
Computación na nube

Big Data Aplicado

26/11/23 - IES Fernando Wirtz

Rafael Chamorro Maceiras

Fecha	Motivo del cambio
	Versión inicial

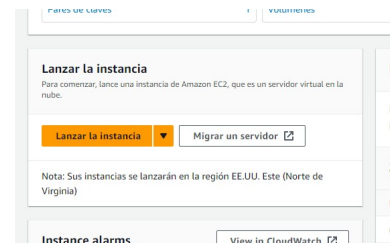
Índice

Crear una instancia de EC2.....2

Crear un bucket S3.....8

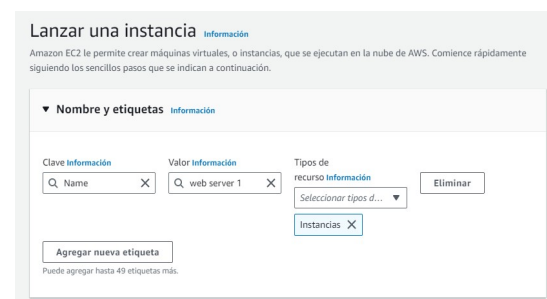
Crear una instancia de EC2

En el panel de control seleccionaremos los servicios de computación EC2 y lanzamos la instancia:

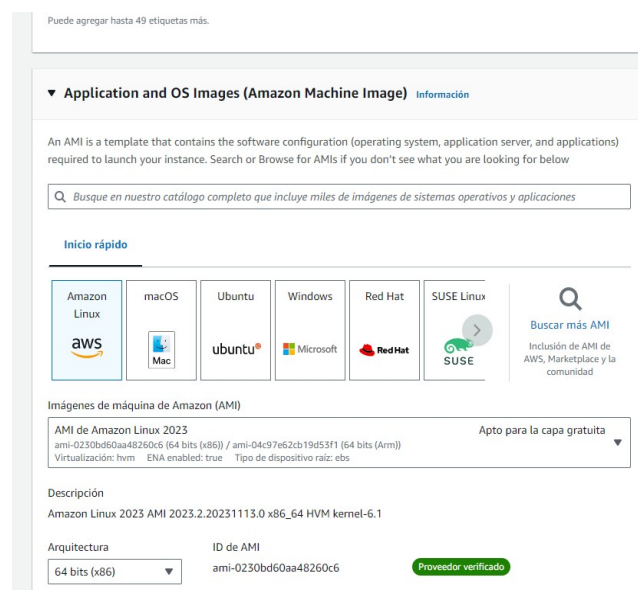


Pondremos un nombre:

Añadiendo etiquetas identificaríamos recursos en el caso de tener varios del mismo tipo



A continuación seleccionamos una AMI (imagen de máquina de Amazon) para nuestra instancia. Por defecto Amazon Linux



Seleccionaremos los recursos de hardware:

En este caso una vCPU y un GiB

▼ Tipo de instancia [Información](#)

Tipo de instancia

t2.micro

Apto para la capa gratuita

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true

Bajo demanda Windows base precios: 0.0162 USD por hora

Bajo demanda SUSE base precios: 0.0116 USD por hora

Bajo demanda RHEL base precios: 0.0716 USD por hora

Bajo demanda Linux base precios: 0.0116 USD por hora

Se aplican costos adicionales a las AMI con software preinstalado


Para conectarnos vía SSH una vez iniciada la instancia crearemos un par de claves. Para el ejemplo utilizamos la opción 'vockey' que ya nos ofrecen.

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

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

Nombre del par de claves - obligatorio

vockey

 [Crear un nuevo par de claves](#)

En el siguiente paso configuraremos la red. Podemos crear varias redes, por ejemplo la de desarrollo y la de producción.

▼ Configuraciones de red [Información](#)

VPC - obligatorio [Información](#)

vpc-00a231973cd76016c
172.31.0.0/16

(predeterminado)

Subred [Información](#)

Sin preferencias

Asignar automáticamente la IP pública [Información](#)

Habilitar

Para el ejemplo asignaremos automáticamente la IP pública

En el Firewall crearemos un grupo de seguridad

Firewall (grupos de seguridad) [Información](#)

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☒ Crear grupo de seguridad

☐ Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad - *obligatorio*

Web Server

Este grupo de seguridad se agregará a todas las interfaces de red. El nombre no se puede editar después de crear el grupo de seguridad. La longitud máxima es de 255 caracteres. Caracteres válidos: a-z, A-Z, 0-9, espacios y ._-:/()#,@[]+=&{}!\$*

Descripción - *obligatorio* [Información](#)

Security group for my web server

Reglas de grupos de seguridad de entrada

No security group rules are currently included in this template. Add a new rule to include it in the launch template.

Agregar regla del grupo de seguridad

Para el almacenamiento utilizaremos el que trae por defecto 8 GiB en una unidad de disco duro SSD de uso general GP3. En caso de ser necesario se puede añadir almacenamiento

▼ Configurar almacenamiento [Información](#)

[Advanced](#)

1x GiB ▼ Volumen raíz (Sin cifrar)

[i](#) Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

✕

Agregar un nuevo volumen

En los detalles avanzados vamos a crear un pequeño script que se encargara de actualizar el servidor, instalar Apache, configurar su arranque automático y activar el servidor Web.

También creamos el típico ‘Hola mundo!’ en la carpeta del servidor http.

```
#!/bin/bash
yum update -y
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello World!</h1></html>' > /var/www/html/index.html
```

☐ Los datos de usuario ya han sido codificados en base64

Ya tenemos todo lo necesario, un último repaso en el panel ‘Resumen’ y a lanzar la instancia.

▼ Resumen

Número de instancias [Información](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.2.2...[read more](#)

ami-0230bd60aa48260c6

Virtual server type (instance type)

t2.micro

Firewall (security group)

Nuevo grupo de seguridad

Storage (volumes)

1 volume(s) - 8 GiB

ⓘ Nivel gratuito:

El primer año incluye 750 horas de uso de instancias t2.micro (o t3.micro en las regiones en las que t2.micro no esté disponible) en las AMI del nivel gratuito al mes, 30 GiB de almacenamiento de EBS, 2 millones de E/S, 1 GB de instantáneas y 100 GB de ancho de banda a Internet.

×

Cancelar

Lanzar instancia

[Revisar comandos](#)

✔ **Correcto**
El lanzamiento de la instancia se inició correctamente (i-07e9da141d0609d93)

Si accedemos a 'Ver todas las instancias' podemos comprobar que ya aparece. Esperamos a que aparezca el estado de 'En ejecución'



Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la ...	Zona de dispon...	DNS de IPv4 pública	Dirección IP...	IP elástica
Web Server 1	i-08c35ad809de0a2a8	En ejecución	t2.micro	2/2 comprobador	View alarms	us-east-1d	ec2-54-242-88-60.com...	54.242.88.60	-

Si la seleccionamos podemos comprobar sus detalles. Entre ellos la 'IP pública' desde la que accederemos a ella:



Detalles | Status and alarms New | Monitoreo | Seguridad | Redes

▼ Resumen de instancia Información

ID de la instancia
 I-0a3d9e86242ee2530 (Web Server 1)

Dirección IPv6

Dirección IPv4 pública copiada
 35.172.226.109 |di

Estado de la instancia

Intentaremos ahora acceder a la instancia desde el navegador web:

35.172.226.109

La conexión ha caducado

El servidor 35.172.226.109 está tardando demasiado en responder.

- El sitio podría estar no disponible temporalmente o demasiado ocupado. Vuelva a intentarlo en unos momentos.
- Si no puede cargar ninguna página, compruebe la conexión de red de su equipo.
- Si su equipo o red están protegidos por un cortafuegos o proxy, asegúrese de que Firefox tiene permiso para acceder a la web.

Reintentar

Vaya! Se nos ha olvidado algo.

El grupo de seguridad no permite el tráfico entrante en el puerto 80 (Http), así que en el panel de navegación de la consola accederemos a 'Red y seguridad', 'Grupos de seguridad', y seleccionamos el grupo de seguridad que creamos antes.:

Vamos a añadir una regla:

HTTP, cualquier lugar-IPv4

Editar reglas de entrada [Información](#)

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

Reglas de entrada [Información](#)

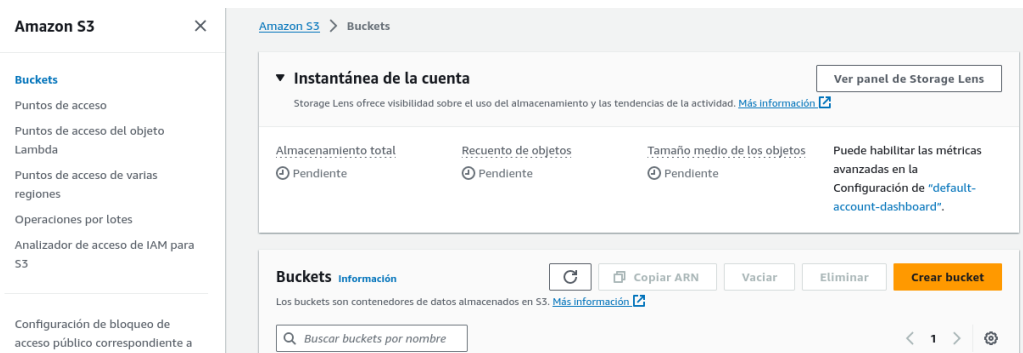
ID de la regla del grupo de seguridad	Tipo Información	Protocolo Información	Intervalo de puertos Información	Origen Información	Descripción: opcional Información	
-	HTTP	TCP	80	An... <input type="text"/>	<input type="text"/>	<input type="button" value="Eliminar"/>
				<input type="text" value="0.0.0.0/0"/>		

Actualizamos y ahora ya podemos acceder a la instancia desde el navegador Web



Crear un bucket S3

En el menú servicios buscamos los 'servicios de almacenamiento' y seleccionamos 'S3'



Seleccionamos Crear Bucket

Pondremos un nombre al Bucket.

El nombre tiene que cumplir unar normas:

- Estar libre
- Todo en minúsculas
- Puede empezar por letra o por número
- Mayor de 3 y menor d 63 caracteres

En la región seleccionaremos la más cercana para minimizar latencia y costes.
(En el entorno educativo utilizaremos la predeterminada)

Para poder acceder desmarcaremos la casilla de 'Bloquear todo el acceso público'

Configuración de bloqueo de acceso público para este bucket

Se concede acceso público a los buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos, active Bloquear todo el acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración individual a continuación para adaptarla a sus casos de uso de almacenamiento específicos. [Más información](#)

☐ Bloquear *todo* el acceso público

Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación. Cada uno de los siguientes ajustes son independientes entre sí.

☐ Bloquear el acceso público a buckets y objetos concedido a través de *nuevas* listas de control de acceso (ACL)

S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y evitará la creación de

y confirmamos que desactivamos el bloqueo

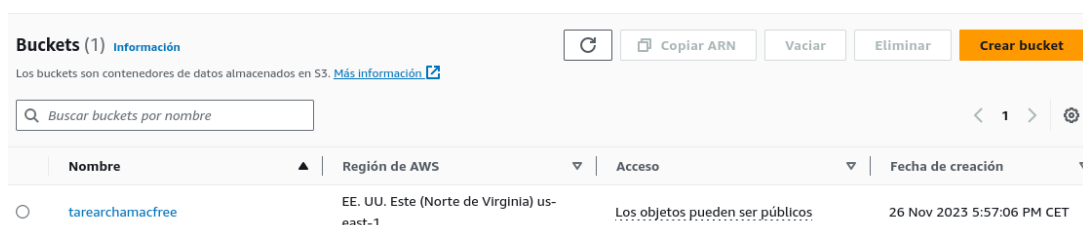
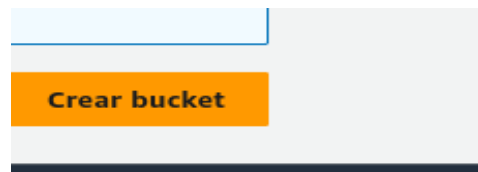


Desactivar el bloqueo de todo acceso público puede provocar que este bucket y los objetos que contiene se vuelvan públicos

AWS recomienda que active la opción para bloquear todo el acceso público, a menos que se requiera acceso público para casos de uso específicos y verificados, como el alojamiento de sitios web estáticos.

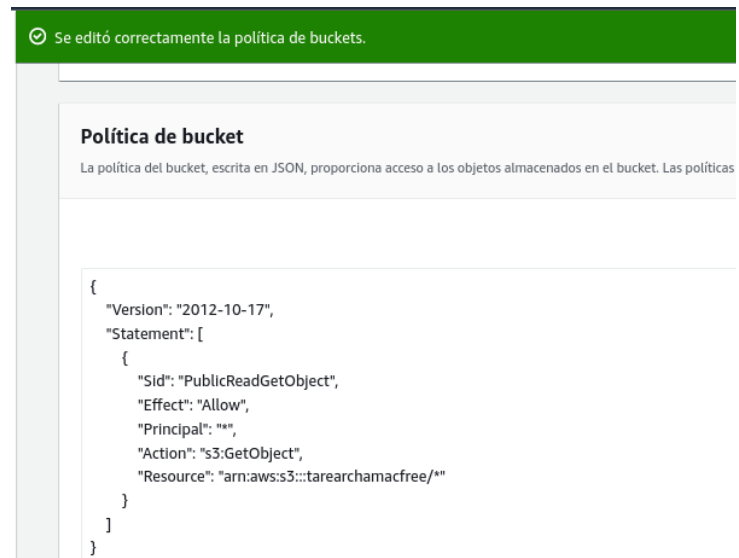
☐ Reconozco que la configuración actual puede provocar que este bucket y los objetos que contiene se vuelvan públicos.

Y ya podemos crear el bucket



Aún nos queda añadir los permisos necesarios para el acceso.

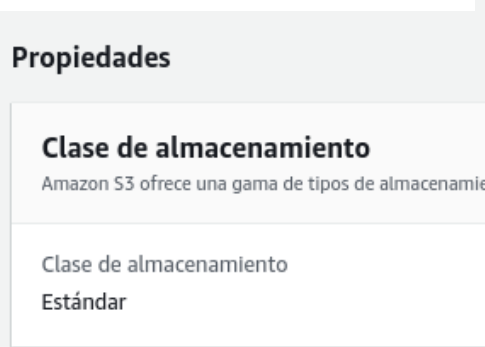
Desde la pestaña 'Permisos' editamos la 'Política de bucket' añadiendo una regla que permita el acceso público al sitio web



Cargaremos nuestro trabajo html al bucket, para ello desde la consola iremos a la pestaña 'Objetos' y arrastraremos nuestros archivos y carpetas a la zona de carga.



Comprobamos que tenemos una clase de almacenamiento estándar desde la sección de propiedades



Una vez cargados los archivos aparecerán en la lista de 'Objetos'

Nos queda indicar el archivo de acceso a nuestra aplicación Web. Para ello habilitamos la sección 'Alojamiento de sitios web estáticos' de la pestaña 'Propiedades' .

Indicamos como 'Documento de índice' el archivo de acceso a nuestra web (habitualmente se llamará index.html).

amazon S3 > Buckets > tarearchamacfree > Editar alojamiento de sitios web estáticos

Editar alojamiento de sitios web estáticos [Información](#)

Alojamiento de sitios web estáticos

Utilice este bucket para alojar un sitio web o redirigir solicitudes. [Más información](#)

Alojamiento de sitios web estáticos

☐ Desactivar

☒ **Habilitar**

Tipo de alojamiento

☒ **Alojar un sitio web estático**
 Utilice el punto de enlace del bucket como dirección web. [Más información](#)

☐ Redirigir las solicitudes de un objeto
 Redirija las solicitudes a otro bucket o dominio. [Más información](#)

ⓘ Para que sus clientes puedan obtener acceso al contenido en el punto de enlace del sitio web, debe hacer que todo el contenido sea legible públicamente. Para ello, puede editar la configuración Bloquear acceso público de S3 del bucket. Para obtener más información, consulte [Utilizar Bloquear acceso público de Amazon S3](#)

Documento de índice

Especifique la página predeterminada o de inicio del sitio web.

Al guardar los cambios nos indicará en la parte inferior de la sección 'Alojamiento de sitios web estáticos' un enlace al sitio web de bucket. Lo copiamos y comprobamos que podemos acceder desde un navegador web:

Alojamiento de sitios web estáticos

Utilice este bucket para alojar un sitio web o redirigir solicitudes. [Más información](#)

Alojamiento de sitios web estáticos

Habilitada

Tipo de alojamiento

Alojamiento de buckets

Punto de enlace de sitio web del bucket

Al configurar su bucket como sitio web estático, el sitio web estará disponible en el punto de enlace del sitio web específico de la región de AWS del bucket. [Más información](#)

<http://tarearchamacfree.s3-website-us-east-1.amazonaws.com/>

← → ↺

Q http://tarearchamacfree.s3-website-us-east-1.amazonaws.com/

Hello World. Take me to your leader.