

Desafío número 3

Grupo 2

Participantes:

- **Mariano Becchero**
- **Josue Reyes**
- **Matias Espinoza**
- **Ignacio Peretti**

Objetivos del desafío:

El objetivo de este desafío será crear algunos servicios básicos en nuestra cuenta de AWS e interactuar con ellos.

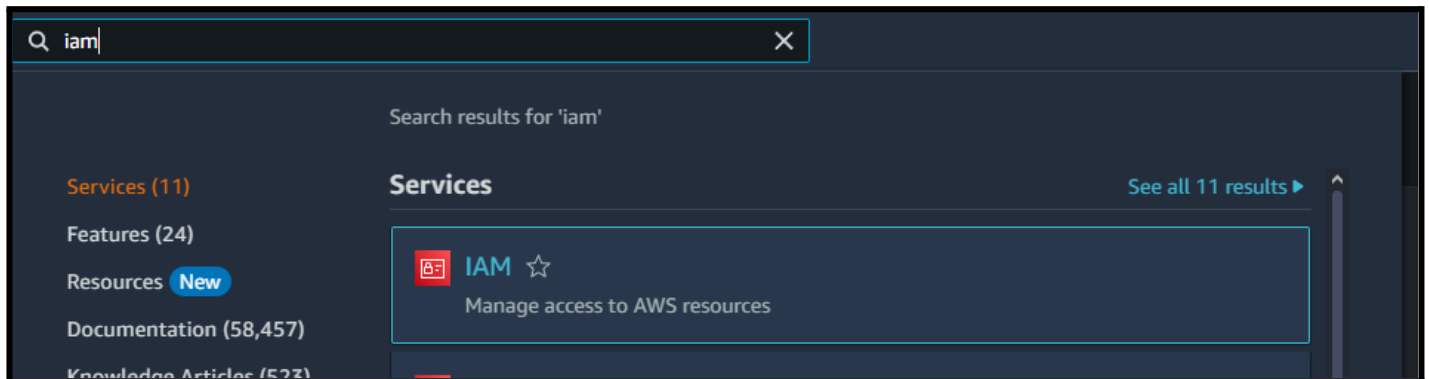
Primero tendremos que verificar los prerequisites, en caso de ya cumplirlos, aclararlo en el instructivo.

Luego crearemos una instancia EC2, un bucket S3 y un volumen de EBS.

Creación del usuario IAM.

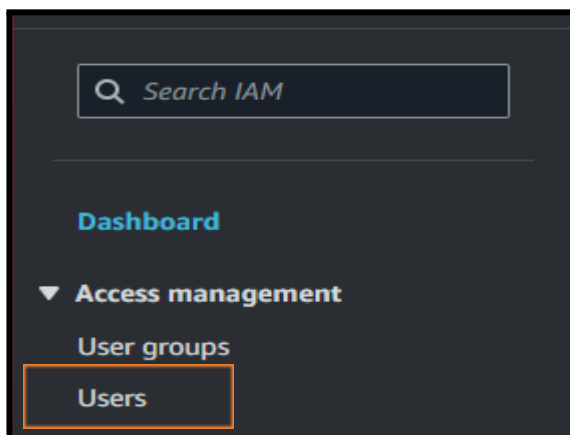
Crearemos el usuario siguiendo los siguientes pasos:

Paso 1.



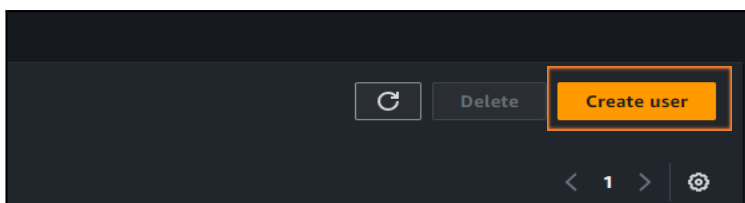
Buscamos el recurso en la barra de búsqueda de la plataforma con las palabras AIM y seleccionamos el recurso.

Paso 2.



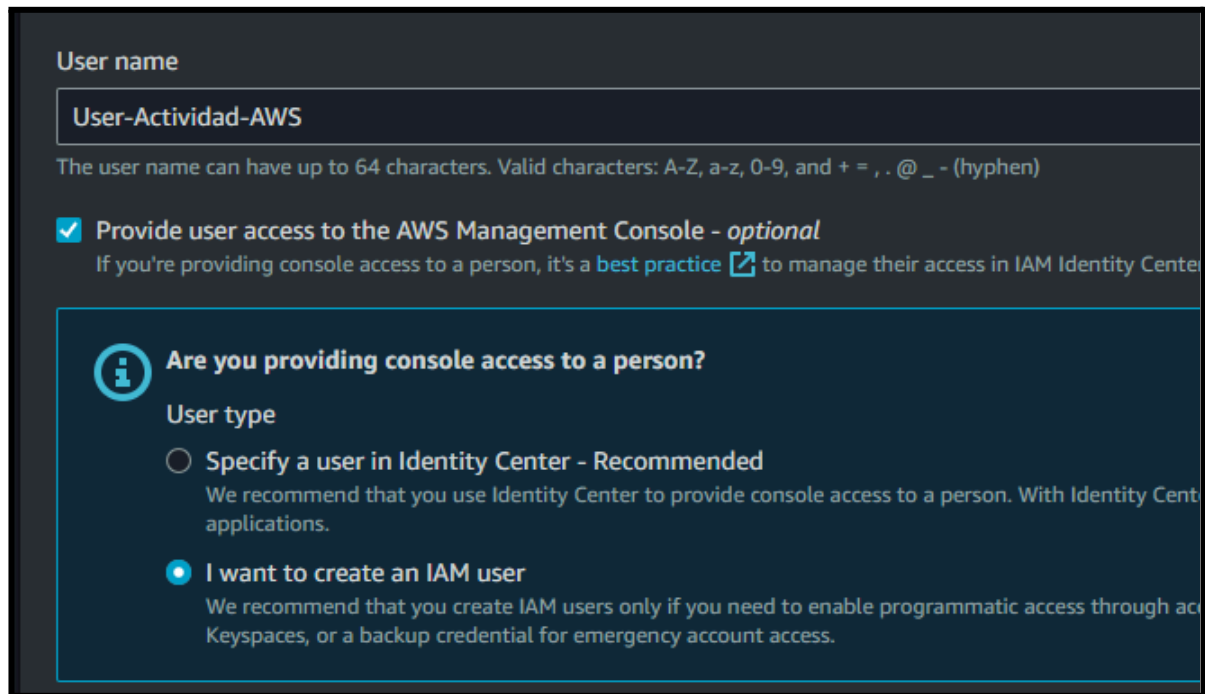
Buscamos User y le damos click.

Paso 3.



Seleccionamos **Create user**

Paso 4.



User name

User-Actividad-AWS

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ **Provide user access to the AWS Management Console - optional**
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

☐ **Specify a user in Identity Center - Recommended**
We recommend that you use Identity Center to provide console access to a person. With Identity Center applications.

☒ **I want to create an IAM user**
We recommend that you create IAM users only if you need to enable programmatic access through access keys, or a backup credential for emergency account access.

En la casilla de User name le asignaremos un nombre de usuario y seleccionaremos los siguientes parámetros:

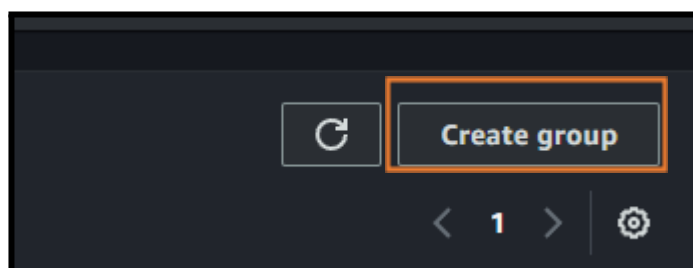
- ☐ **Provide user access to the AWS Management Console**
- ☐ **I want to create an IAM user**
- ☐ **Custom password (y creamos una contraseña personalizada)**

Click en botón Next

Paso 5.

En este paso le daremos los permisos al usuario en caso que ya se tengan un grupo creado se lo asignaremos. En nuestro caso crearemos uno nuevo.

para los cual vamos al botón Create Group



User group name
Enter a meaningful name to identify this group.


Grupo-2



Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.



Le asignamos un nombre, buscamos y le asignaremos los siguientes permisos:



- ☐ ***AmazonEC2FullAccess***
- ☐ ***AmazonS3FullAccess***
- ☐ ***AmazonEBSCSIDriverPolicy***
- ☐ ***ROSAAmazonEBSCSIDriverOperatorPolicy***



Search

☐ Policy name 

☐   [AmazonEBSCSIDriverPolicy](#)

☐   [AmazonEC2FullAccess](#)

☐   [AmazonS3FullAccess](#)

☐   [ROSAAmazonEBSCSIDriverOperatorPolicy](#)

Paso 6.

Agregarles las Tags

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

Key	Value - optional
<input type="text" value="Owner"/>	<input type="text" value="Josue Reyes"/>
<input type="text" value="E-mail"/>	<input type="text" value="josuereydev@gmail.com"/>
<input type="text" value="Team"/>	<input type="text" value="Grupo-2"/>
<input type="text" value="Proyecto-1"/>	<input type="text" value="Actividad-AWS"/>

Use "Actividad-AWS"

Y por ultimo le damos **Create User**

Y nos abrirá la siguiente ventana con la información del usuario creado

Console sign-in details

Console sign-in URL

User name

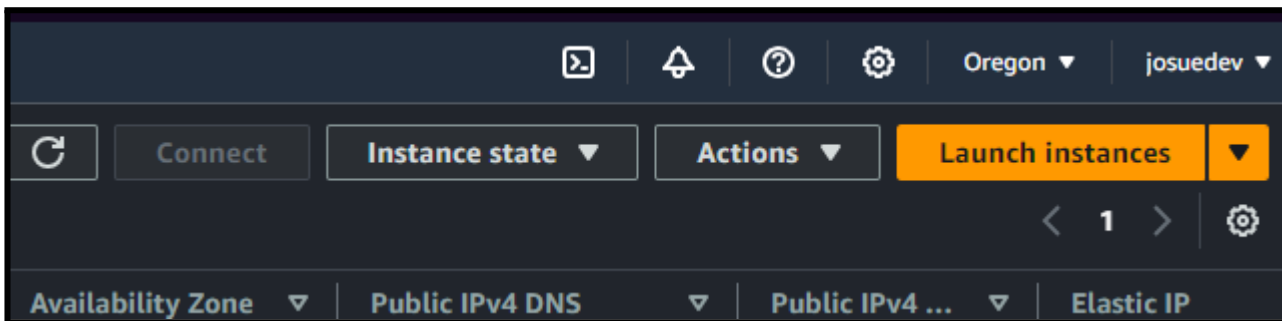
Console password
 [Show](#)

Lanzar instancias en EC2

Para lanzar una instancia en EC2 es importante tener en cuenta la región o zona en la que se lanzará, en nuestro caso lo haremos en **us-east-1 (N. Virginia)**

En la barra de búsqueda escribimos EC2 y vamos a **Launch instances**

Paso 1.



Paso 2. Elegir un nombre para nuestra instancia

Launch an instance Info

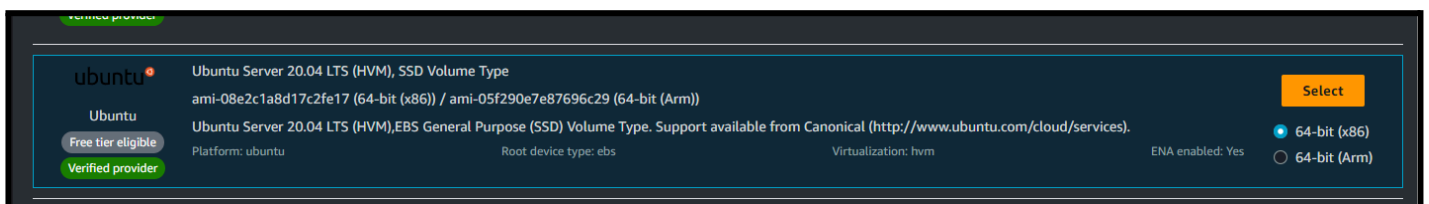
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

[Add additional tags](#)

Paso 3. Buscamos y seleccionamos el recurso o la AMI



Paso 4. Elegir el tipo de Instancia (En este caso elegiremos la permitida en la capa gratuita de AWS)

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux base pricing: 0.0116 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand RHEL base pricing: 0.0716 USD per Hour

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

Paso 5. Creamos un Key Pair Login (Este Key Pair lo podemos utilizar en cualquier máquina desplegada en la región de Virginia)

Create key pair

×

Key pair name

Key pairs allow you to connect to your instance securely.

KP-Grupo2-DesafioAWS

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ **RSA**
RSA encrypted private and public key pair

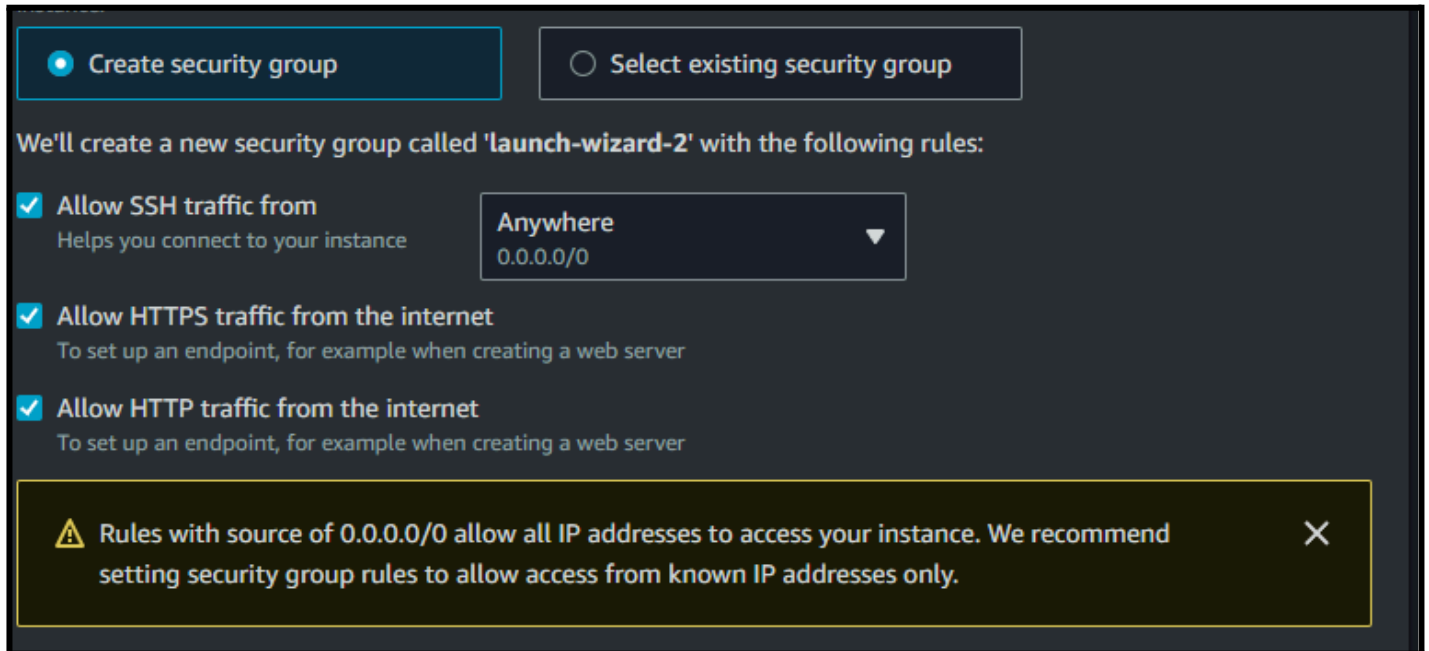
☐ **ED25519**
ED25519 encrypted private and public key pair

Private key file format

☒ **.pem**
For use with OpenSSH

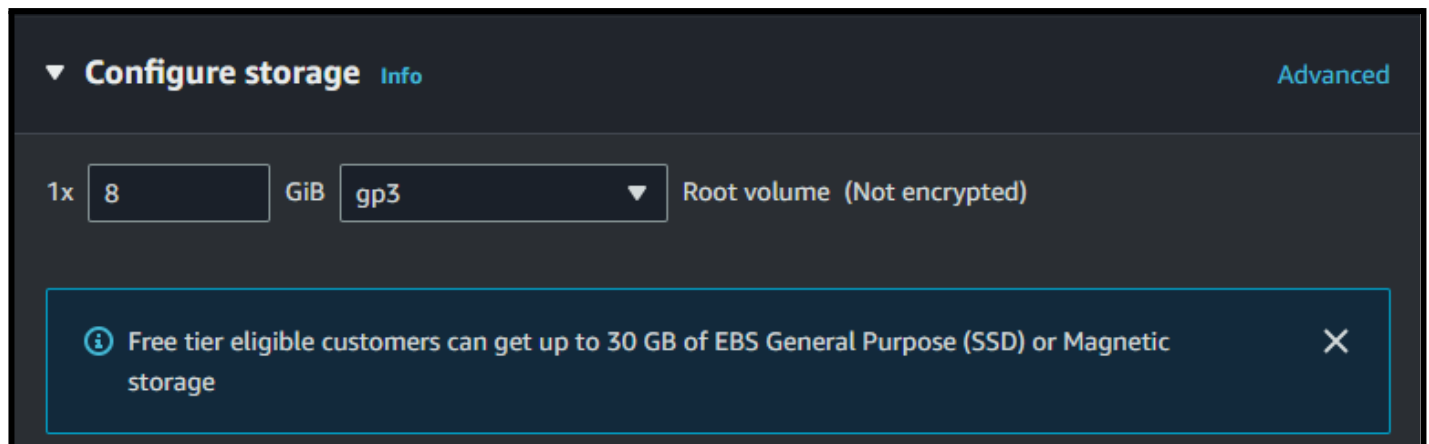
Paso 6. Configuramos los parámetros de Red

- Predeterminado Create security Group
- Allow SSH traffic from **Anywhere** (*Dejarlo en Anywhere es una mala práctica porque permitiría que haya conexión de cualquier lugar*) de momento lo dejaremos así.



The screenshot shows the AWS IAM console interface for creating a new security group. At the top, there are two radio buttons: "Create security group" (selected) and "Select existing security group". Below this, a message states: "We'll create a new security group called 'launch-wizard-2' with the following rules:". There are three checked rules: "Allow SSH traffic from" (with a subtext "Helps you connect to your instance" and a dropdown menu showing "Anywhere" and "0.0.0.0/0"), "Allow HTTPS traffic from the internet" (with a subtext "To set up an endpoint, for example when creating a web server"), and "Allow HTTP traffic from the internet" (with a subtext "To set up an endpoint, for example when creating a web server"). At the bottom, there is a yellow warning box with a triangle icon and the text: "Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only." with a close button (X).

Paso 7. Configurar el almacenamiento.



The screenshot shows the AWS IAM console interface for configuring storage. At the top, there is a section titled "Configure storage" with a dropdown arrow and an "Info" link. To the right of this section is a link labeled "Advanced". Below this, there are two input fields: "1x" and "8" (with a unit "GiB" next to it), and a dropdown menu showing "gp3". To the right of these fields is the text "Root volume (Not encrypted)". At the bottom, there is a blue information box with an "i" icon and the text: "Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage" with a close button (X).

Paso 8. Instalamos Apache2 desde nuestra Instancia de la siguiente manera

En Advanced Details escribiremos el siguiente script.

User data - optional

Info

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
apt-get update -y
apt-get install apache2 -y
echo "Instalacion de Apache2-Server"
systemctl start apache2
```

Paso 9. Lanzar la Instancia

En la sección de **Intances** podemos verificar que la instancia creada está corriendo.

Instances (1/2) Info			
Find Instance by attribute or tag (case-sensitive)			All states ▼
	Name	Instance ID	Instance state
<input checked="" type="checkbox"/>	ActividadAWS-Linux22	i-074824a61891b678d	Running
<input type="checkbox"/>	UbutuServer-DesafioAWS	i-0aea28ebd79faf8d3	Stopped

Conectarse a la Instancia por SSH desde nuestra VM

Hay varias formas para conectarnos a la instancia en esta ocasión lo haremos por medio de conexión SSH desde nuestra terminal de Linux

Paso 1. Copiamos nuestro clave codificada o KeyPair en algún fichero en nuestra VM

una vez en ese directorio corremos el comando **chmod 400** para darle permisos y luego corremos el comando **ssh -i** + el contenido de nuestro archivo .pem

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID
i-074824a61891b678d (ActividadAWS-Linux22)

1. Open an SSH client.

2. Locate your private key file. The key used to launch this instance is KP-Grupo2-DesafioAWS.pem

3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "KP-Grupo2-DesafioAWS.pem"

4. Connect to your instance using its Public DNS:
ec2-3-93-187-245.compute-1.amazonaws.com

Example:
ssh -i "KP-Grupo2-DesafioAWS.pem" ubuntu@ec2-3-93-187-245.compute-1.amazonaws.com

Si los datos son correctos nos conectaremos a la instancia EC2 que hemos creado.

```
/home/linux/Documentos/AWS-credenciales
root@ubuntu20:/home/linux/Documentos/AWS-credenciales# chmod 400 "KP-Grupo2-DesafioAWS.pem"
root@ubuntu20:/home/linux/Documentos/AWS-credenciales# ssh -i "KP-Grupo2-DesafioAWS.pem" ubuntu@ec2-3-93-187-245.compute-1.amazonaws.com
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1017-aws x86_64)

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

System information as of Sun May  5 23:40:33 UTC 2024

System load:  0.0               Processes:            102
Usage of /:   25.2% of 7.57GB   Users logged in:     1
Memory usage: 21%              IPv4 address for eth0: 172.31.16.65
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

7 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

Paso 2. Verificamos si el servidor Apache2 fue instalado con el comando:

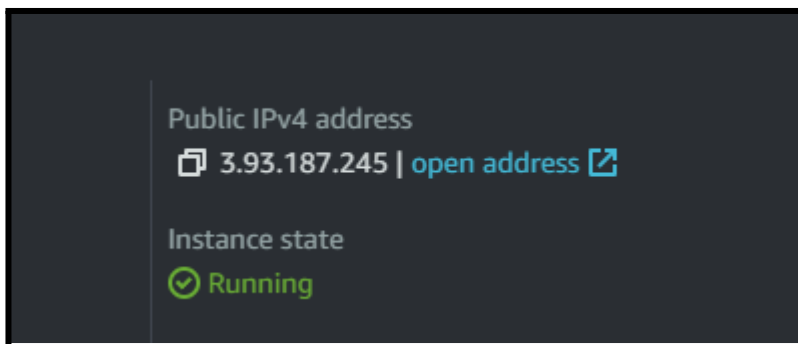
sudo systemctl status apache2.

```
Last login: Sun May  5 23:28:06 2024 from 186.22.245.136
ubuntu@ip-172-31-16-65:~$ sudo systemctl reload apache2
ubuntu@ip-172-31-16-65:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-05-05 23:19:00 UTC; 22min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 346 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Process: 925 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
  Main PID: 411 (apache2)
    Tasks: 55 (limit: 1121)
   Memory: 7.5M
      CPU: 150ms
   CGroup: /system.slice/apache2.service
           └─411 /usr/sbin/apache2 -k start
             └─929 /usr/sbin/apache2 -k start
               └─930 /usr/sbin/apache2 -k start
```

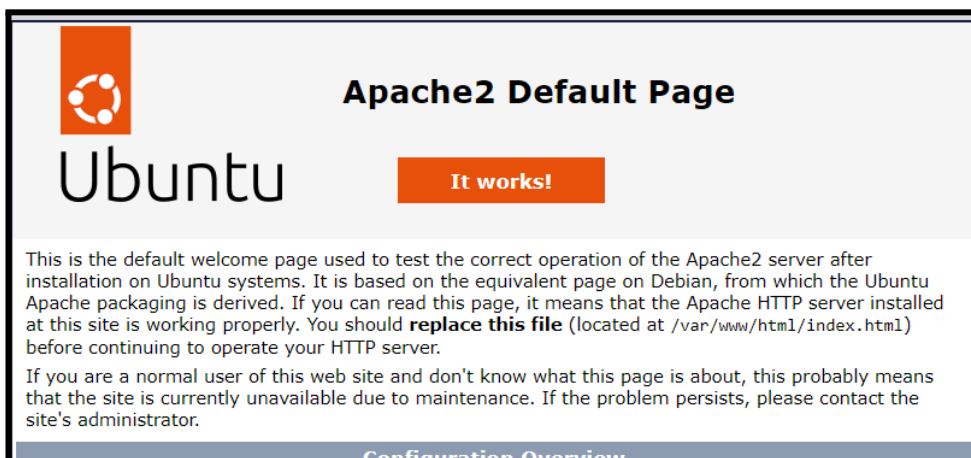
La imagen del servidor indica que está corriendo.

Paso 3. Verificar en un navegador

Para verificar que podemos navegar en el servidor lo hacemos con la dirección IP Pública de nuestra Instancia.



Copiamos la dirección en la barra de navegación y nos abrirá el servidor.



Crear un bucket en el servicio S3

Una vez logueados al usuario que creamos con los permisos de **AmazonS3FullAccess** podremos crear un bucket para almacenamiento.

Paso 1.

Ingresamos un nombre para el bucket y dejamos todos los servicios predeterminados, por último cliqueamos en el botón **Crear Bucket**.

Configuración general

Región de AWS

EE. UU. Este (Norte de Virginia) us-east-1

Tipo de bucket [Información](#)

☒ **Uso general**

Recomendado para la mayoría de los casos de uso y patrones de acceso. Los buckets de uso general son del tipo de bucket de S3 original. Permiten una combinación de clases de almacenamiento que almacenan objetos de forma redundante en múltiples zonas de disponibilidad.

☐ **Directorio: nuevo**

Recomendado para casos de uso de baja latencia. Estos buckets utilizan únicamente la clase de almacenamiento S3 Express One Zone, que proporciona un procesamiento más rápido de los datos dentro de una única zona de disponibilidad.

Nombre del bucket [Información](#)

bucketgrupo2

Configuración de bloqueo de acceso publico 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 nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos existentes que permiten acceso público a los recursos de S3 mediante ACL.

☒ **Bloquear el acceso público a buckets y objetos concedido a través de cualquier lista de control de acceso (ACL)**

S3 ignorará todas las ACL que conceden acceso público a buckets y objetos.

☒ **Bloquear el acceso público a buckets y objetos concedido a través de políticas de bucket y puntos de acceso públicas nuevas**

S3 bloqueará las nuevas políticas de buckets y puntos de acceso que concedan acceso público a buckets y objetos. Esta configuración no afecta a las políticas ya existentes que permiten acceso público a los recursos de S3.

☒ **Bloquear el acceso público y entre cuentas a buckets y objetos concedido a través de cualquier política de bucket y puntos de acceso pública**

S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso que tengan políticas que concedan acceso público a buckets y objetos.

Paso 2. Subir un archivo al bucket

Una vez creado el bucket listamos e ingresamos al bucket haciendo clic sobre el bucket.

Buckets de uso general (1) [Información](#) Todas las regiones de AWS

Los buckets son contenedores de datos almacenados en S3.

	Nombre	Región de AWS
<input checked="" type="radio"/>	bucketgrupo2	EE. UU. Este (Norte de Virginia) us-east-1

Paso 3. Cargar o subir el archivo.

Archivos y carpetas (1 Total, 53.4 KB) Eliminar Agregar archivos Agregar carpeta

Se cargarán todos los archivos y las carpetas de esta tabla.

< 1 >

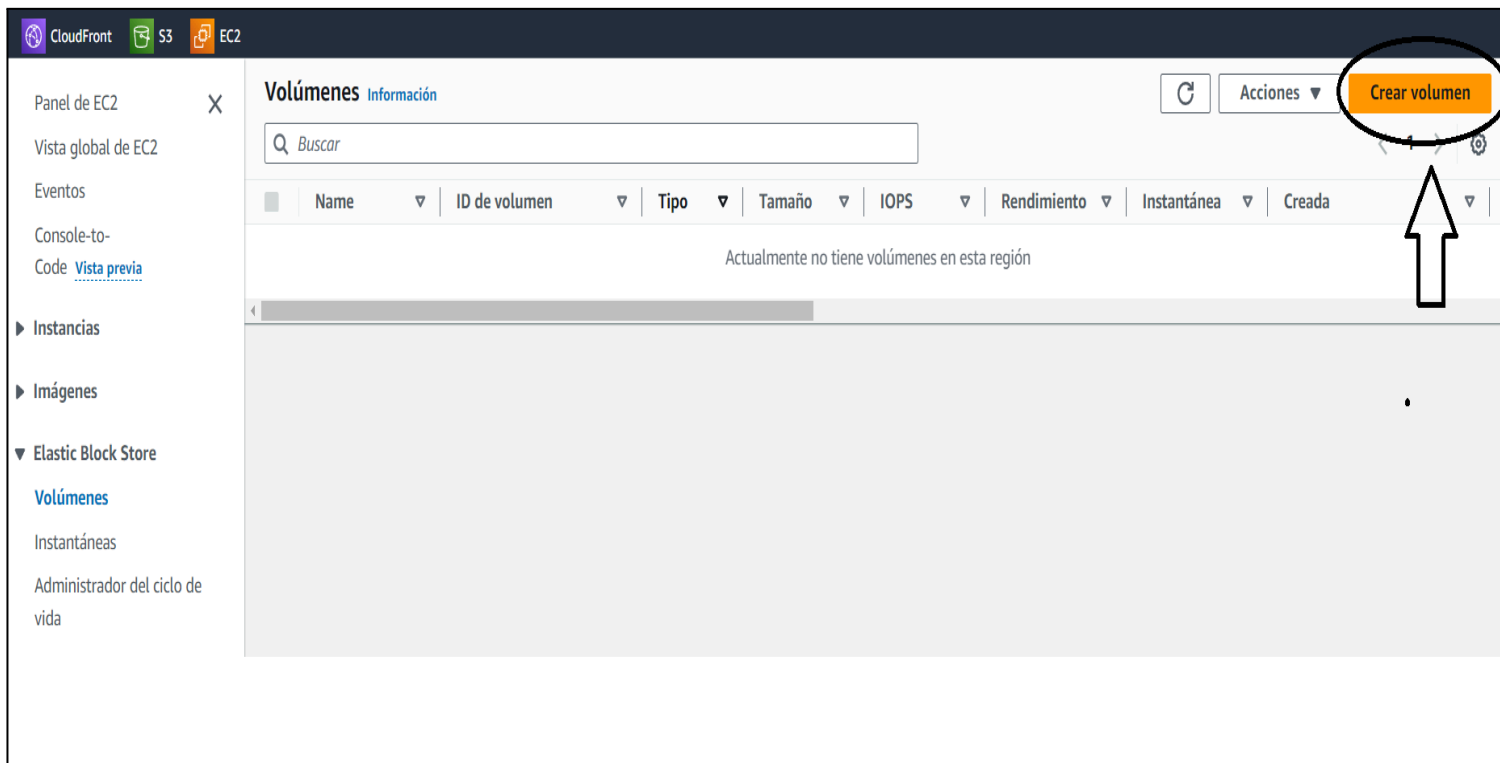
<input checked="" type="checkbox"/>	Nombre	Carpeta
<input checked="" type="checkbox"/>	Actividad-AWS.pdf	-

Elastic Block Store (EBS)

Crear un volumen de EBS y linkearlo a la instancia que creamos previamente.

Paso 1.

En el panel del servicio EC2 nos dirigimos al apartado Elastic Block Store (EBS), Volúmenes y daremos clic en la opción **Crear Volumen**.



En este volumen usaremos los valores por default que nos recomiendan y el tamaño será de **2 GB**, luego verificamos que estemos en la misma región y AZ.

Configuración del volumen

Tipo de volumen

Información

SSD de uso general (gp3)

Tamaño (GiB)

Información

2

Mín.: 1 GiB, máx.: 16384 GiB. El valor debe ser un número entero.

IOPS

Información

3000

Mín.: 3000 IOPS, máx.: 16000 IOPS. El valor debe ser un número entero.

Rendimiento (MiB/s)

Información

125

Mín.: 125 MiB, máx.: 1000 MiB. Línea de base: 125 MiB/s.

Zona de disponibilidad

Información

us-east-1a

ID de instantánea - opcional

Información

No crear un volumen a partir de una instantánea

Cifrado

Información

Utilice el cifrado de Amazon EBS como una solución de cifrado para los recursos de EBS asociados a las instancias EC2.

☐ Cifrar este volumen

Una vez creado el volumen nos dirigimos a él y dentro de **Acciones** hacemos clic en la opción **Asociar Volumen**.

EC2 > Volúmenes > vol-010b812d0fa549958

↑ vol-010b812d0fa549958

Acciones ▲ Eliminar Modificar

Crear instantánea

Asociar volumen

Desasociar el volumen

Desasociar el volumen forzosamente

Administrar habilitación automática de E/S

ID de volumen vol-010b812d0fa549958	Tamaño 2 GiB	Tipo gp3
Hallazgo de AWS Compute Optimizer Participe en AWS Compute Optimizer para recibir recomendaciones. Más información	Estado del volumen Disponible	IOPS 3000

Dentro de los detalles seleccionamos la instancia previamente creada.

WS Servicios [Alt+S] Buscar

EC2 > Volúmenes > vol-0ca43f23097d83a82 > Asociar volumen

Asociar volumen Información

Asocie un volumen a una instancia para utilizarlo de la misma forma en la que usaría una unidad de disco duro física normal.

Detalles básicos

ID de volumen
vol-0ca43f23097d83a82

Zona de disponibilidad
us-east-1d

Instancia Información

Buscar ID de instancia o etiqueta de nombre

i-0ba0d1d03064b1906
(Actividad-AWS-Grupo2-test) (stopped)

Cancelar Asociar volumen

Luego de elegir la instancia seleccionamos el nombre del dispositivo y damos clic en **Asociar Volumen**.

EC2 > Volúmenes > vol-0ca43f23097d83a82 > Asociar volumen

Asociar volumen Información

Asocie un volumen a una instancia para utilizarlo de la misma forma en la que usaría una unidad de disco duro física normal.

Detalles básicos

ID de volumen
vol-0ca43f23097d83a82

Zona de disponibilidad
us-east-1d

Instancia Información

i-0ba0d1d03064b1906

Solo se muestran las instancias de la misma zona de disponibilidad que el volumen seleccionado.

Nombre del dispositivo Información

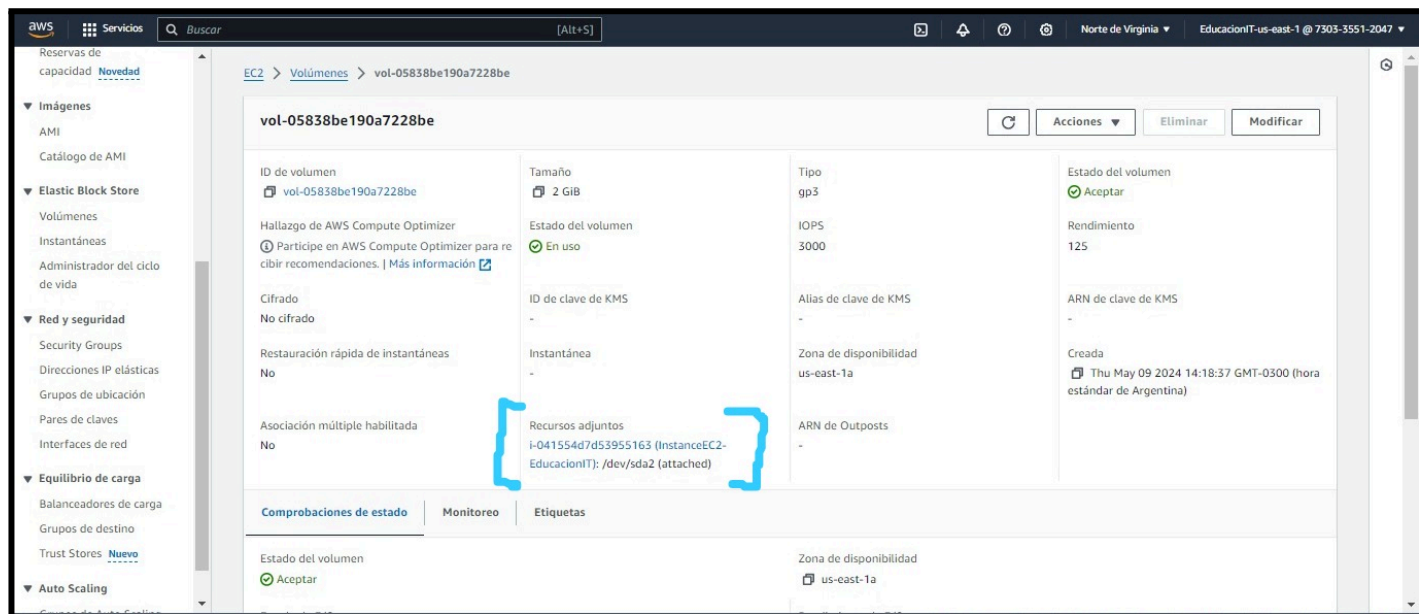
/dev/sde

Nombres de dispositivos recomendados para Linux: /dev/xvda para el volumen raíz, /dev/sd[f-p] para los volúmenes de datos.

Nota: Los kernels de Linux más recientes pueden cambiar el nombre de sus dispositivos a /dev/xvdf through /dev/xvdp internamente, aunque el nombre introducido aquí (y mostrado en los detalles) sea /dev/sdf through /dev/sdp.

Cancelar Asociar volumen

Verificamos que el volumen se agregó de forma correcta a nuestro sistema.



Listamos volúmenes. (el nuestro es xvdb - 2 GB)

```
ubuntu@ip-172-31-18-27:~$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0       7:0      0   25.2M  1 loop /snap/amazon-ssm-agent/7983
loop1       7:1      0   55.7M  1 loop /snap/core18/2812
loop2       7:2      0   63.9M  1 loop /snap/core20/2264
loop3       7:3      0    87M  1 loop /snap/lxd/27948
loop4       7:4      0   39.1M  1 loop /snap/snapd/21184
loop5       7:5      0    87M  1 loop /snap/lxd/28373
loop6       7:6      0   38.7M  1 loop /snap/snapd/21465
xvda        202:0    0     8G  0 disk 
├─xvda1     202:1    0    7.9G  0 part /
├─xvda14    202:14   0     4M  0 part 
├─xvda15    202:15   0   106M  0 part /boot/efi
└─xvdb      202:16   0     2G  0 disk
```

Formateamos el EBS. (Nos muestra un aviso de que ya está formateado)

```
ubuntu@ip-172-31-18-27:~$ sudo mkfs -t ext4 /dev/xvdb
mke2fs 1.46.5 (30-Dec-2021)
/dev/xvdb contains a ext4 file system
last mounted on Thu May 9 23:59:15 2024
Proceed anyway? (y,N) y
Creating filesystem with 524288 4k blocks and 131072 inodes
Filesystem UUID: 051d434b-d3af-4b86-809f-f2f4434c93b5
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

Utilizamos los comandos

- lsblk Para ver cual es el nombre.
- sudo mkfs -t ext4 /dev/xvdf --- Para formatearlo con la extensión ext4.

Agregamos a FSTAB y montamos el FS en el directorio /desafíos.

Creamos el directorio y le damos los permisos correspondientes para que se pueda escribir.

- `mkdir /desafíos`
- `sudo chmod 777 /desafíos`

```
ubuntu@ip-172-31-18-27:~$ ls
ubuntu@ip-172-31-18-27:~$ sudo mkdir desafios
ubuntu@ip-172-31-18-27:~$ ls
desafios
ubuntu@ip-172-31-18-27:~$
```

```
ubuntu@ip-172-31-18-27:~$
ubuntu@ip-172-31-18-27:~$
ubuntu@ip-172-31-18-27:~$
ubuntu@ip-172-31-18-27:~$ sudo chmod 777 /desafios
ubuntu@ip-172-31-18-27:~$
```

Editamos con nano o vi el archivo /etc/fstab y agregamos esta línea.

`/dev/xvdf /desafíos ext4 defaults,nofail 0 2`

```

LABEL=cloudimg-rootfs / ext4 discard,errors=remount-ro 0 1
LABEL=UEFI /boot/efi vfat umask=0077 0 1
/dev/xvdb1 /desafíos ext4 defaults,nofail 0 2
```

Lo que logramos con esto es que agrega el sistema de archivo del disco nuevo al arranque del sistema.

Por último utilizamos el comando **sudo mount -a** para montar el sistema de archivos en el directorio /desafíos.

```
ubuntu@ip-172-31-18-27:~$ sudo nano /etc/fstab
ubuntu@ip-172-31-18-27:~$ sudo mkdir desafios
ubuntu@ip-172-31-18-27:~$ sudo mount -a
ubuntu@ip-172-31-18-27:~$ mount -l
/dev/xvda1 on / type ext4 (rw,relatime,discard,errors=remount-ro) [cloudimg-rootfs]
devtmpfs on /dev type devtmpfs (rw,nosuid,noexec,relatime,size=478444k,nr_inodes=119611,mode=755,inode64)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,size=194408k,nr_inodes=819200,mode=755,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
/var/lib/containers/snapshots/amazon-ssm-agent_7983.snap on /snap/amazon-ssm-agent/7983 type squashfs (ro,nodev,relatime,errors=continue,threads=single,x-gdu.hide)
/var/lib/containers/snapshots/snapd_21465.snap on /snap/snapd/21465 type squashfs (ro,nodev,relatime,errors=continue,threads=single,x-gdu.hide)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=97200k,nr_inodes=24300,mode=700,uid=1000,gid=1000,inode64)
/dev/xvda15 on /boot/efi type vfat (rw,relatime,fmask=0077,dmask=0077,codepage=437,iocharset=iso8859-1,shortname=mixed,errors=remount-ro) [UEFI]
/dev/xvdb on /desafios type ext4 (rw,relatime)
```

Luego listamos los volúmenes montados.

Probamos crear un archivo para ver si se puede escribir sobre ese punto de montaje.

```
ubuntu@ip-172-31-18-27:~$ cd desafios
ubuntu@ip-172-31-18-27:~/desafios$ sudo nano prueba.txt
ubuntu@ip-172-31-18-27:~/desafios$ ls
prueba.txt
ubuntu@ip-172-31-18-27:~/desafios$ |
```

Por último al bucket le asignamos los permisos públicos y con el comando **wget** descargamos el archivo, luego verificamos que se pueda escribir en el mismo y descargamos el desafío desde el bucket.

```
ubuntu@ip-172-31-18-27:~/desafios$ sudo wget https://s3bucket-educacionit.s3.amazonaws.com/Actividad-AWS_1.pdf
--2024-05-10 00:29:43-- https://s3bucket-educacionit.s3.amazonaws.com/Actividad-AWS_1.pdf
Resolving s3bucket-educacionit.s3.amazonaws.com (s3bucket-educacionit.s3.amazonaws.com)... 3.5.30.180, 52.216.36.169, 52.216.44.169, ...
Connecting to s3bucket-educacionit.s3.amazonaws.com (s3bucket-educacionit.s3.amazonaws.com)|3.5.30.180|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 54633 (53K) [application/pdf]
Saving to: 'Actividad-AWS_1.pdf'

Actividad-AWS_1.pdf      100%[=====] 53.35K  --.-KB/s   in 0.002s

2024-05-10 00:29:44 (22.9 MB/s) - 'Actividad-AWS_1.pdf' saved [54633/54633]

ubuntu@ip-172-31-18-27:~/desafios$ ls
Actividad-AWS_1.pdf  prueba.txt
ubuntu@ip-172-31-18-27:~/desafios$
```

Fin del instructivo.