1Nwr77N5wi+7KRJ8a49ijCU6npDj1kAsAVUoMSe3thBbWBkJbf3w8nFRiywkVgZSA8SIDfh
alucloud40-keypair
```

Para verificar que el servidor web está activo, es posible abrir un navegador y conectarse a la IP (o nombre DNS) que identifica la instancia. En nuestro caso (asegúrate de que el navegador no ha indicado ‘https’, pues suele hacerlo por defecto): <http://ec2-54-226-177-26.compute-1.amazonaws.com>

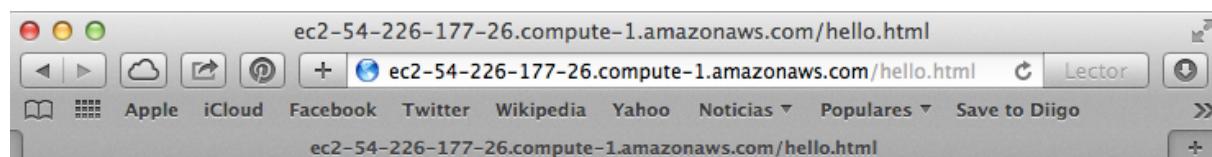


Si no recibes contestación del servidor web es posible que hayas olvidado desplegar la instancia de Amazon EC2 con un grupo de seguridad que permita el tráfico al puerto 80 (puerto en el que escucha el servidor web). En ese caso, deberás modificar el grupo de seguridad, de manera que todas las instancias lanzadas con dicho grupo de seguridad reflejarán automáticamente el cambio. La modificación del grupo de seguridad se puede hacer simplemente añadiendo una nueva regla a tu grupo de seguridad ya existente, para permitir la conexión al puerto 80. Revisa el apartado correspondiente a la creación de grupos de seguridad para asegurarte de que incluye las reglas apropiadas. Los cambios se aplicarán a todas las instancias de manera automática e instantánea. Asegúrate de estar usando el protocolo 'http' y no 'https'.

Podemos probar a realizar un cambio en la página web por defecto del servidor web de la instancia para verificar que se actualiza desde el navegador web. La localización de los ficheros que muestra el servidor web Apache cambia de una distribución a otra. Por ejemplo en Ubuntu suelen estar en /var/www/html. Sin embargo, en esta AMI dichos ficheros están en /opt/bitnami/apache2/htdocs.

```
bitnami@ip-10-31-224-79:~$  
echo "<h1> Hello from the Cloud </h1>" > /opt/bitnami/apache2/htdocs/hello.html
```

Al acceder a la URL <http://ec2-54-226-177-26.compute-1.amazonaws.com/hello.html> se verá el nuevo mensaje:



## Hello from the Cloud

Si experimentas algún problema en el arranque de una instancia en Amazon EC2 es posible obtener los mensajes que mostraría por pantalla dicha máquina durante el arranque. Para ello, es posible usar la

AWS Management Console (explicado más adelante), seleccionar una instancia y elegir la opción “Get System Log”. Tienes más información sobre como determinar qué problemas tiene una instancia que no consigue arrancar en [15].

Para salir de la sesión SSH con la instancia desplegada en Amazon EC2 y volver al *prompt* del entorno de realización de prácticas utiliza el comando exit:

```
bitnami@ip-10-31-224-79:~$ exit
```

### 5.3. Sobre las Características de las Instancias basadas en EBS

Estas instancias tienen carácter persistente ya que el despliegue de la instancia va ligado al despliegue de un volumen EBS que alojará el dispositivo raíz de la instancia [25]. Por ello, todos los cambios que se realicen en la instancia se verán reflejados al parar y volver a arrancar la instancia (a diferencia de lo que ocurre con una instancia basada en S3). Mientras una instancia basada en EBS está parada no genera gasto derivado de segundos de cómputo. Sin embargo, el volumen EBS asociado sí que lleva un coste asociado, incluso aunque la instancia esté parada. La terminación de la instancia basada en EBS provoca la destrucción del volumen EBS asociado.

Es posible obtener un listado de todos los volúmenes creados desde la opción “Volumes” de la AWS Management Console dentro del servicio EC2.

| Volúmenes (8)            |                  |                       |          |        |      |             |                 |                        |                   |  |
|--------------------------|------------------|-----------------------|----------|--------|------|-------------|-----------------|------------------------|-------------------|--|
|                          | Name             | ID de volumen         | Tipo     | Tamaño | IOPS | Rendimiento | Instantánea     | Creada                 | Zona de disponib. |  |
| <input type="checkbox"/> | lamba-vpc-nat... | vol-0bd2a9fe81b3fb87  | standard | 8 GiB  | -    | -           | snap-0b5e4e2... | 2020/11/09 13:56 GMT+1 | us-east-1b        |  |
| <input type="checkbox"/> | -                | vol-08579e21a70f1fa28 | gp2      | 20 GiB | 100  | -           | snap-066cd8...  | 2021/03/01 22:28 GMT+1 | us-east-1e        |  |
| <input type="checkbox"/> | -                | vol-0847b241b71a6bc3  | gp2      | 30 GiB | 100  | -           | snap-0a52a8f... | 2021/08/18 09:01 GMT+2 | us-east-1e        |  |
| <input type="checkbox"/> | -                | vol-09d49d49a0530945f | standard | 8 GiB  | -    | -           | snap-596eb6d... | 2017/03/24 11:58 GMT+1 | us-east-1a        |  |
| <input type="checkbox"/> | -                | vol-0da93662929362359 | gp2      | 20 GiB | 100  | -           | snap-017bd4a... | 2021/04/30 10:19 GMT+2 | us-east-1a        |  |
| <input type="checkbox"/> | -                | vol-0c6cc7ae999a79d5e | gp2      | 10 GiB | 100  | -           | snap-0b4e8fe... | 2021/05/18 12:57 GMT+2 | us-east-1a        |  |
| <input type="checkbox"/> | -                | vol-0cea52bbc63a52ad  | gp3      | 8 GiB  | 3000 | 125         | -               | 2022/09/08 09:16 GMT+2 | us-east-1a        |  |
| <input type="checkbox"/> | -                | vol-099219ac402c461c8 | gp2      | 10 GiB | 100  | -           | snap-0807d27... | 2022/09/08 09:16 GMT+2 | us-east-1a        |  |

El listado de volúmenes refleja que al crear una instancia a partir de una imagen basada en EBS se procede automáticamente a la creación de un volumen en EBS (en este caso de 10 GBytes) para alojar los datos de la instancia. La información obtenida indica que el volumen está conectado a la instancia en /dev/xvda.

The screenshot shows the AWS Management Console interface for managing volumes. At the top, there's a search bar and a 'Crear volumen' button. Below it is a table titled 'Volúmenes (8)' listing eight volumes. One volume is selected, showing its details in a modal window below.

**Volume Details:**

- ID de volumen: vol-099219ac402c461c8
- Estado: En uso
- Sin alarmas
- Instancia adjuntada: i-0b2c2c4f328a5f9e6 (alucloud40-linux): /dev/xvda (attached)
- Opciones: Aceptar

**Volume Details View:**

| Detalles                               | Comprobaciones de estado                           | Monitoreo                            | Etiquetas   |
|--|--|--------------------------------------|---|
| <b>Detalles</b>                        |  |                                      |   |
| ID de volumen<br>vol-099219ac402c461c8 | Tamaño<br>10 GiB                                   | Tipo<br>gp2                          | Estado del volumen<br>Aceptar   |
| Estado del volumen<br>En uso           | IOPS<br>100  | Rendimiento<br>-                     | Cifrado<br>No cifrado   |
| ID de clave de KMS<br>-                | Alias de clave de KMS<br>-                         | ARN de clave de KMS<br>-             | Instantánea<br>snap-0807d27b02bf4d9d1   |
| Zona de disponibilidad<br>us-east-1a   | Creada<br>Thu Sep 08 2022 09:16:45 GMT+0200 (CEST) | Asociación múltiple habilitada<br>No | Instancias adjuntadas<br>i-0b2c2c4f328a5f9e6 (alucloud40-linux): /dev/xvda (attached) |
| ARN de Outposts                        |  |                                      |   |

Para verificar que efectivamente los cambios realizados en la instancia se mantienen, aunque esta se detenga, aprovecharemos que ya hemos modificado algún fichero dentro de la instancia (la página web) y procederemos a detener la instancia. Para ello la seleccionamos y con el botón derecho elegimos “Stop instance”.

The screenshot shows the AWS EC2 Instances page. A single instance named "alucloud40" is listed, with its status set to "En ejecución" (Running). The instance type is "t3.micro". On the right side of the instance card, there is a context menu with options: "Detener instancia", "Iniciar instancia", "Reiniciar instancia", "Hibernar instancia", and "Terminar instancia". The "Detener instancia" option is highlighted.

La instancia parada no genera gasto adicional por despliegue de instancia, pero sí cuesta el volumen EBS que, obviamente, no ha sido destruido y de hecho sigue conectado a la instancia. Puedes aprovechar y modificar el tipo de instancia a t3.small para introducir así una operación de escalado vertical (paso de t3.micro a t3.small). El cambio del tipo de instancia puede ser interesante para disponer de mayor cantidad de memoria y de capacidad de cómputo, por ejemplo, si la instancia aloja un servidor de base de datos y se detecta que es necesario aumentar la memoria del sistema. Esto es posible hacerlo de forma sencilla en Amazon EC2 (si bien hay un pequeño *downtime* [24] mientras se detiene, se cambia el tipo de instancia y se vuelve a iniciar) de la siguiente manera.

This screenshot shows the same AWS EC2 Instances page as before, but the context menu has been expanded. The "Cambiar tipo de instancia" option is now highlighted. Other options visible in the menu include "Asociar al grupo de Auto Scaling", "Cambiar protección de terminación", "Cambiar la protección de detención", "Cambiar comportamiento de cierre", "Cambiar el comportamiento de recuperación automática", and "Monitoreo y solución de problemas".

Una vez que la instancia esté en estado “stopped”, selecciónala y con el botón derecho elige la opción “Acciones” → “Configuración de la instancia” → “Cambiar tipo de instancia”.

Fíjate que es igualmente posible pasar de un tipo de instancia de mayores prestaciones (t3.small) a una de menores prestaciones (t3.micro).

Asegúrate de elegir siempre los tipos de instancia indicados en este boletín (utiliza t3.small para esta prueba). De lo contrario, obtendrás un mensaje de error:

The screenshot shows a modal dialog titled "Start Instances". It asks if the user is sure they want to start the instances. Below the question, it lists the instance IDs: "i-0ebc5d91d591e4fe4". A red-bordered error box contains the following text:

```

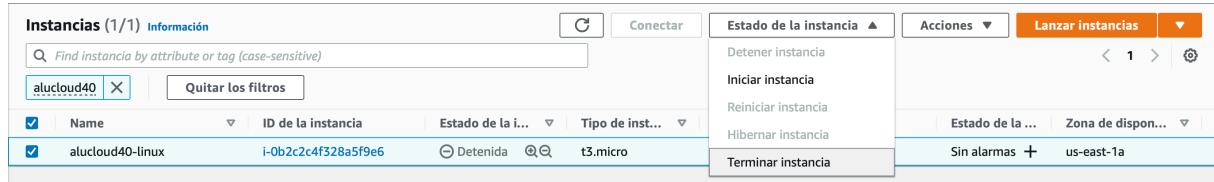
    ⓘ Error starting instances
    You are not authorized to perform this operation. Encoded authorization failure message:
    T7uyB9szgk9gnDFaWF_qUAJMzaAfx-hwBsYRIP6FkGh0pZjCYf51B7dWKWhZpEp_uQukuTvJRz_KBQ-
    T5iZPLA9s0xBwW2USoTt9BhTPVjy330mN-
    2BBiCCPqFVkdNwQoYg5c0mAU5uNgT76GJzc9o7zY0mcINfqsrPEo3EuHL85DNe3ykL5zbV14MjeP-NUt26KD82RiHwOwTO-
    3CmlTu9qmNtKYLuo5lwQq6j2m5_0xLBmxQcdrOnf3n2406whW-0rXXGhitKp1YQGLW9r3ymFDpqPw-vl-
    skXvRZE2005lyAtbyY0vSGG5_p_oTx48UrR6kyEBmnbIOu5APeGZ5RLvz5hW5iSWLQ2jUcnOq-
    RayU5f72GeP5VILAiSwfT1ZmgN80nDaQoKDS5hZMJDhsqN-
    UvJatjk28q3EyaTbn0_l5yuv_7hLuuglBoqDChsby61ygst0heApB9kY6vg84GW_wNOW32leVe5JD8Y6rz-
    7WOVhr51sMzhhmoybxKwWX1ZUrnRF0w77ivP256Q3dNT8uyCzCUP6rZJ510_Xg_B3d8LzOxIvQFzICQp6t1qxzE9dGIC4-
    PeUtsIMhmTsR22Tve4721nQrGzBaVPmSfPZOCoYBX3MmtK6z6pZZ2c
  
```

At the bottom of the dialog are two buttons: "Cancel" and "Yes, Start".

Iniciamos nuevamente la máquina y verificamos que el fichero de página web creado sigue existiendo en /opt/bitnami/apache2/htdocs/hello.html

Fíjate que, al detener y posteriormente iniciar la nueva instancia, la IP ha cambiado. En realidad, al detener la instancia se libera su dirección pública por lo que queda temporalmente sin dirección pública hasta que vuelva a ser iniciada, momento en el que recibe una nueva dirección pública y, por tanto, un nuevo nombre DNS público.

Terminamos la instancia seleccionándola y pulsando con el botón derecho para elegir la opción “Estado de la instancia” → “Terminar instancia”, tal y como se muestra a continuación.



Si consultamos a continuación el estado, se observa que está en estado *shutting-down* y finalmente pasa a estado *terminated*. En este momento se han liberado los recursos asociados y se deja de incurrir en gastos. Ten en cuenta que una instancia terminada no puede volver a ser iniciada. El volumen raíz desaparece y lo único que se conserva son los volúmenes EBS adicionales (no el raíz) que pudieran estar conectados a dicha instancia. La única opción posible de deshacer la terminación de una instancia es desplegar una nueva instancia a partir de la misma AMI.

¡Enhorabuena! Ya sabes cómo aprovisionar infraestructura de máquinas virtuales bajo demanda, de forma sencilla y mediante un modelo de pago por uso, sin necesidad de invertir en hardware y sin levantarte de la silla.

## 6. Despliegue de Instancias Basadas en Windows

En esta sección se describe cómo desplegar instancias Windows en Amazon EC2. La conexión a la instancia será mediante el protocolo de escritorio remoto (*Remote Desktop Protocol*, RDP). Para ello, será necesario desplegar una instancia de una AMI basada en Windows, utilizando un grupo de seguridad que permita la conexión al puerto usado por RDP (que es el 3389), y posteriormente conectarse a la AWS Management Console para obtener la contraseña necesaria para iniciar sesión en la instancia Windows vía el cliente RDP. A continuación, se detalla paso a paso las acciones necesarias utilizando la AWS Management Console.

### 6.1. Creación del Grupo de Seguridad y Selección de la AMI

Creamos un grupo de seguridad llamado gs-aws-\$ID-win que permita el tráfico dirigido al puerto 3389 de las instancias de Amazon EC2 que se desplieguen con dicho grupo de seguridad. A continuación, se muestra la regla que debes añadir **en la pestaña Inbound** y cómo se realiza desde la consola de administración:

| Type | Protocol | Port Range | Source                      |
|------|----------|------------|-----------------------------|
| RDP  | TCP      | 3389       | Anywhere- IPv4<br>0.0.0.0/0 |

#### 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  
gs-aws-48-win

El nombre no se puede editar después de su creación.

Descripción Información  
Permite el acceso SSH a los desarrolladores

VPC Información  
vpc-83a213fb (default)

**Reglas de entrada** Información

| Tipo | Protocolo | Intervalo de puertos | Descripción: opcional |
|------|-----------|----------------------|-----------------------|
| RDP  | TCP       | 3389                 | 0.0.0.0/0             |

**Agregar regla**

Pulsa el botón “Create” para confirmar la creación del grupo de seguridad y las reglas de acceso.

Recuerda que si quisieras soportar algún servicio específico en dicha instancia deberías habilitar los puertos requeridos por dichos servicios. Por ejemplo, el puerto 80 para el servidor web Internet Information Server (IIS), el puerto 1433 para acceder a MS SQL Server, etc.

A continuación, elegimos una AMI. Para ello nos dirigimos al AWS Marketplace desde la consola de EC2, pulsando sobre “Launch Instance” y eligiendo “AWS Marketplace”. Busca por “Windows Server” para obtener una AMI apropiada:

Elegir una Amazon Machine Image (AMI)

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Puede seleccionar una AMI proporcionada por AWS o nuestra comunidad de usuarios, o bien a través de AWS Marketplace.

**AMI de inicio rápido (20)** AMI de uso común

**Mis AMI (2)** Creadas por mí

**AMI de AWS Marketplace (747)** AWS y AMI de terceros de confianza

**AMI de la comunidad (500)** Publicadas por cualquiera

**Acotar los resultados**

**Borrar todos los filtros**

**Solo cara**

windows server (20 filtrados, 20 sin filtrar)

**Microsoft Windows Server 2022 Base**  
ami-0fb5befc1450ca205 (64 bits (x86))  
Microsoft Windows 2022 Datacenter edition. [English]

Apto para la capa gratuita Plataforma: windows Tipo de dispositivo raíz: ebs Virtualización: hvm Habilitado para ENA: Sí 64 bits (x86)  
Proveedor verificado

**Seleccionar**

Elegiremos la AMI de “Microsoft Windows Server 2022 Base”.

## 6.2. Despliegue, Datos de Acceso y Conexión a la Instancia

Desplegamos una instancia de dicha AMI con el grupo de seguridad creado en la fase anterior. Elegiremos como tipo de la instancia *t3.small* para que Windows tenga suficiente memoria para arrancar. Para ello, en los correspondientes paneles configura los siguientes valores:

|                   |   |
|-------------------|---|
| Nombre            | alucloudXX-windows (XX debe ser tu identificador de alumno) |
| Region            | Valor por defecto (us-east-1)                               |
| EC2 Instance Type | <b>t3.small</b>   |
| VPC Network       | vpc-83a213fb   default                                      |
| VPC Subnet        | (Cualquiera de ellas siempre que sea pública),              |
| Security Group    | Elige gs-aws-\$ID-win del desplegable                       |
| Key Pair          | alucloudXX-keypair.   |

Una vez establecida la configuración correcta, despliega la instancia:

EC2 > Instancias > Lanzar una instancia

**Correcto**  
Lanzamiento de la instancia iniciado correctamente (i-0988b34435e0a0988)

▶ Registro de lanzamiento

**Pasos siguientes**

**Obtener notificaciones de los cargos estimados**  
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier)

**How to connect to your instance**  
Your instance is launching and it might be a few minutes until it is in the running state, when it will be ready for you to use  
Haga clic en View Instances (Ver instancias) para monitorear el estado de la instancia. Cuando esta se encuentre en el estado de ejecución, usted podrá conectarse a ella desde la pantalla Instancias. Obtenga información sobre cómo conectarse a la instancia.

Vea más recursos para comenzar

**Ver todas las instancias**

Si pulsas sobre el identificador de la instancia te aparecerá la consola web de EC2. Anota la dirección IP pública de la instancia EC2:

The screenshot shows the AWS Management Console interface for managing instances. At the top, there's a search bar with the placeholder 'Find instancia by attribute or tag (case-sensitive)'. Below it, a filter bar has 'alucloud00-windows' selected. The main table lists one instance:

| Name               | ID de la instancia  | Estado de la i... | Tipo de inst... | Comprobación de estado | Estado de la ... | Zona de disponib... |
|--------------------|---------------------|-------------------|-----------------|------------------------|------------------|---------------------|
| alucloud00-windows | i-0119fdf149a3b5cff | En ejecución      | t3.small        | Initializando          | Sin alarmas      | us-east-1a          |

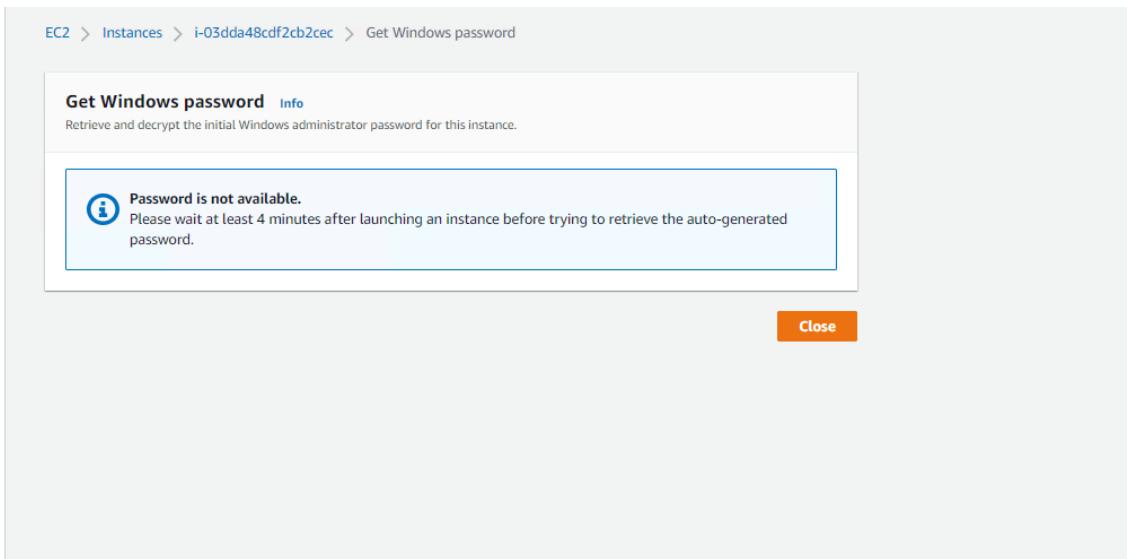
Below the table, a detailed view for the instance 'alucloud00-windows' is shown. It includes tabs for 'Detalles', 'Seguridad', 'Redes', 'Almacenamiento', 'Comprobaciones de estado', 'Monitoreo', and 'Etiquetas'. Under 'Resumen de instancia', it shows the instance ID, public IPv4 address (3.233.222.40), and private IP address (172.31.6.24).

Si realizas el despliegue pero no te aparece ninguna instancia nueva desplegada en la AWS Management Console asegúrate de que has elegido como tipo de instancia t3.small, ya que tipos de instancia superiores están restringidos por el instructor y fallará el despliegue de la instancia (es posible que no obtengas ningún mensaje de error).

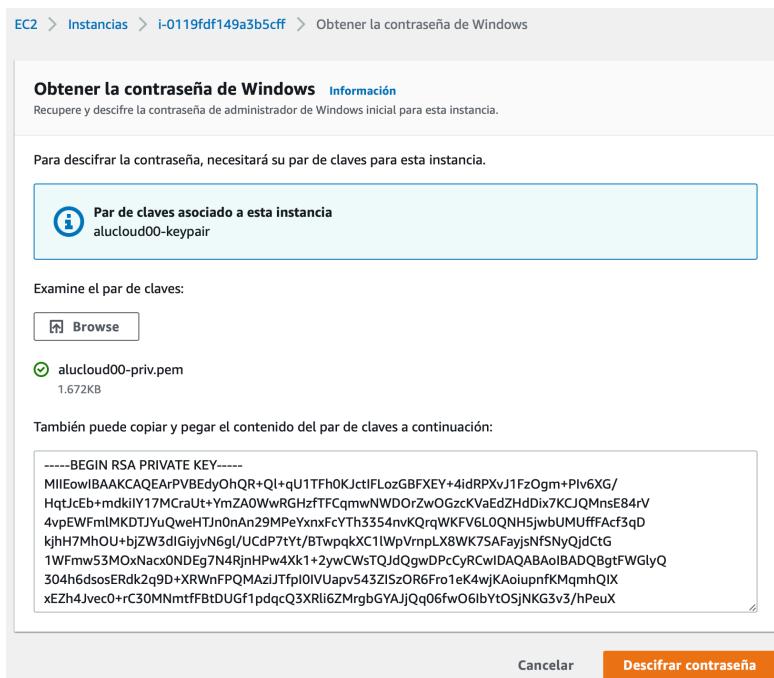
Antes de conectarte mediante escritorio remoto a la instancia hay que averiguar los datos de acceso (usuario y contraseña) a la instancia, por lo que deberemos acceder mediante la AWS Management Console para seleccionar la instancia y, con el botón derecho elegir la opción “Seguridad → Obtener la contraseña de Windows”.

The screenshot shows the same AWS Management Console interface as before, but with a context menu open over the instance 'alucloud00-windows'. The menu is titled 'Acciones' and includes options like 'Conectar', 'Ver detalles', 'Administrador el estado de la instancia', 'Configuración de la instancia', 'Redes', 'Seguridad' (which is highlighted in blue), 'Imagen y plantillas', and 'Monitoreo y solución de problemas'.

Es posible que tengas que esperar un tiempo desde que lanzas la instancia hasta que puedes obtener la contraseña, por lo que quizás obtengas un mensaje como el que se muestra en la siguiente figura. Se recomienda esperar al menos 4 minutos antes de obtener el password de la cuenta de Administrador para conectarse a la instancia por escritorio remoto, tal y como se muestra en el siguiente mensaje:



En el panel para obtener la contraseña de Windows necesaria para conectarte de forma remota a la instancia es necesario indicar la clave privada (disponible en el fichero alucloud\$ID-priv.pem) para descifrar dicha contraseña. Para ello puedes o bien elegir el fichero o copiar todo su contenido en el campo de texto, incluyendo las líneas de BEGIN RSA PRIVATE KEY y de END RSA PRIVATE KEY, tal y como se muestra en la siguiente figura:



Pulsa sobre el botón “Descifrar contraseña” (Decrypt Password). Si obtienes el siguiente mensaje de error “*There was an error decrypting your password. Please ensure that you have entered your private key correctly*” deberás asegurarte que: i) has indicado la clave privada asociada al par de claves con el que has desplegado la instancia previamente y que ii) estás indicando todo el contenido del fichero alucloud\$ID-priv.pem, incluyendo las líneas indicadas anteriormente.

Finalmente, obtendrás tanto la información del usuario (*Administrator – no lo confundas con Administrador* -) como la contraseña en un panel como el que se muestra a continuación:

**Obtener la contraseña de Windows** [Información](#)

Recupere y descifre la contraseña de administrador de Windows inicial para esta instancia.

**Se recomienda cambiar la contraseña**  
Le recomendamos que cambie la contraseña predeterminada. Nota: Si se cambia la contraseña predeterminada, no se podrá recuperar con esta herramienta. Es importante que cambie la contraseña por una que pueda recordar.

Puede utilizar la siguiente información para conectarse a su instancia de Windows mediante el Escritorio remoto.

Dirección IP privada  
 172.31.6.24

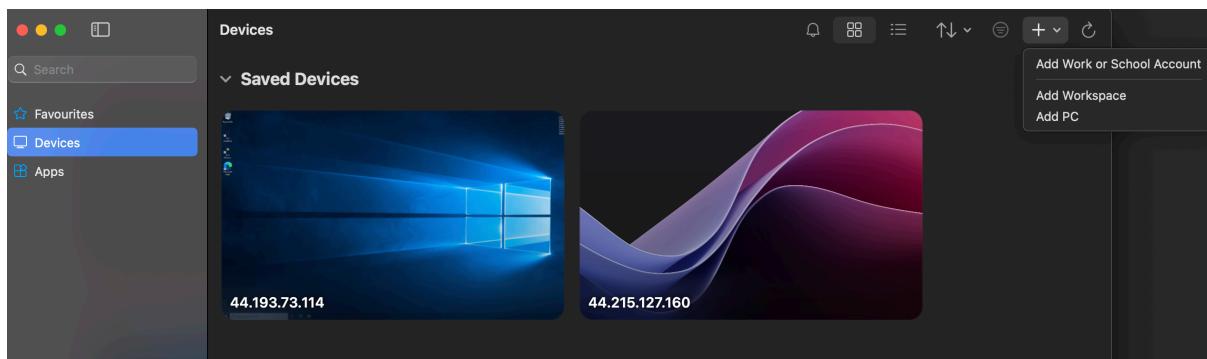
Nombre de usuario  
 Administrator

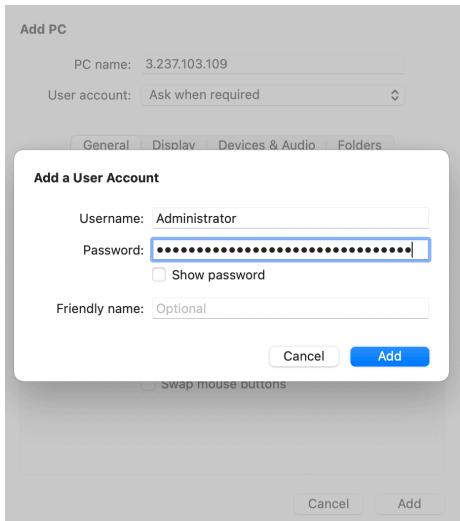
Contraseña  
 nI GEKG VbM7A;(15umbOdwDQALQ!RBV;2

**Cerrar**

Ten en cuenta que, aunque te muestre la IP privada, te hará falta la IP pública para conectarte.

Iniciamos sesión de escritorio remoto con un cliente RDP. Windows suele incluir un cliente RDP, también conocido como Terminal Services, por defecto (si estás usando Windows prueba a ejecutar el comando `mstsc` para saber si lo tienes instalado). Para macOS es posible utilizar *Windows App* **¡Error! No se encuentra el origen de la referencia.** y para GNU/Linux tienes disponibles herramientas como *Remmina*. En nuestro caso, utilizamos el cliente para macOS, especificando bien el nombre DNS o la IP pública de la instancia, así como el usuario (Administrator) y la contraseña de acceso (en *User account* puedes añadir esta información).





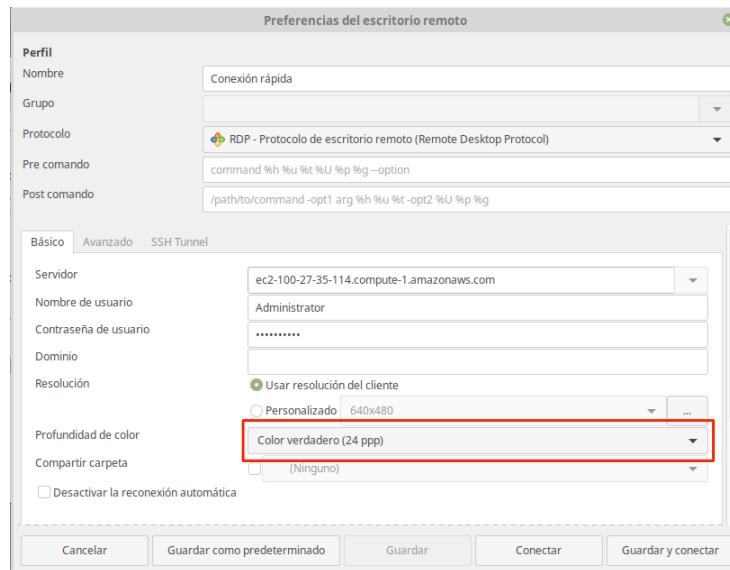
Tendrás que hacer doble click en el nuevo “PC” añadido. Se obtiene un mensaje de advertencia de que el nombre del servidor en el certificado no es correcto, pero elegimos conectarnos igualmente pulsando sobre Continuar.



Si obtienes un error indicando que las credenciales no son válidas asegúrate de haber indicado como usuario *Administrator* en lugar de *Administrador*.

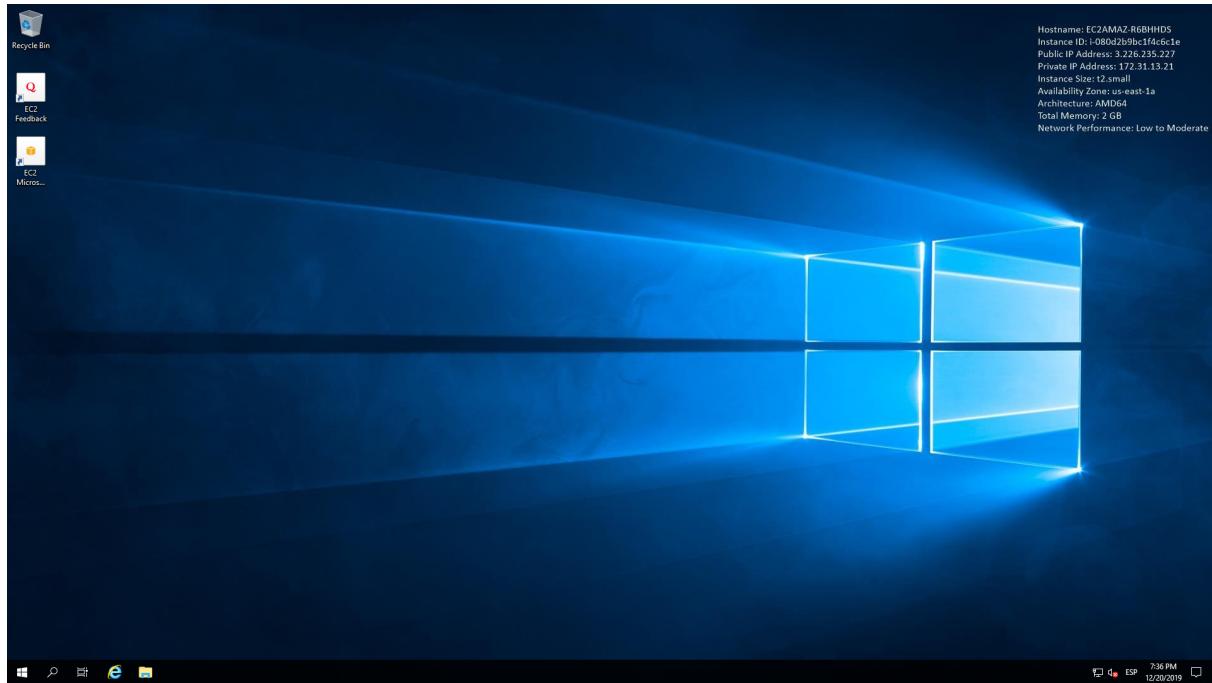
Una vez realizada la conexión, encontrarás un escritorio como el que se muestra en la Figura 2.

Si utilizas Remmina, tienes que tener en cuenta que deberás cambiar el ajuste de configuración de color por defecto a, por ejemplo, “Color verdadero (24 ppp)”, tal y como se muestra en la imagen:



Hay algunos aspectos a tener en cuenta. La instancia dispone de un disco de arranque (unidad C:) de 30 GB formateado como exFAT.

Ten en cuenta que es posible detener la instancia (al estar basada en un volumen EBS) sin que esto provoque la desaparición de los datos almacenados en C:. Una vez vuelta a iniciar la instancia detenida, será posible volver a conectarse mediante el cliente RDP (aunque la IP de la instancia cambia).



**Figura 2. Aspecto del escritorio de una instancia Windows desplegado en Amazon EC2.**

Ten en cuenta las siguientes consideraciones:

- Las instancias Windows están limitadas a dos conexiones remotas simultáneas [11], aunque es posible modificar el número de conexiones remotas concurrentes [12] [28].
- Si necesitas crear cuentas de usuario adicionales deberás utilizar las herramientas de administración de Windows para hacerlo.

En las siguientes prácticas estudiarás servicios adicionales para externalizar el almacenamiento de datos (mediante Amazon S3) y para reaccionar automáticamente ante aumentos en las cargas de trabajo de las instancias (mediante Auto Scaling).

Una vez finalizada las actividades, procede a terminar la instancia de Windows:

The screenshot shows the AWS Management Console interface for managing instances. It displays a single instance named "alucloud00-windows" which is currently running ("En ejecución"). The instance has an ID of "i-0119fdf149a3b5cff" and is of type "t3.small". The "Actions" menu is open, providing options such as stopping or starting the instance, restarting it, hibernating it, or terminating it. The instance is part of a group labeled "as" and is located in the "us-east-1a" availability zone.

Ten en cuenta que, cuando terminas una instancia, esta se mostrará durante un tiempo en la consola web en estado “terminated”, pero no es necesario que realices ninguna acción por tu parte. Eventualmente, desaparecerá.

¡Enhorabuena! Has completado todas las actividades de forma satisfactoria. Espero que te haya resultado interesante y útil.

## 7. Conclusiones

En esta práctica se han utilizado los servicios más relevantes de Amazon Web Services para conseguir el despliegue de infraestructuras virtuales bajo demanda en la forma de instancias. Has podido comprobar la ventaja de desplegar instancias de AMIs basadas en EBS. Has aprendido la creación de grupos de seguridad, pares de clave y la conexión remota a las instancias basadas en GNU/Linux mediante SSH. Esta práctica ha usado fundamentalmente la AWS Management Console. Si quieres conocer cómo se interacciona con Amazon EC2 desde la interfaz de línea de comandos (AWS CLI) tienes a tu disposición otra versión de esta misma práctica.

## Información Adicional

Esta práctica se realiza en el marco del “Curso Online de Cloud Computing con Amazon Web Services”, ofertado por el Instituto de Instrumentación para Imagen Molecular de la Universitat Politècnica de València. Tienes más información sobre este curso de formación en Cloud Computing en la siguiente dirección: <https://www.grycap.upv.es/cursocloudaws>

## Referencias

- [1] Jurg van Vliet, Flavia Paganelli. “Programming Amazon EC2”, O'Reilly, 2011.
- [2] Amazon Web Services (AWS). <http://aws.amazon.com/es/>
- [3] Amazon EC2 API Tools. <http://aws.amazon.com/developertools/351>
- [4] AWS Marketplace. <https://aws.amazon.com/marketplace>
- [5] Amazon Web Services Documentation. <http://aws.amazon.com/es/documentation/>
- [6] Aws: Simple Command-Line Access to Amazon EC2 and Amazon S3. <http://timkay.com/aws/>
- [7] cURL. <http://curl.haxx.se/>
- [8] <http://bitnami.org/stack/tomcatstack#cloudImage>
- [9] Windows App. <https://learn.microsoft.com/en-us/windows-app/overview>

- [10] rdesktop. <http://www.rdesktop.org>
- [11] Getting Started with Amazon EC2 Windows Instances.  
[http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/EC2Win\\_GetStarted.html](http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/EC2Win_GetStarted.html)
- [12] Configure the Number of Simultaneous Remote Connections Allowed for a Connection.  
<http://technet.microsoft.com/en-us/library/cc753380.aspx>
- [13] Amazon EC2 pricing. <http://aws.amazon.com/es/ec2/pricing>
- [14] Marvel Universal Social Graph. <http://aws.amazon.com/datasets/5621954952932508>
- [15] Troubleshooting instances. <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-troubleshoot.html>
- [16] LAMP. <http://es.wikipedia.org/wiki/LAMP>
- [17] Bitnami. <http://bitnami.com>
- [18] Interfaz de línea de comandos de AWS. <http://aws.amazon.com/es/cli/>
- [19] Amazon Machine Images (AMI).  
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>
- [20] Amazon Linux AMI. <http://aws.amazon.com/amazon-linux-ami/>
- [21] AWS Identity and Access Management (IAM). <http://aws.amazon.com/es/iam/>
- [22] Putty. <http://www.putty.org>
- [23] Paid AMI. <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/paid-amis.html>
- [24] Downtime. <http://en.wikipedia.org/wiki/Downtime>
- [25] Amazon EC2 Root Device Volume.  
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html>
- [26] ECDSA. <http://es.wikipedia.org/wiki/ECDSA>
- [27] Ataque Man-in-the-Middle. [http://es.wikipedia.org/wiki/Ataque\\_Man-in-the-middle](http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle)
- [28] How to Enable Multiple Concurrent User in Remote Desktop Windows 7.  
<http://www.nextofwindows.com/how-to-enable-multiple-concurrent-user-in-remote-desktop-windows-7/>
- [29] Linux AMI Virtualization Types.  
[http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/virtualization\\_types.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/virtualization_types.html)
- [30] They're Here – Longer EC2 Resource IDs Now Available.  
<https://aws.amazon.com/es/blogs/aws/theyre-here-longer-ec2-resource-ids-now-available/>
- [31] Monitoring Your Instances with CloudWatch.  
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch.html>
- [32] Using Your Own Linux Kernels.  
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/UserProvidedKernels.html>
- [33] Tagging Your Amazon EC2 Resources.  
[http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)
- [34] Health Check.  
[http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS\\_Concepts.html#healthcheck](http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html#healthcheck)
- [35] Amazon Virtual Private Cloud (VPC). <https://aws.amazon.com/es/vpc/>
- [36] How do I enable a password login instead of a key pair when logging into my EC2 instance using SSH? <https://aws.amazon.com/es/premiumsupport/knowledge-center/ec2-password-login/>

## ANEXO

Cuando te conectas por SSH a la instancia EC2 se te muestra la huella (*fingerprint*) de la clave ECDSA [26] del *host* (la instancia de EC2). Debes saber que cuando una instancia de EC2 arranca, se crean varias claves de host (una de tipo RSA, otra DSA y otra de tipo ECDSA) que permiten identificar la instancia. Al conectarste por SSH se te muestra la huella de la clave del host para que puedas verificar que efectivamente te estás conectando a dicha instancia y no a cualquier otra máquina que pueda estar efectuando algún ataque de tipo man-in-the-middle [27]. Puedes obtener la información sobre la clave del host desde la consola de administración de EC2, seleccionando la instancia y, con el botón derecho, eligiendo la opción “Instance Settings” → “Get System Log”. Verás que en un punto del log se indica cual es el fingerprint de dicha clave ECDSA recién creada, que debe coincidir con la que te indica el comando ssh. Durante las prácticas, no es necesario que realices este procedimiento, pero no está de más conocerlo.

```
Generating public/private ecdsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_ecdsa_key.
Your public key has been saved in /etc/ssh/ssh_host_ecdsa_key.pub.
The key fingerprint is:
cb:43:89:75:17:ad:99:bc:0b:7b:86:c7:fc:8d:15:e6 root@ip-10-158-72-71
The key's randomart image is:
+---[ECDSA 256]---+
|          .. |
|          .. |
| . . . . + |
| . S . . o |
| o . . . o .|
| + * . E. |
| .o B +    |
| + .o .    |
+-----+
```