

# **Práctica 4.3**

Despliegue de una arquitectura  
EFS-EC2-MultiAZ

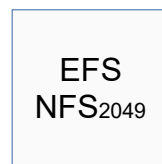
Guadalupe Luna  
Velázquez

## Índice

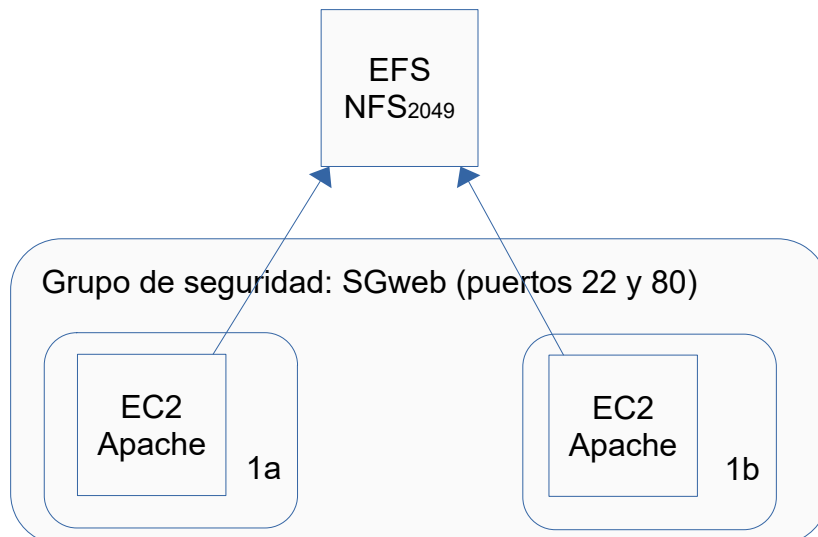
1. Despliegue.....	Página 3-4
2. Desarrollo del despliegue .....	Página 5-12
2.1 Creación de los grupos de seguridad .....	Página 5
2.2 Creación de las instancias nodos.....	Página 5-6
2.3 Creación del sistema de archivos.....	Página 7
2.4 Configuración de los servidores web.....	Página 8-10
2.5 Creación y configuración del balanceador.....	Página 12
2.6 Securización de los puertos.....	Página 13
3. Servicios y sus ventajas.....	Página 14

## 1. Despliegue

Crearemos en el servicio EFS un sistema de ficheros que será un sistema distribuido con un sistema NFS por el protocolo NFS y puerto 2049. Tendrá un grupo de seguridad con el puerto 2049 abierto y que solo puedan acceder las máquinas EC2 con apache para securizar todo.

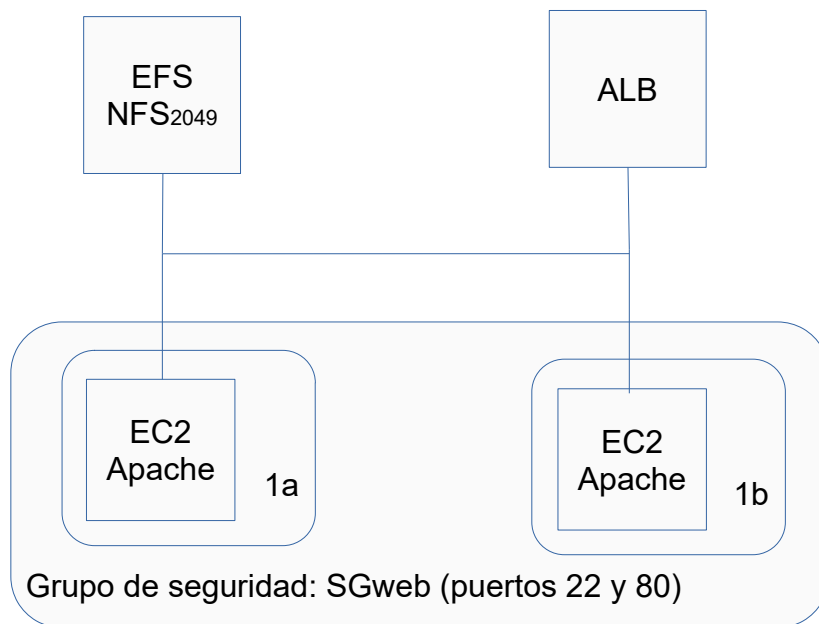


Una máquina EC2, que tenga instalado Apache en la zona 1a.  
Otra máquina EC2, que tenga instalado Apache en la zona 1b, que ambas configuradas para que sepan leer de la estructura de ficheros EFS, y con el puerto 22 y 80 abierto.



Con esto tendremos una página web estática de alta disponibilidad y Multi A-Z, por si se nos cae la zona de disponibilidad 1a trabajaría con la 1b y al contrario.

Además le añadiremos un balanceador de carga que será creado con una EC2 y se conectará a los servidores web para que distribuya automáticamente el tráfico.



Con esto ya estaría listo nuestro despliegue con su balanceador de carga que distribuya el tráfico de la red a los dos servidores web que hemos levantado, que están en diferentes zonas de disponibilidad, en la a y b, con apache instalado y operando, en estos servidores guardamos nuestra página web.

También tenemos un sistema de ficheros para que administre nuestros archivos e irá creciendo o disminuyendo en función de la cantidad de archivos que tengamos.

Tanto el balanceador de carga como el sistema de ficheros estarán securizados para que solo se pueda acceder desde la EC2.

Las EC2 también tendrán seguridad para que no se pueda modificar desde cualquier lado.

## 2. Desarrollo del despliegue

### 2.1 Creación de los grupos de seguridad

Para esta práctica primero en el servicio EC2, iremos a Grupos de Seguridad y creamos 2 grupos de seguridad, en uno lo llamaremos SGweb y abriremos el puerto 80, HTTP desde cualquier IPv4 y el puerto 22 de SSH por si hay que modificarlo, el otro se llamará SGEfs con el puerto 2049 de NFS para cualquier IPv4. Quedando así:

**Reglas de entrada** [Información](#)

ID de la regla del grupo de seguridad	Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>	Origen <a href="#">Información</a>	Descripción: opcional <a href="#">Información</a>
sgr-0dc20d5f3c4c15c79	HTTP	TCP	80	Anywh...	<div>Eliminar</div>
sgr-050887f1573039c1e	SSH	TCP	22	Persona...	<div>0.0.0.0/0 X</div> <div>Eliminar</div>

**Reglas de entrada** [Información](#)

ID de la regla del grupo de seguridad	Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>	Origen <a href="#">Información</a>	Descripción: opcional <a href="#">Información</a>
sgr-09baca571ea2999f3	NFS	TCP	2049	Persona...	<div>0.0.0.0/0 X</div> <div>Eliminar</div>

### 2.2 Creación de instancias nodos

Seguimos en el servicio EC2 y ahora creamos una EC2 que se llamará Linux\_01, con Amazon Linux, par de claves vockey, la VPC predeterminada pero elegimos la subred a, y permitimos que asigne una ip pública, se le asigna el grupo de seguridad que antes hemos creado con el nombre Sgweb.

**Nombre y etiquetas** [Información](#)

Nombre

Linux\_01

[Agregar etiquetas adicionales](#)

**▼ Imágenes de aplicaciones y sistemas operativos (Amazon Machine Image)** [Información](#)

Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones

Recientes

Inicio rápido

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

S

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

**▼ Configuraciones de red** [Información](#)

VPC - obligatorio [Información](#)

vpc-0270caa9ac719c077 (predeterminado)

172.31.0.0/16

Subred [Información](#)

subnet-05ffb64aba836cd47

VPC: vpc-0270caa9ac719c077 Propietario: 945659123201

Zona de disponibilidad: us-east-1a Direcciones IP disponibles: 4088

CIDR: 172.31.80.0/20

[Create new subnet](#)

Asignar automáticamente la IP pública [Información](#)

Habilitar

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

Grupos de seguridad comunes [Información](#)

Seleccionar grupos de seguridad

Sgweb sg-01d1344ca4cc3e4b9 X

VPC: vpc-0270caa9ac719c077

[Compare reglas de grupo de seguridad](#)

Los grupos de seguridad que agrega o elimine aquí se agregarán a todas las interfaces de red o se eliminarán de ellas.

Guadalupe Luna Velázquez  
Administración de Sistemas Informáticos en Red  
Gestión de Bases de Datos

En configuración avanzada introducimos los datos de usuario que se muestran a continuación:

```
#!/bin/bash
yum update -y
yum install httpd -y
systemctl start httpd
systemctl enable httpd
yum -y install nfs-utils
```

Datos de usuario - *optional* [Información](#)  
Enter user data in the field.

```
#!/bin/bash
yum update -y
yum install httpd -y
systemctl start httpd
systemctl enable httpd
yum -y install nfs-utils
```

▼ **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](#)

Y lanzamos la instancia, mientras crearemos otra instancia llamada Linux\_02, con la misma configuración Amazon Linux, par de claves vockey, VPC predeterminada pero con subred b y el mismo grupo de seguridad llamado SGweb y volvemos a configuración avanzada para pegar los datos de usuario, por último lanzamos la instancia.

Nombre  
Linux\_02 [Agregar etiquetas adicionales](#)

▼ **Imágenes de aplicaciones y sistemas operativos (Amazon Machine Image)** [Información](#)  
Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones

Recientes **Inicio rápido**

Amazon Linux macOS Ubuntu Windows Red Hat S [Browse more AMIs](#)  
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-0aa7d40eeae50c9a9 (64 bits (x86)) / ami-084237e82d7842286 (64 bits (Arm))  
Virtualización: hvm Habilitado para ENA: true Tipo de dispositivo raíz: ebs [Apto para la capa gratuita](#)

▼ **Configuraciones de red** [Información](#)

VPC - *obligatorio* [Información](#)  
vpc-0270caa9ac719c077 (predeterminado) [Actualizar](#)

Subred [Información](#)  
subnet-042924bd9752fb61e  
VPC: vpc-0270caa9ac719c077 Propietario: 945659123201  
Zona de disponibilidad: us-east-1b Direcciones IP disponibles: 4089  
CIDR: 172.31.16.0/20 [Create new subnet](#)

Asignar automáticamente la IP pública [Información](#)  
Habilitar

**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

**Grupos de seguridad comunes** [Información](#)  
Seleccionar grupos de seguridad

SGweb sg-01d1344ca4cc3e4b9 [X](#)  
VPC: vpc-0270caa9ac719c077 [Compare reglas de grupo de seguridad](#)

Los grupos de seguridad que agrega o elimine aquí se agregarán a todas las interfaces de red o se eliminarán de ellas.

Además creamos un par de ips elásticas para que al cerrar el laboratorio, esta no cambie, las creamos y las asociamos una por máquina.

## 2.3 Creación del Sistema de archivos

En el servicio EFS, vamos a crear un sistema de ficheros, llamado minfs y tendrá el VPC por defecto y elegimos la opción Estándar para que esté disponible en todas las zonas de disponibilidad.

Crear un sistema de archivos

Cree un sistema de archivos de EFS con la configuración recomendada por el servicio.  
[Más información](#)

Nombre - *opcional*

Asigne un nombre al sistema de archivos.

minfs

El nombre puede incluir letras, números y símbolos -, ., /, con un máximo de 256 caracteres.

Virtual Private Cloud (VPC)

Elija la VPC en la que desea que las instancias EC2 se conecten a su sistema de archivos. [Más información](#)

vpc-0270caa9ac719c077  
predeterminado

Clase de almacenamiento [Más información](#)

☒ Estándar  
Almacenar datos de forma redundante en varias zonas de disponibilidad

☐ Única zona  
Almacenar datos de forma redundante en una única zona de disponibilidad

Cancelar

Personalizar

Crear

Entramos en nuestro sistema de ficheros llamado minfs y accederemos a los grupos de seguridad y en todas las subredes le asignaremos el grupo de seguridad SGEfs.

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 por zona de disponibilidad. <a href="#">Más información</a>				
Zona de disponibilidad	ID de la subred	Dirección IP	Grupos de seguridad	
us-east-1a	subnet-05ffb64aba836cd47	172.31.86.102	<div>Elegir grupos de seguridad</div> <div>sg-02eba6e6d3c37f1ad X SGEfs</div>	Eliminar
us-east-1b	subnet-042924bd9752fb61e	172.31.23.3	<div>Elegir grupos de seguridad</div> <div>sg-02eba6e6d3c37f1ad X SGEfs</div>	Eliminar
us-east-1c	subnet-0b10926d1a2ab6d56	172.31.44.15	<div>Elegir grupos de seguridad</div> <div>sg-02eba6e6d3c37f1ad X SGEfs</div>	Eliminar
us-east-1d	subnet-0fafacea0bedd3ee4	172.31.2.93	<div>Elegir grupos de seguridad</div> <div>sg-02eba6e6d3c37f1ad X SGEfs</div>	Eliminar
us-east-1e	subnet-09889a5d757333603	172.31.51.90	<div>Elegir grupos de seguridad</div> <div>sg-02eba6e6d3c37f1ad X SGEfs</div>	Eliminar
us-east-1f	subnet-0999c3b9d7375e998	172.31.75.175	<div>Elegir grupos de seguridad</div> <div>sg-02eba6e6d3c37f1ad X SGEfs</div>	Eliminar

7

## 2.4 Configuración de los servidores web

Cuando se han terminado de crear, conectaremos a ellas donde podemos verificar que se haya instalado correctamente Apache y después de verificar entraremos en /var/www/html y crearemos una carpeta llamada efs-mount con el comando “mkdir efs-mount”.

```
[ec2-user@ip-172-31-94-123 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
  Drop-In: /usr/lib/systemd/system/httpd.service.d
           └─php-fpm.conf
   Active: active (running) since Fri 2023-02-10 15:02:25 UTC; 29min ago
     Docs: man:httpd.service(8)
  Main PID: 3149 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    CGroup: /system.slice/httpd.service
            └─3149 /usr/sbin/httpd -DFOREGROUND
              └─3161 /usr/sbin/httpd -DFOREGROUND
                └─3162 /usr/sbin/httpd -DFOREGROUND
                  └─3163 /usr/sbin/httpd -DFOREGROUND
                    └─3164 /usr/sbin/httpd -DFOREGROUND
                      └─3165 /usr/sbin/httpd -DFOREGROUND

Feb 10 15:02:25 ip-172-31-94-123.ec2.internal systemd[1]: Starting The Apache HTTP Server...
Feb 10 15:02:25 ip-172-31-94-123.ec2.internal systemd[1]: Started The Apache HTTP Server.
[ec2-user@ip-172-31-94-123 ~]$ cd /var/www/html
[ec2-user@ip-172-31-94-123 html]$ mkdir efs-mount
```

Ahora vamos a utilizar el comando para montar en un sistema nfs sobre la carpeta que hemos creado, y ejecutamos el comando cambiando el id por el nuestro.

“sudo mount -t nfs -o  
nfsvers=4.1,rsiz=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport fs-  
0b3af357a01238bb9.efs.us-east-1.amazonaws.com:/ efs-mount”.

Ahora con otro comando nos descargaremos la página web:

“wget https://s3.eu-west-1.amazonaws.com/www.profesantos.cloud/Netflix.zip”, lo descomprimos con el comando “unzip Netflix.zip” y ya estaría la página web.

```
[ec2-user@ip-172-31-94-123 efs-mount]$ wget https://s3.eu-west-1.amazonaws.com/www.profesantos.cloud/Netflix.zip
--2023-02-10 15:56:36-- https://s3.eu-west-1.amazonaws.com/www.profesantos.cloud/Netflix.zip
Resolving s3.eu-west-1.amazonaws.com (s3.eu-west-1.amazonaws.com)... 52.218.42.11, 52.218.62.35, 52.218.89.139, ...
Connecting to s3.eu-west-1.amazonaws.com (s3.eu-west-1.amazonaws.com)|52.218.42.11|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1993 (1.9K) [application/zip]
Netflix.zip: Permission denied

Cannot write to 'Netflix.zip' (Success).
[ec2-user@ip-172-31-94-123 efs-mount]$ sudo wget https://s3.eu-west-1.amazonaws.com/www.profesantos.cloud/Netflix.zip
--2023-02-10 15:56:44-- https://s3.eu-west-1.amazonaws.com/www.profesantos.cloud/Netflix.zip
Resolving s3.eu-west-1.amazonaws.com (s3.eu-west-1.amazonaws.com)... 52.218.45.32, 52.218.57.3, 52.218.96.18, ...
Connecting to s3.eu-west-1.amazonaws.com (s3.eu-west-1.amazonaws.com)|52.218.45.32|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1993 (1.9K) [application/zip]
Saving to: 'Netflix.zip'

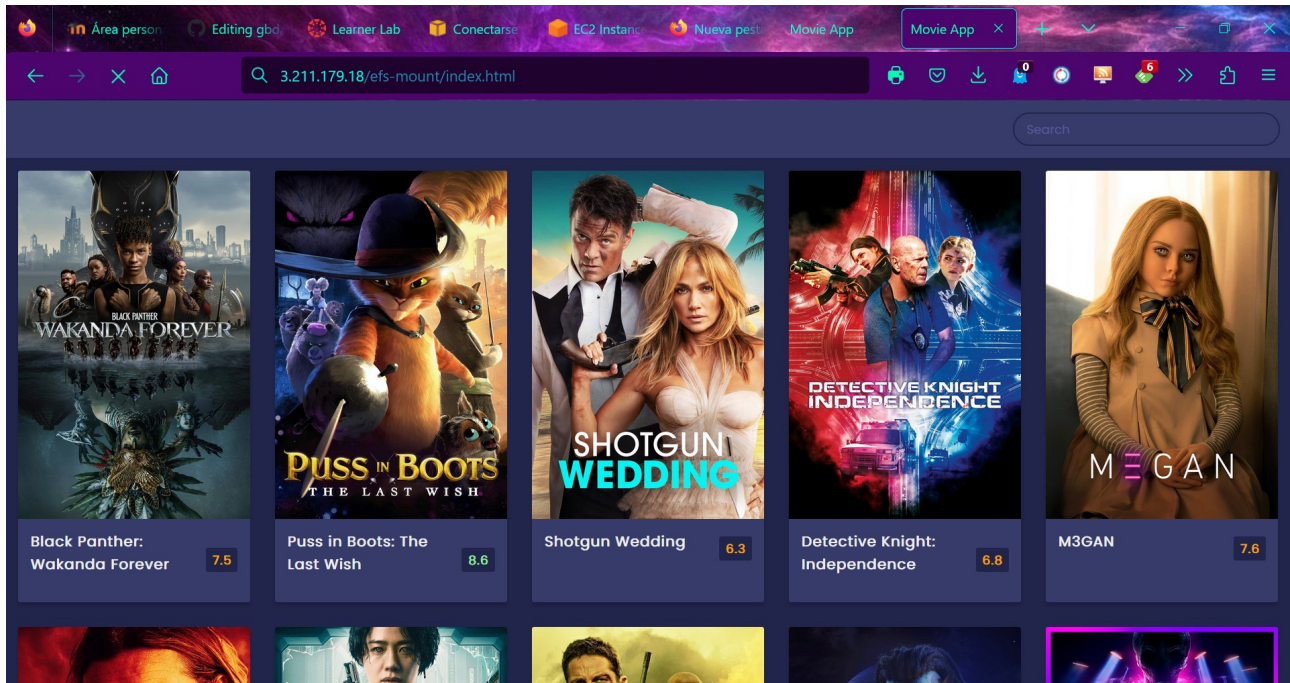
100%[=====>] 1,993 --.-K/s in 0s

2023-02-10 15:56:45 (27.5 MB/s) - 'Netflix.zip' saved [1993/1993]

[ec2-user@ip-172-31-94-123 efs-mount]$ sudo unzip Netflix.zip
Archive:  Netflix.zip
  inflating: index.html
  inflating: script.js
  inflating: style.css
[ec2-user@ip-172-31-94-123 efs-mount]$
```



Estos pasos también los hacemos en la segunda máquina EC2 para así que se vea la misma página web en los dos servidores. Si buscamos nuestra ip en internet y en la ruta accedemos al html de la página web se visualizará.



Ahora vamos a modificar el archivo de Apache para simplemente acceder a la página con nuestra ip.

Así que modificaremos el archivo `/etc/httpd/conf/httpd.conf` con “sudo nano” o “vim” y modificaremos el DocumentRoot a DocumentRoot `"/var/www/html/efs-mount"`, y después reiniciaremos el servicio httpd con “systemctl restart httpd”, esto se hará en los dos servidores.

```
GNU nano 2.9.8 /etc/httpd/conf/httpd.conf

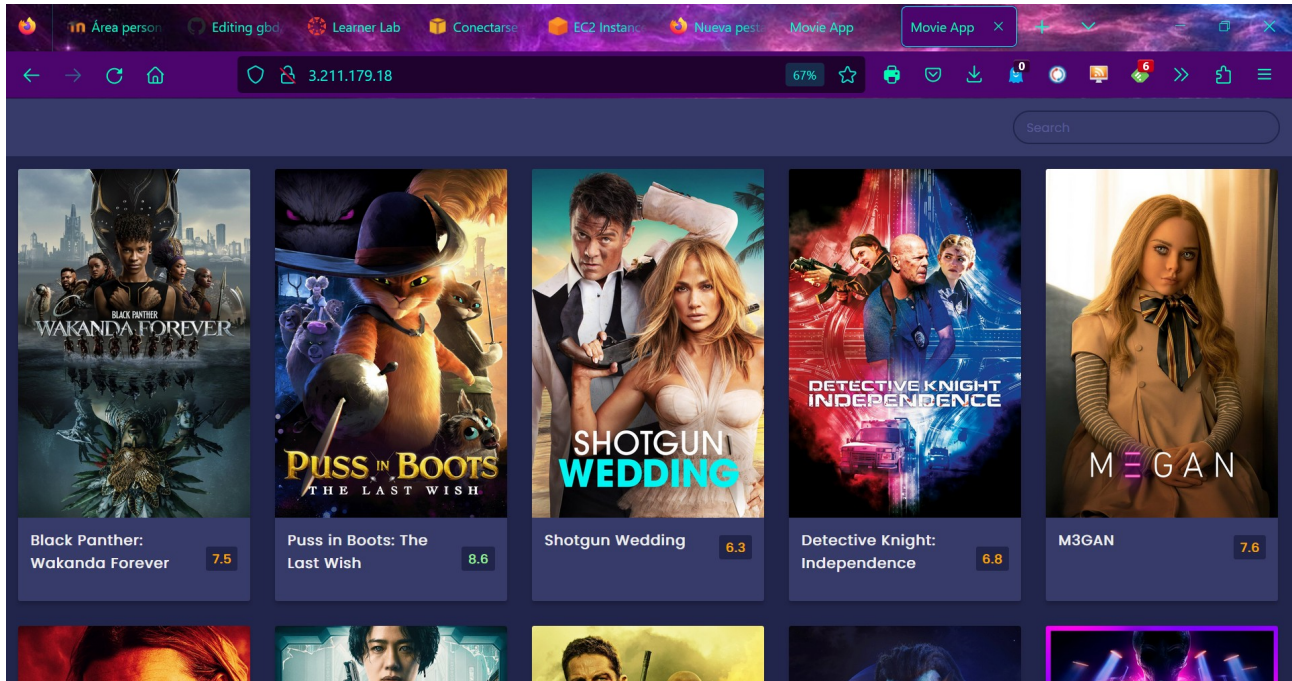
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html/efs-mount"
#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    # Require all granted
</Directory>

# Further relax access to the default document root:
```

Guadalupe Luna Velázquez  
Administración de Sistemas Informáticos en Red  
Gestión de Bases de Datos

Con esto ya estaría los servidores web configurados y si ponemos simplemente la ip de los servidores nos mostrará la página web.



## 2.5 Creación y configuración del balanceador

Creamos otra EC2 más para hacer nuestro balanceador, se llamará Balanceador\_Linux, con sistema Ubuntu, con par de claves vockey y le creamos un nuevo grupo de seguridad, donde abriremos los puertos SSH, HTTP y HTTPS. También le asignaremos una ip elástica como a los nodos y se la asociaremos.

**Nombre y etiquetas** [Información](#)

Nombre

Balanceador\_Linux

[Agregar etiquetas adicionales](#)

**▼ Imágenes de aplicaciones y sistemas operativos (Amazon Machine Image)** [Información](#)

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones

Recientes

Inicio rápido

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu®

Windows

Microsoft

Red Hat

RedHat

S

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-00874d747d0e814fa (64 bits (x86)) / ami-016250e155ee390e9 (64 bits (Arm))

Virtualización: hvm Habilitado para ENA: true Tipo de dispositivo raíz: ebs

Apto para la capa gratuita

**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

Crearemos un nuevo grupo de seguridad denominado "launch-wizard-4" con las siguientes reglas:

☒ Permitir el tráfico de SSH desde

Ayuda a establecer conexión con la instancia

Cualquier lugar

0.0.0.0/0

☒ Permitir el tráfico de HTTPS desde Internet

Para configurar un punto de enlace, por ejemplo, al crear un servidor web

☒ Permitir el tráfico de HTTP desde Internet

Para configurar un punto de enlace, por ejemplo, al crear un servidor web

⚠ Las reglas con la fuente 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia. ✕

Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

10

Cuando se cree el balanceador, nos conectaremos a él e instalaremos Apache con "sudo apt install apache2", también debemos reiniciar el servicio con el comando "sudo systemctl restart apache2".

```
ubuntu@ip-172-31-88-249:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser bzip2-doc
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap mime-support
  ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 87 not upgraded.
Need to get 2138 kB of archives.
After this operation, 8501 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 libapr1 amd64 1.7.0-8build1 [107 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4 [92.4 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-5ubuntu4 [11.3 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 libaprutil1-ldap amd64 1.6.1-5ubuntu4 [9162 B]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 liblua5.3-0 amd64 5.3.6-1build1 [140 kB]
```

A continuación, editamos el fichero /etc/apache2/sites-enabled/000-default.conf para configurar nuestro gestor de balanceo y pondremos lo siguiente:

```
ProxyPass /balancer-manager !

<Proxy balancer://Balanceador_Linux>
    # Server 1
    BalancerMember http://172.31.94.123

    # Server 2
    BalancerMember http://172.31.26.236
</Proxy>
ProxyPass / balancer://Balanceador_Linux/
ProxyPassReverse / balancer://Balanceador_Linux/

<Location /balancer-manager>
    SetHandler balancer-manager
    Order Deny,Allow
    Allow from all
</Location>
```

```
GNU nano 6.2 /etc/apache2/sites-enabled/000-default.conf
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

ProxyPass /balancer-manager !

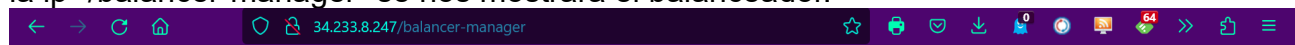
<Proxy balancer://Balanceador_Linux>
    # Server 1
    BalancerMember http://172.31.94.123

    # Server 2
    BalancerMember http://172.31.26.236
</Proxy>

ProxyPass / balancer://Balanceador_Linux/
ProxyPassReverse / balancer://Balanceador_Linux/

<Location /balancer-manager>
    SetHandler balancer-manager
    Order Deny,Allow
    Allow from all
</Location>
```

Tras esto reiniciaremos Apache de nuevo con "sudo systemctl restart apache2" y al buscar la ip de nuestro balanceador saldrá la página web, si ponemos a continuacion de la ip "/balancer-manager" se nos mostrará el balanceador.



## Load Balancer Manager for 34.233.8.247

Server Version: Apache/2.4.52 (Ubuntu)  
Server Built: 2023-01-23T18:34:42  
Balancer changes will NOT be persisted on restart.  
Balancers are inherited from main server.  
ProxyPass settings are inherited from main server.

### LoadBalancer Status for [balancer://balanceador\\_linux](http://34.233.8.247/balancer-manager) [p1c2996fe\_balanceador\_linux]

MaxMembers	StickySession	DisableFailover	Timeout	FailoverAttempts	Method	Path	Active
2 [2 Used]	(None)	Off	0	1	byrequests	/	Yes

Worker URL	Route	RouteRedir	Factor	Set	Status	Elected	Busy	Load	To	From
<a href="http://172.31.94.123">http://172.31.94.123</a>			1.00	0	Init Ok	3	0	-100	1.6K	2.8K
<a href="http://172.31.26.236">http://172.31.26.236</a>			1.00	0	Init Ok	2	0	100	1.0K	2.0K

Apache/2.4.52 (Ubuntu) Server at 34.233.8.247 Port 80

Con esto el balanceador funciona y si en algún momento se cae un nodo, el otro seguiría mostrando la página web.

## 2.7 Securización de los puertos

Por último, debemos proteger y securizar el puerto 80 de los nodos que contienen la página Web para que solo se puedan acceder por el balanceador y no estén expuestos al público.

Iremos al grupo de seguridad de estos que es el SGWeb y en la regla HTTP, en vez de Anywhere IPv4, pondremos la ip privada del balanceador.

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 <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>	Origen <a href="#">Informición</a>	Descripción: opcional <a href="#">Información</a>
sgr-07e33ace37ec9cc5d	RDP	TCP	3389	Persona... <input type="text" value="0.0.0.0/0"/>	<input type="text"/> <input type="button" value="Eliminar"/>
sgr-0dc20d5f3c4c15c79	HTTP	TCP	80	Persona... <input type="text" value="172.31.4.247/32"/>	<input type="text"/> <input type="button" value="Eliminar"/>
sgr-050887f1573039c1e	SSH	TCP	22	Persona... <input type="text" value="0.0.0.0/0"/>	<input type="text"/> <input type="button" value="Eliminar"/>

Agregar regla

Aun modificando esto nuestra página web se verá igual de bien y no será tan fácilmente accesible.

### **3. Servicios y sus Ventajas**

El servicio que se utilizará será EC2 principalmente para crear las instancias que tienen instalado Apache que servirán como servidores web, las ventajas de usar este servicio es que es fácil de manejar y presenta muchas opciones muy útiles para crear infraestructuras, al añadir una ip elástica, crear y modificar al gusto los grupos de seguridad, se pueden crear varias instancias con especificar la configuración en una sola vez, también su fácil conexión a la instancia a través de SSH.

Además este servicio ofrece una gran escalabilidad lo que nos permitiría añadir servidores web o lo que fuera necesario en caso de necesitar ampliar el despliegue o añadir más funciones, también ha hecho posible darle a nuestro despliegue la gran disponibilidad que ofrece.

Este servicio también se ha usado para crear el balanceador de carga con el que conseguimos distribuir el tráfico de red

También utilizaremos el servicio EFS para crear un sistema de ficheros que montaremos en nuestro servidor web, este servicio nos ha permitido crearlo fácil y rápidamente sin tener muchos conocimientos sobre ellos y configurarlo a nuestra manera decidiendo las zonas de disponibilidad y administrándolas conjuntamente con el servicio EC2.

Este servicio es una manera segura y fiable de acceder a nuestros archivos creando un sistema de archivos completamente administrado y diseñado que también contará con gran durabilidad y disponibilidad.