

Trabajo SWAP 2018/2019



Miguel Ángel Mena Barrera

Benjamin Mannich

Índice

● Introducción	2
○ ¿Que es Amazon EC2?	
○ Características	
○ Conceptos básicos	
○ Redes y seguridad	
○ Almacenamiento	
● Tareas para prepararse para utilizar Amazon EC2	5
○ Inscripción en AWS	
○ Creación de un usuario de IAM	
○ Creación de un par de claves	
○ Crear una nube virtual privada (VPC)	
○ Creación de un grupo de seguridad	
● Introducción a las instancias Amazon EC2 de Linux	17
○ Información general	
○ Paso 1: Lanzamiento de una instancia	
○ Paso 2: Conexión a la instancia	
○ Paso 3: Eliminación instancia	
● Referencias	20

Introducción

1. ¿Qué es Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad informática en la nube segura y de tamaño modifiable. Está diseñado para simplificar el uso de la informática en la nube a escala web para los desarrolladores.

Amazon EC2 permite obtener y configurar capacidad Proporciona un control completo sobre los recursos informáticos. Amazon EC2 reduce el tiempo necesario para obtener e iniciar nuevas instancias de servidor en cuestión de minutos, lo que permite escalar rápidamente la capacidad, en función de las necesidades. Amazon EC2 cambia el modelo económico de la informática al permitir pagar solo por la capacidad que utiliza realmente. Amazon EC2 les brinda a los desarrolladores las herramientas necesarias para crear aplicaciones resistentes a errores y para aislarlas de los casos de error comunes.

2. Características

- **Escalable:** Podemos usar Auto-Scaling de Amazon EC2 para conservar la disponibilidad de su flota de EC2 y aumentar o disminuir automáticamente la escala de la flota en función de sus necesidades
- **Control:** Tiene control total de las instancias, incluido el acceso a raíz y la capacidad para interactuar con estas como lo haría con cualquier máquina.
- **Flexibilidad:** Tenemos la posibilidad de elegir entre varios tipos de instancia, sistemas operativos y paquetes de software. Amazon EC2 permite seleccionar una configuración de memoria, CPU y almacenamiento de la instancia

- **Fiável:** Amazon EC2 ofrece un entorno de elevada confianza en el que las instancias de sustitución se pueden encargarse con rapidez y anticipación.
- **Seguro:** Utilizando una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.
- **Económico:** Pagando una tarifa muy baja por la capacidad informática que realmente utilicemos

3. Conceptos básicos

- **AMI:** imagen de máquina de Amazon es una plantilla que contiene una configuración. Desde una AMI, se lanza una instancia que es una copia de la AMI que se ejecuta como un servidor virtual en la nube.
- **Instancia:** Básicamente, un tipo de instancia determina el hardware del equipo host utilizado para la instancia. Cada tipo de instancia ofrece diferentes capacidades de memoria y computación
- **Etiquetas:** Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras.

4. Redes y seguridad

- Amazon proporciona varios servicios dedicados a la seguridad y privacidad. Entre ellos se incluyen: *Firewalls*, *Cifrado con TLS*, *Tráfico cifrado entre todas las redes de AWS*.
- Control de ataques de denegación de servicio: Los métodos de detección de ataques, actúan de manera automática, previniendo así la caída del servicio, la falta de disponibilidad y reducción de dicho impacto.

- Amazon ofrece herramientas de evaluación de seguridad, **Amazon Inspector**, mediante el cual se evalúa la seguridad de las configuraciones y uso que le damos a sus máquinas.
- Control de acceso controlado mediante cuentas de usuario individuales con distintos permisos.

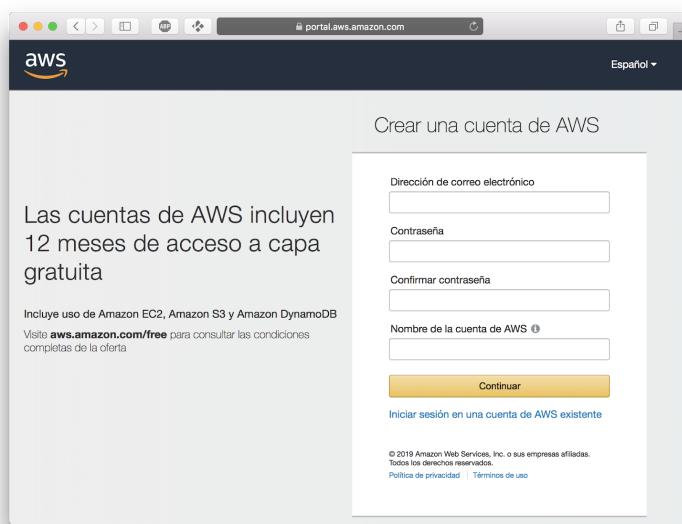
5. Almacenamiento

Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento de nivel de bloque para su uso con instancias de EC2. Los volúmenes de EBS son volúmenes de almacén de instancias de alta fiabilidad y disponibilidad que se pueden adjuntar a cualquier instancia en ejecución que esté en la misma zona de disponibilidad. Los volúmenes EBS que se adjuntan a una instancia de EC2 se exponen como volúmenes de almacenamiento que persisten de forma independientemente de la duración de la instancia. Al igual que con Amazon EC2 con Amazon EBS se paga únicamente por lo que se utiliza. No entraremos más en detalle de Amazon EBS ya que este trabajo se centrará únicamente en Amazon EC2.

Tareas para prepararse para utilizar Amazon EC2

1. Inscripción en AWS

Este proceso es muy simple ya que únicamente tendremos que ir a la página de AWS (<https://aws.amazon.com/>) y, a continuación, elegir la opción de “Create an AWS Account”.



Una vez allí seguimos las instrucciones en línea.

2. Creación de un usuario de IAM

Aunque puede crear claves para tener acceso a AWS, AWS no recomienda esta configuración ya que ellos mismo ofrecen un proceso de autenticación mucho más seguro, AWS Identity and Access Management (IAM).

De esta forma debe de agregar su usuario creado a un grupo de IAM concediendo sus permisos administrativos. El acceso a AWS se hace a través de una dirección URL y su usuario de IAM. Al estar inscrito a AWS sin un usuario de IAM puede obtenerlo creándolo en la consola de IAM.

Para crear un usuario de IAM y agregarlo al grupo de administradores se debe de seguir lo siguiente:

1. Inicie sesión en AWS, en la consola de IAM, con su correo electrónico y contraseña dados para su cuenta.

The screenshot shows the AWS IAM console's welcome screen. On the left, there's a sidebar with options like Panel, Grupos, Usuarios, Roles, Políticas, Proveedores de identidad, Configuración de cuenta, Informe de credenciales, and Claves de cifrado. The 'Usuarios' option is selected. The main area displays a welcome message: 'Le damos la bienvenida a Identity and Access Management (IAM)'. It shows statistics: Usuarios: 0, Roles: 2, Grupos: 0, and Proveedores de identidad: 0. Below this is a section titled 'Estado de seguridad' with five items, each with a checkmark or warning icon: 'Eliminar las claves de acceso raíz', 'Activar MFA en la cuenta raíz', 'Crear usuarios de IAM individuales', 'Utilizar grupos para asignar permisos', and 'Aplicar una política de contraseñas de IAM'. To the right, there's a 'Aspectos destacados de las características' section with a video thumbnail titled 'Introduction to AWS IAM' and a 'Información adicional' section with links to IAM best practices, documentation, and other resources.

2. Elija “usuarios” seguido por “Añadir usuario”

The screenshot shows the 'Users' page in the AWS IAM console. The 'Panel' sidebar is visible on the left. The main area has two buttons at the top: 'Añadir usuario(s)' (highlighted with a red circle) and 'Eliminar al usuario'. Below these buttons is a search bar and a table header with columns: 'Nombre de usuario', 'Grupos', 'Antigüedad de la clave de acceso', 'Antigüedad de la contraseña', 'Última actividad', and 'MFA'. A note at the bottom of the table says 'No hay usuarios de IAM. [Más información](#)'. The 'Añadir usuario(s)' button is circled in red.

3. En nombre de usuario escriba Administrator, active la casilla de “Acceso a la consola de administración de AWS, seleccione contraseña personalizada y active la casilla de restablecimiento de contraseña.

The screenshot shows the 'Add user' form on the AWS IAM console. In the 'User name' field, 'Administrator' is entered. Under 'Select AWS access type', the 'Access to the AWS Management Console' checkbox is selected. Below it, under 'Console password', 'Custom password' is chosen, and a password 'Passw0rd' is typed. The 'Require password reset at next login' checkbox is checked. At the bottom, there are 'Cancel' and 'Next Step: Permissions' buttons.

4. Seleccione “Siguiente: Permisos”, y diríjase a la sección de “Establecer permisos->Añadir usuario al grupo”

The screenshot shows the 'Add user' wizard Step 2: Set permissions. The 'Add user to group' button is highlighted. A note says 'You have not created any groups. Using groups is a recommended best practice for managing user permissions by working with work groups, access to AWS services or custom permissions.' There is also a 'Create a group' button. At the bottom, there are 'Cancel', 'Previous', and 'Next Step: Tags' buttons.

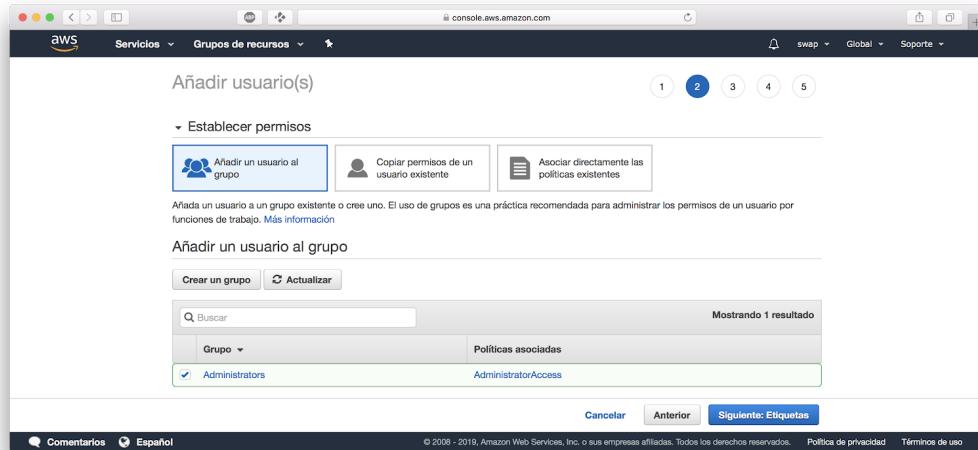
5. Cree un nuevo grupo, con *Administrators* de nombre, y filtre políticas por “Administrado por AWS: función de trabajo”

Nombre de la política	Tipo	Utilizado como	Descripción
Administrado por el cliente (0)	Función de trabajo	Ninguna	Provides full access to AWS services and resources.
Administrado por AWS (428)	Función de trabajo	Ninguna	Grants permissions for billing and cost management. This includes ...
Administrado por AWS: función de trabajo (10)	Función de trabajo	Ninguna	Grants full access permissions to AWS services and actions requir...
Se utilizó para los permisos (0)	Función de trabajo	Ninguna	Grants permissions to AWS data analytics services.
Utilizado como límite (0)	Función de trabajo	Ninguna	Grants full access permissions to AWS services and actions requir...
Se utilizó para los permisos (0)	Función de trabajo	Ninguna	Provides full access to AWS services and resources, but does not ...
Utilizado como límite (0)	Función de trabajo	Ninguna	The security audit template grants access to read security configur...

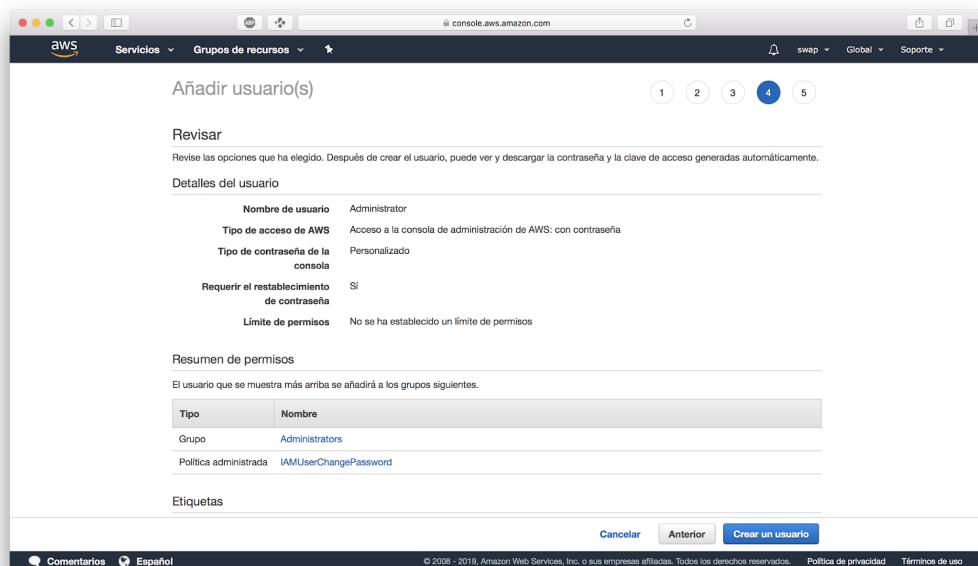
6. Activar la casilla de verificación *AdministratorAccess* seguido por Crear un grupo.

Nombre de la política	Tipo	Utilizado como	Descripción
AdministratorAccess	Función de trabajo	Ninguna	Provides full access to AWS services and resources.
Billing	Función de trabajo	Ninguna	Grants permissions for billing and cost management. This includes ...
DatabaseAdministrator	Función de trabajo	Ninguna	Grants full access permissions to AWS services and actions requir...
DataScientist	Función de trabajo	Ninguna	Grants permissions to AWS data analytics services.
NetworkAdministrator	Función de trabajo	Ninguna	Grants full access permissions to AWS services and actions requir...
PowerUserAccess	Función de trabajo	Ninguna	Provides full access to AWS services and resources, but does not ...
SecurityAudit	Función de trabajo	Ninguna	The security audit template grants access to read security configur...

7. Active el nuevo grupo en la lista de grupos y continúe en “Siguiente: Etiquetas” (En esta sección no cambiaremos nada).



8. Finalmente elija “Siguiente: Revisar” para ver la lista de suscripciones a grupos para el nuevo usuario. Una vez listo para continuar seleccione *Create user*.

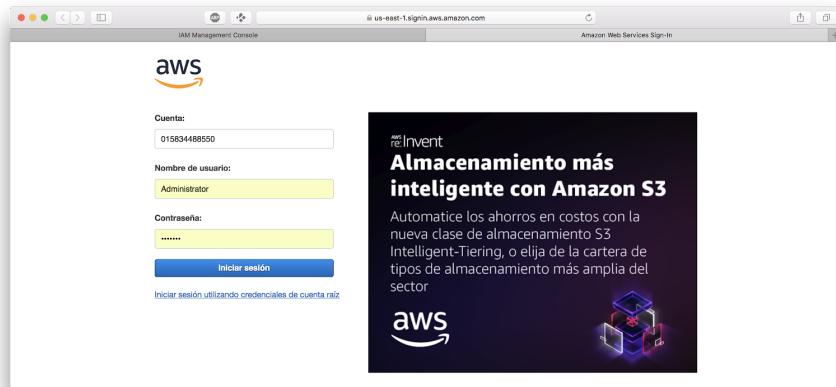


Este proceso sirve para crear más grupos y usuarios, así como para otorgar el acceso a otros usuarios para los recursos de su cuenta AWS.

Para iniciar sesión como usuario IAM introduzca la siguiente dirección URL en su navegador:

`https://id_aws.signin.aws.amazon.com/console/`

Siendo ***id_aws*** el número de cuenta de AWS sin guiones. A continuación le pedirá su usuario AIM y su contraseña.



También existe la posibilidad de sustituir el ***id_aws*** en la dirección URL por un alias definido por el usuario.

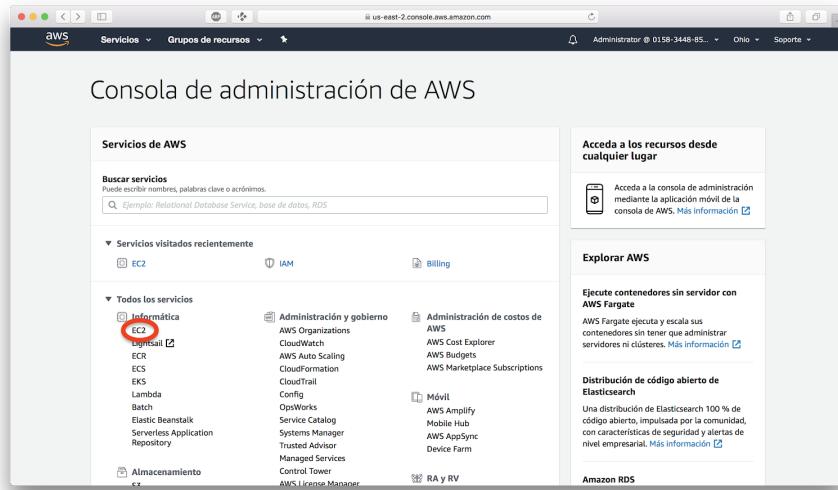
3. Creación de un par de claves

AWS protege la información de acceso de la instancia a través de criptografía de clave pública. Primero deberá de especificar el nombre del par de claves cuando se lanza la instancia y después proporcionar la clave privada al iniciar sesión con SSH.

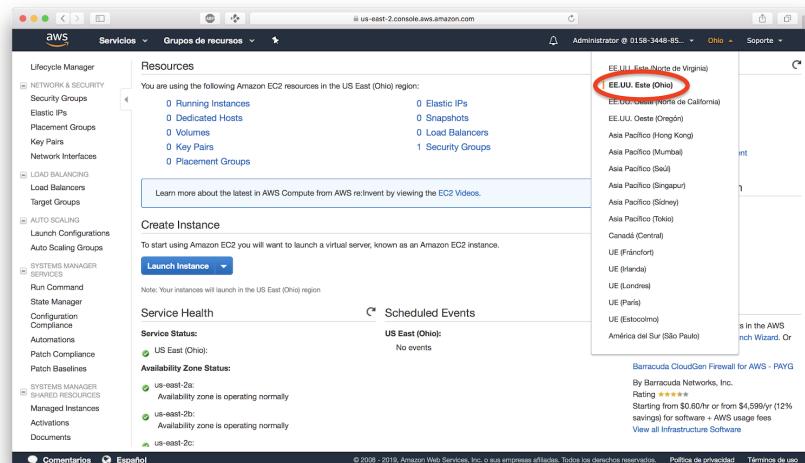
Se puede crear un par de claves con la consola de Amazon EC2. Se deberá crear un par de claves por cada región a la que se quiere lanzar instancias.

Pasos para crear un par de claves:

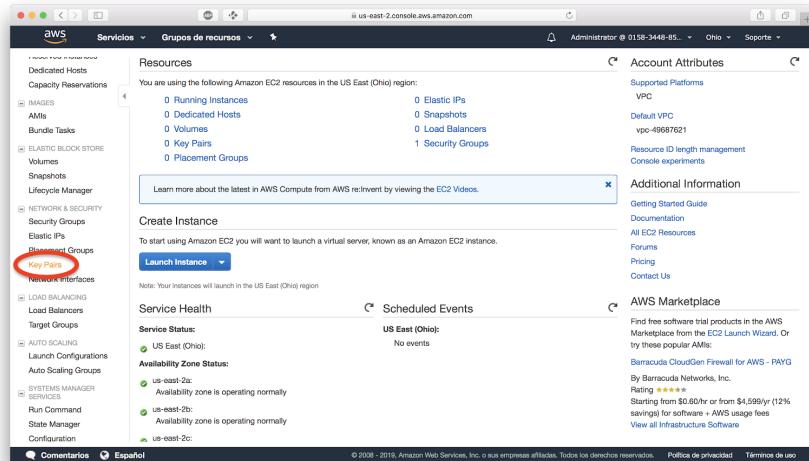
1. Inicie sesión en AWS con su URL de la sección previa, y en el panel AWS elija EC2 para abrir la consola de Amazon EC2.



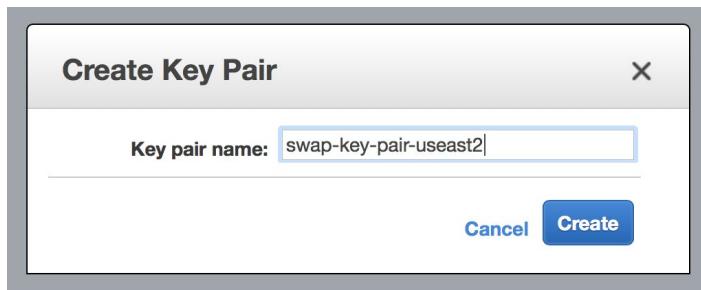
2. En la barra de navegación puede seleccionar cualquier región disponible, no importa la ubicación en la que se encuentre. Únicamente debe de tener en cuenta que los pares de claves son específicos de una región. En nuestro caso seleccionaremos la opción por defecto “EE.UU. Este (Ohio)”.



3. Seleccione “Key Pairs” en el panel de navegación en “Network and Security” y elija “Create Key Pairs”.



4. En el campo Key pair name escriba un nombre para el nuevo par de claves. A continuación seleccione Create.



5. El navegador descargará el archivo de clave privada en donde el nombre del archivo base es el que seleccionó como nombre del par de claves con la extensión .pem.
6. Cliente SSH en equipo Mac o Linux utilice el comando para establecer los permisos de su archivo.

```
chmod 400 your_user_name-key-pair-region_name.pem
```

Conexión a la instancia mediante el par de claves

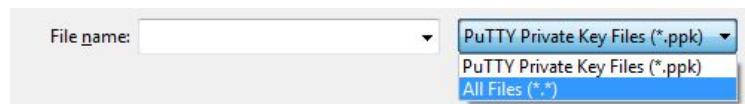
Si se encuentra utilizando un equipo Mac o Linux y desea conectarse a la instancia de Linux se le especificará el archivo .pem a su cliente SSH con la opción -i y la ruta a su clave privada. Desde un equipo Windows deberá utilizar MindTerm o PuTTY.

Conexión a una instancia de Linux desde Windows mediante PuTTY.

1. Descargar e instalar PuTTY encontrados en el siguiente link:
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
2. Inicie PuTTYgen
3. Elija RSA cuando le pidan Type of key to generate (Tipo de clave a generar).



4. Cargue de forma predeterminada, PuTTYgen muestra los archivos con extensión .ppk y para localizar el archivo .pem debe seleccionar la opción mostrar todos los tipos de archivo.



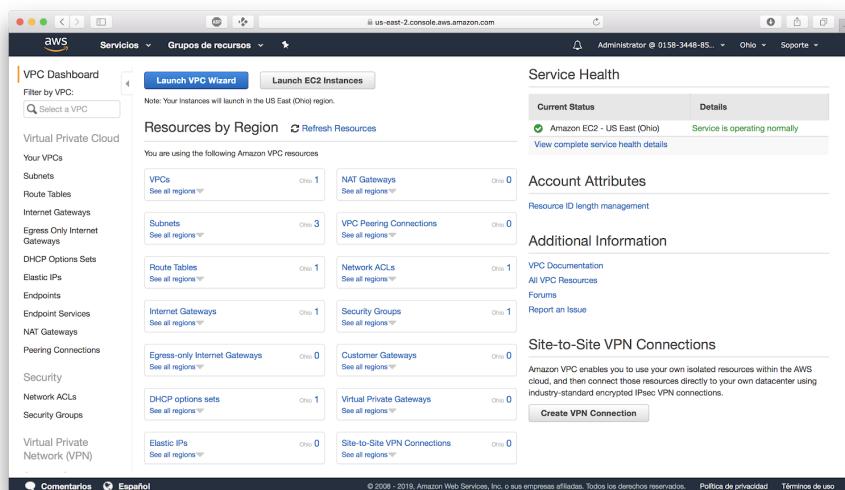
5. Abra el archivo de clave privada que creó en el procedimiento anterior y acepte.
6. Guarde clave privada en Save private key. Elija Yes cuando se muestre una advertencia sobre guardar la clave sin contraseña.
7. Utilice el mismo nombre de clave que utilizó para el par de claves, se añadirá automáticamente la extensión de archivo .ppk

4. Crear una nube virtual privada (VPC)

Amazon VPC le permite lanzar recursos de AWS en la red virtual que ha definido, lo que se conoce como una *nube virtual privada* (VPC).

En caso de no tener una VPC predeterminada en el panel (“Account Attributes->Default VPC”), puede crear una VPC no predeterminada siguiendo los pasos que se indican a continuación:

1. Abra la consola [Amazon VPC](#) y en la barra de navegación seleccione la región que escogió previamente.



2. Seleccione “Launch VPC Wizard”.
3. En la página “Step 1: Select a VPC Configuration” simplemente presione “Select”.
4. En la página “Step 2: VPC with a Single Public Subnet”, escriba un nombre fácil de recordar para la VPC, y deje los valores predeterminados en las demás opciones de configuración. Finalmente presione “Create VPC”.

The screenshot shows the "Step 2: VPC with a Single Public Subnet" configuration page. It has fields for IPv4 CIDR block (10.0.0.0/16), IPv6 CIDR block (selected as "No IPv6 CIDR Block"), VPC name (swap-cloud), Public subnet's IPv4 CIDR (10.0.0.0/24), Availability Zone (No Preference), Subnet name (Public subnet), Service endpoints (Add Endpoint), Enable DNS hostnames (Yes selected), and Hardware tenancy (Default). At the bottom are "Cancel and Exit", "Back", and "Create VPC" buttons.

5. Creación de un grupo de seguridad

Los grupos de seguridad, mediante reglas actúan como firewall para las instancias asociadas al controlar el tráfico entrante y saliente en el ámbito de la instancia.

Una de las reglas necesarias es la de conectarse a la instancia desde su dirección IP mediante SSH. También se pueden añadir reglas que permitan HTTP de entrada y salida y acceso HTTPS desde cualquier lugar.

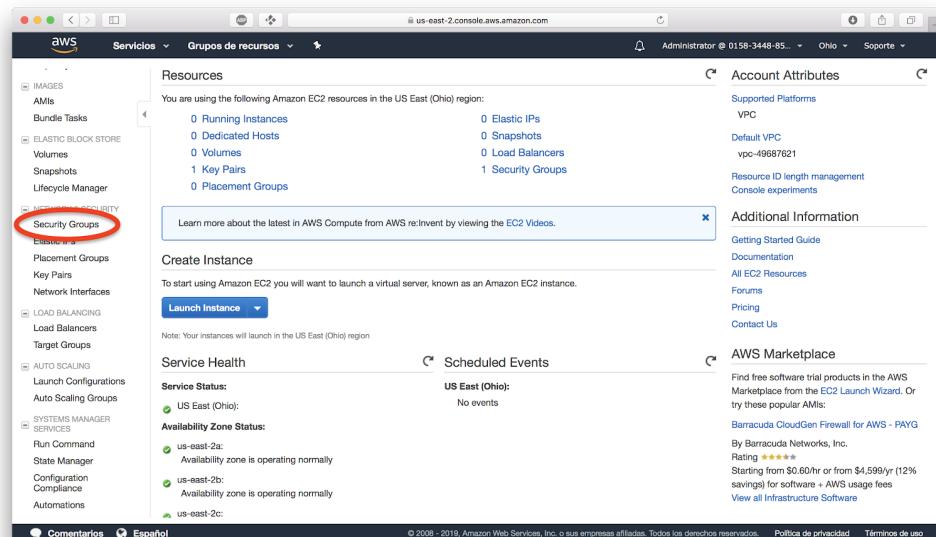
Al igual que siempre, los grupos de seguridad dependen de la región en la que estamos trabajando.

Requisitos previos

- Dirección IPv4 pública de su equipo local.
- Rango de direcciones IP utilizadas por los equipos cliente. (Si se conecta a través de un ISP o protegido por un firewall sin una dirección IP estática)

Para crear un grupo de seguridad con los privilegios mínimos

1. Abra la consola de Amazon EC2 y seleccione la región elegida anteriormente para el grupo de seguridad. Una vez ahí elija “Security Groups”.



2. Elija “Create Security Group” y escriba un nombre y una descripción para el nuevo grupo de seguridad. En la lista “VPC”, seleccione la VPC predeterminada. Y por último, en la pestaña “Inbound”, cree las reglas que se muestran en la captura de pantalla:

Create Security Group

Security group name	swap_SG_uswest2
Description	Grupo de seguridad principal para nuestras instancias
VPC	vpc-49687621 (default)

Security group rules:

Inbound Outbound

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	Anywhere	0.0.0.0/0, ::/0
HTTPS	TCP	443	Anywhere	0.0.0.0/0, ::/0
SSH	TCP	22	My IP	189.216.131.132/32

Add Rule

Cancel Create

Group ID: sg-06097459 VPC ID: vpc-49687621

Introducción a las instancias Amazon EC2 de Linux

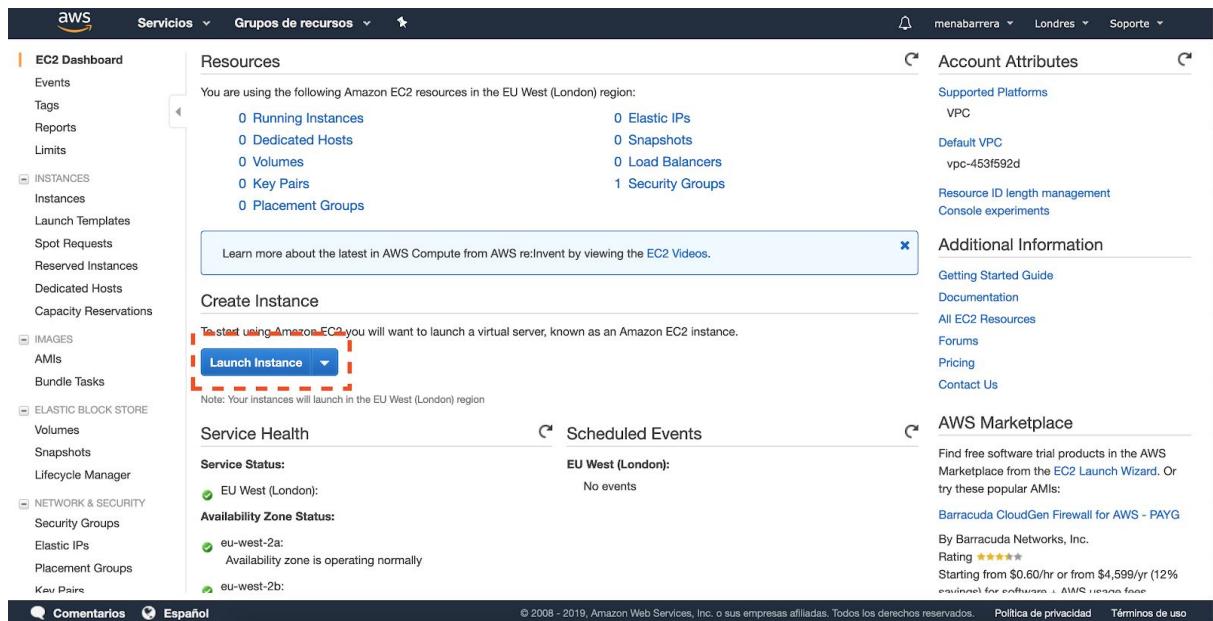
1. Información general

Comencemos a utilizar Amazon Elastic Compute Cloud (Amazon EC2) mediante el lanzamiento, la conexión y el uso de una instancia de Linux. Una instancia es un servidor virtual en la nube de AWS. Con Amazon EC2, puede instalar y configurar el sistema operativo y las aplicaciones que se ejecutan en la instancia.

Al lanzar la instancia, la protege especificando con un par de claves y un grupo de seguridad. Al conectarse a la instancia, debe especificar la clave privada del par de claves que especificó cuando lanzó la instancia.

2. Paso 1: Lanzamiento de una instancia

Para el lanzamiento de la instancia tenemos que seguir los siguientes pasos:



Step 1: Choose an Amazon Machine Image (AMI)

	AMI Name	Description	Select
<input type="checkbox"/>	Amazon Linux	The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.	<input type="button" value="Select"/>
<input type="checkbox"/>	Red Hat Enterprise Linux 7.5 (HVM), SSD Volume Type	Red Hat Enterprise Linux version 7.5 (HVM), EBS General Purpose (SSD) Volume Type	<input type="button" value="Select"/>
<input type="checkbox"/>	SUSE Linux Enterprise Server 15 (HVM), SSD Volume Type	SUSE Linux Enterprise Server 15 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	<input type="button" value="Select"/>
<input type="checkbox"/>	Ubuntu Server 18.04 LTS (HVM), SSD Volume Type	Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).	<input type="button" value="Select"/>

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)								
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Up to 5 Giabit	Yes

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-07dc734dc14746eab

Free tier eligible Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root Device type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

3. Paso 2: Conexión a la instancia

Para la conexión a la instancia una vez que está funcionando es tan simple como abrir un terminal y con la clave que descargamos y ejecutar `ssh -i clave.pem user@dns_amazon`

```
[MacBook-Pro-de-Miguel:~ mena$ ssh -i /Users/mena/Downloads/amazon.pem ubuntu@ec2-3-9-10-85.eu-west-2.compute.amazonaws.com
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-1032-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information as of Sun May  5 13:14:25 UTC 2019

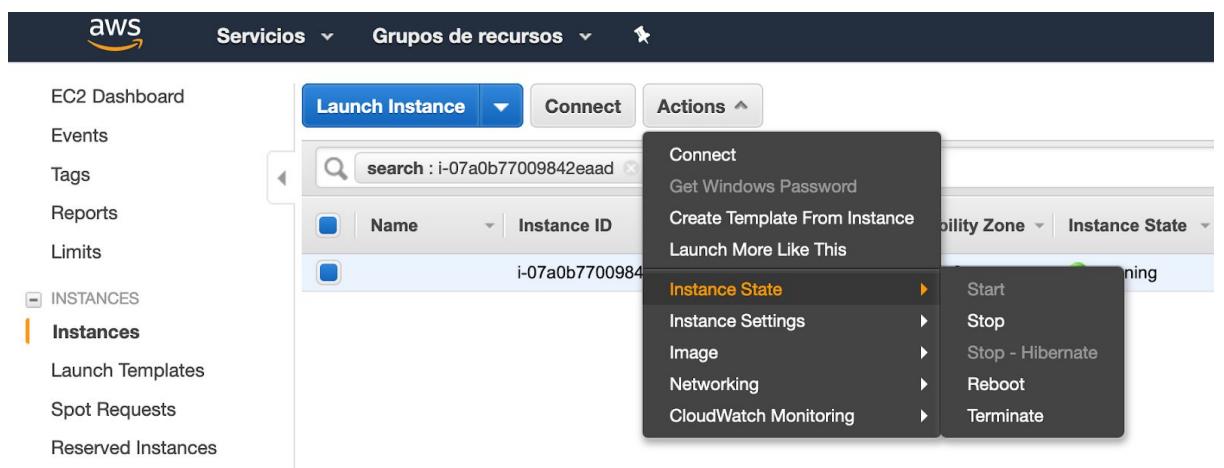
 System load:  0.02           Processes:          83
 Usage of /:   13.6% of 7.69GB  Users logged in:    0
 Memory usage: 14%            IP address for eth0: 172.31.28.32
 Swap usage:   0%

 Get cloud support with Ubuntu Advantage Cloud Guest:
 http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.
```

4. Paso 3: Eliminación instancia

En el panel de navegación, seleccione Instances (Instancias). En la lista de instancias, seleccione la instancia. Elija Actions (Acciones), Instance State (Estado de la instancia), Terminate (Terminar). Elija Yes, Terminate (Sí, terminar) cuando se le pida confirmación.



Referencias

- AWS (2019) *Configuración con Amazon EC2*. Link:
https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html
- AWS (2019) *Introducción a las instancias Amazon EC2 de Linux*. Link:
https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/EC2_GetStarted.html
- AWS (2019) *¿Qué es Amazon EC2?*. Link:
https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html
- AWS (2019) *Configuración con Amazon EC2*. Link:
https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html#create-an-iam-user