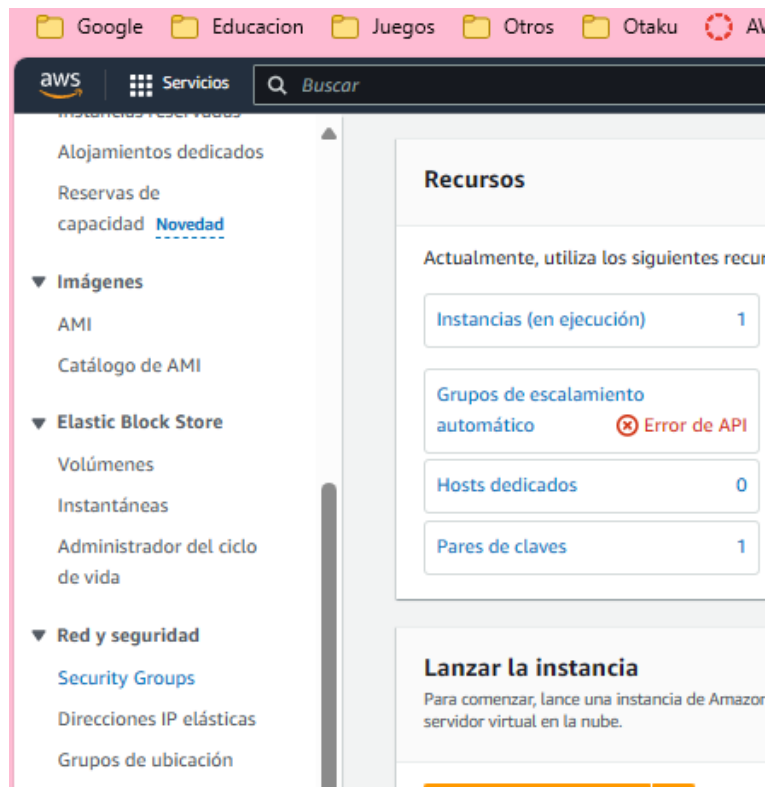


Presentación de Amazon Elastic File System

Primeramente, vamos a crear un grupo de seguridad para acceder al sistema de archivos de EFS, para ello accedemos al servicio de EC2, seleccionamos Grupos de Seguridad:



Aquí nos aparecen 3 grupos, elegimos el EFSClient y copiamos su id:

<input type="checkbox"/>	Name	ID de grupo de seguridad	Nombre del grupo de seguridad
<input type="checkbox"/>	-	sg-00a3c32824c725089	default
<input type="checkbox"/>	EFSClient	sg-022e9dc24e02656d6	EFSClient
<input type="checkbox"/>	-	sg-056373505acc842bd	default

[sg-022e9dc24e02656d6](#)

Una vez hecho esto, le damos a crear grupo de seguridad y rellenamos los siguientes apartados los siguientes:

The screenshot shows the AWS IAM console 'Detalles básicos' (Basic details) for a security group. The 'Nombre del grupo de seguridad' (Security group name) is 'EFS Mount Target'. The 'Descripción' (Description) is 'Inbound NFS access from EFS clients'. The 'VPC' is 'vpc-006aad9b28bb2298e (Lab VPC)'. Below this, the 'Reglas de entrada' (Inbound rules) section shows a single rule with 'Tipo' (Type) as 'NFS', 'Protocolo' (Protocol) as 'TCP', 'Intervalo de puertos' (Port range) as '2049', and 'Origen' (Source) as 'sg-022e9dc24e02656d6'. There is an 'Agregar regla' (Add rule) button at the bottom left of the rules section.

Esta configuración ya es suficiente, le damos a crear grupo. Ahora vamos a crear un sistema de archivos de EFS (Los sistemas de archivos de EFS se pueden montar en varias instancias de EC2 que se ejecuten en diferentes zonas de disponibilidad dentro de la misma región. Estas instancias usan *destinos de montaje* creados en cada *zona de disponibilidad* para montar el sistema de archivos mediante la semántica estándar de NFSv4.1. Puedes montar el sistema de archivos en instancias de una sola nube virtual privada (VPC) a la vez. Tanto el sistema de archivos como la VPC deben estar en la misma región.), para ello entramos en el servicio EFS y le damos a crear sistema de archivos:

Aquí pulsamos personalizar.

En el paso 1:

The screenshot shows the AWS EFS console configuration page. Under 'Copias de seguridad automáticas' (Automatic backups), there is a checkbox for 'Permitir copias de seguridad automáticas' (Allow automatic backups) which is currently unchecked. Under 'Administración del ciclo de vida' (Lifecycle management), there is a description: 'Ahorre dinero automáticamente a medida que cambian los patrones de acceso. Para ello, traslade los archivos a la clase de almacenamiento Infrequent Access (IA) en función del tiempo transcurrido desde la última vez que se accedió a ellos en el almacenamiento estándar.' Below this, there are three columns for lifecycle transitions: 'Transición a Infrequent Access (IA)', 'Transición a archivo' (Transition to archive), and 'Transición a Standard'. Each column has a description and a dropdown menu set to 'Ninguno' (None). At the bottom, there are two input fields: 'Clave de la etiqueta' (Tag key) with the value 'name' and 'Valor de la etiqueta - opcional' (Optional tag value) with the value 'My First EFS File System'.

Le damos a siguiente.

En el paso 2, ponemos la VPC del laboratorio y ponemos el grupo de seguridad que hemos creado:

Red

⚠ Le recomendamos que habilite el rol vinculado al servicio EFS mediante AWS IAM. Los roles vinculados a servicios le permiten delegar permisos fá los servicios de AWS y obtener más transparencia en cuando se utilizan en su nombre. [Más información](#)

Virtual Private Cloud (VPC) [Más información](#)

Elija la VPC en la que desea que las instancias EC2 se conecten a su sistema de archivos.

vpc-006aad9b28bb2298e
Lab VPC

Destinos de montaje

Un destino de montaje proporciona un punto de enlace NFSv4 en el que puede montar un sistema de archivos de Amazon EFS. Le recomendamos que cree un destino de montaje | disponibilidad. [Más información](#)

Zona de disponibilidad	ID de la subred	Dirección IP	Grupos de seguridad	
us-east-1a	subnet-0335fac340...	Automático	Elegir grupos de seg...	Eliminar
			sg-0ec1800a022356a98 EFS Mount Target	
us-east-1b	subnet-0dfb8b344c...	Automático	Elegir grupos de seg...	Eliminar
			sg-0ec1800a022356a98 EFS Mount Target	

En el paso 3 le damos a siguiente y en el 4 revisamos y crear.

Ahora vamos a conectarnos por ssh a la instancia de EC2. Para ellos necesitamos descargarnos las credenciales de la instancia y la ip publica, todo esto lo encontramos en los detalles del laboratorio. También necesitamos el cliente PuTTY para acceder por ssh.

Debemos poner la siguiente configuración:

Category:

Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP

Options controlling the connection
Sending of null packets to keep session active
Seconds between keepalives (0 to turn off) 30
Low-level TCP connection options
☒ Disable Nagle's algorithm (TCP_NODELAY option)
☐ Enable TCP keepalives (SO_KEEPALIVE option)
Internet protocol version
☒ Auto ☐ IPv4 ☐ IPv6
Logical name of remote host
Logical name of remote host (e.g. for SSH key lookup):

Category:

Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP

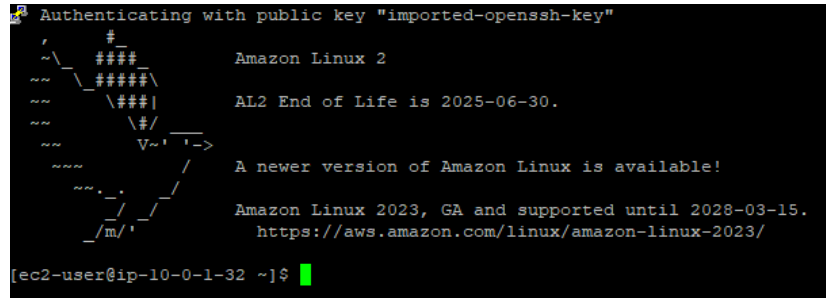
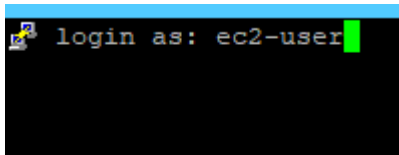
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address) 34.199.116.25 Port 22
Connection type:
☒ SSH ☐ Serial ☐ Other: Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings Load Save Delete
Close window on exit:
☐ Always ☐ Never ☒ Only on clean exit

Category:

Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Auth
Credent
GSSAPI
TTY
X11

Credentials to authenticate with
Public-key authentication
Private key file for authentication:
C:\Users\vicor\Downloads\Vabsuser.ppk Browse...
Certificate to use with the private key (optional):
Browse...
Plugin to provide authentication responses
Plugin command to run

Ya estando todo configurado, nos conectamos y nos pedirá un login: ec2-user



Vemos que podemos acceder por ssh sin problemas a la instancia.

Vamos a crear un directorio nuevo y montar el sistema de archivos de EFS. Dentro de la sesión ssh, vamos a crear una carpeta con el comando `sudo mkdir efs`. Una vez creada, entramos al servicio EFS desde la consola AWS, y seleccionamos la que creamos previamente(debí ponerle nombre).

	Nombre ▾	ID del sistema de archivos ▾	Cifrado ▾	Tamaño total ▾	Tamaño en estándar ▾	Tamaño en acceso poco frecuente ▾
		fs-0aad5b5961308af11	✓ Cifrado	6.00 KiB	6.00 KiB	0 bytes

Etiquetas Administrar etiquetas	
Clave de la etiqueta ▾	Valor de la etiqueta ▾
name	My First EFS File System

Aquí, le damos a asociar arriba a la derecha, esto nos dará un comando que debemos poner en la sesión ssh, solo necesitamos el cliente NFS:

Asociar

Monte el sistema de archivos de Amazon EFS en una instancia de Linux. [Más información](#)

☒ Montaje a través de DNS ☐ Montaje a través de IP

Mediante el asistente de montaje de EFS:

```
sudo mount -t efs -o tls fs-0aad5b5961308af11:/ efs
```

Mediante el cliente de NFS:

```
sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport fs-0aad5b5961308af11.efs.us-east-1.amazonaws.com:/ efs
```

[Consulte nuestra guía del usuario para obtener más información. Más información](#)

Cerrar

```
sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport fs-0aad5b5961308af11.efs.us-east-1.amazonaws.com:/ efs
```

Lo ponemos en la sesión ssh, además, podemos ver un resumen de los discos con el comando siguiente:

```
sudo df -hT
```

Vamos a examinar el comportamiento de rendimiento del nuevo sistema de archivos de EFS. Para ello, podemos hacer uso de Flexible IO(comando) o Amazon CloudWatch.

Flexible IO:

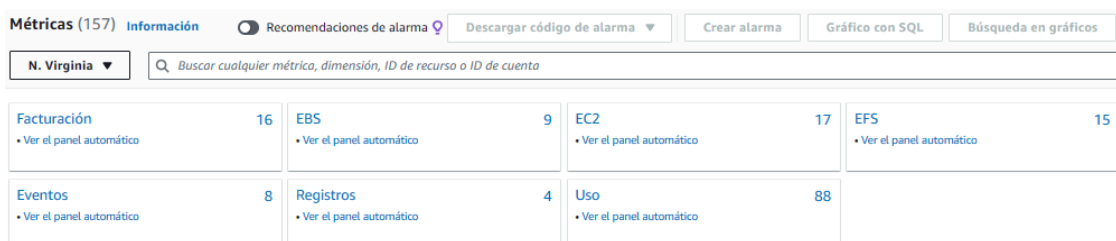
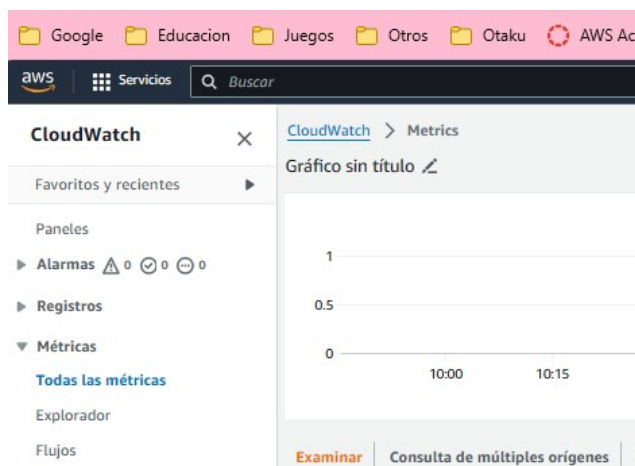
Ponemos el siguiente comando en la terminal:

```
sudo fio --name=fio-efs --filesize=10G --filename=./efs/fio-efs-test.img --bs=1M --nrfiles=1 --direct=1 --sync=0 --rw=write --iodepth=200 --ioengine=libaio
```

Este comando tardará de 5 a 10 minutos en completarse.

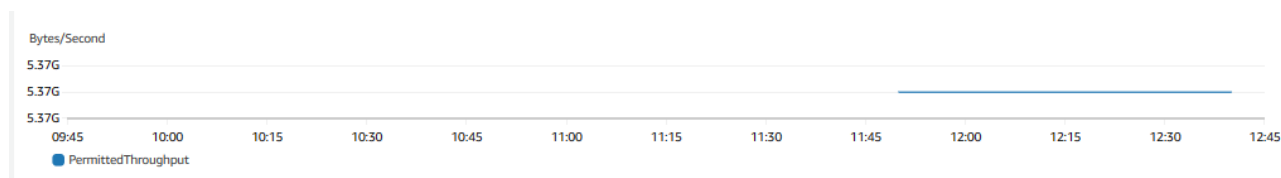
Amazon CloudWatch:

Abrimos el servicio CloudWatch y seleccionamos metricas:



Pulsamos en EFS y métricas del sistema de archivos. Por ultimo, buscamos esta coincidencia:

PermittedThroughput, la seleccionamos y el gráfico de arriba cambiará:



Y así varias cosas que podemos comprobar de nuestro sistema de archivos.