



# DESPLIEGUE DE APLICACIÓN WEB EN SERVIDOR AWS

Jose Almiron Lopez

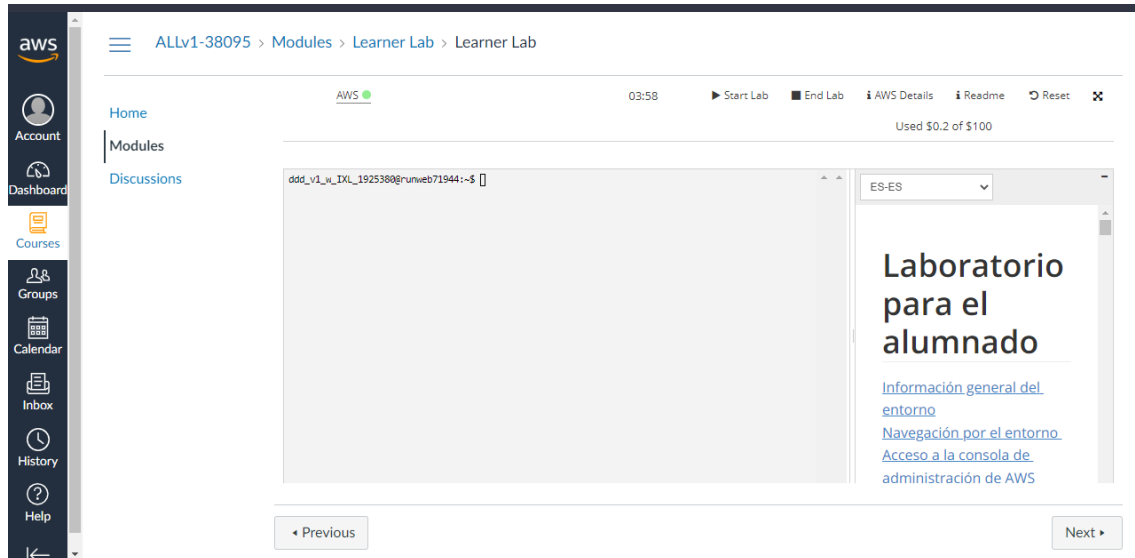
## Contenido

|  |    |
|--|----|
| Acceso AWS y creación de instancia AWS EC2.....  | 2  |
| Instalación de componentes para el despliegue, prueba local y gestión de posibles errores..... | 8  |
| Configuraciones de acceso remoto y pruebas de autenticación al Servidor AWS .....              | 13 |
| Extra: creación del certificado SSL para mejorar la seguridad .....                            | 15 |

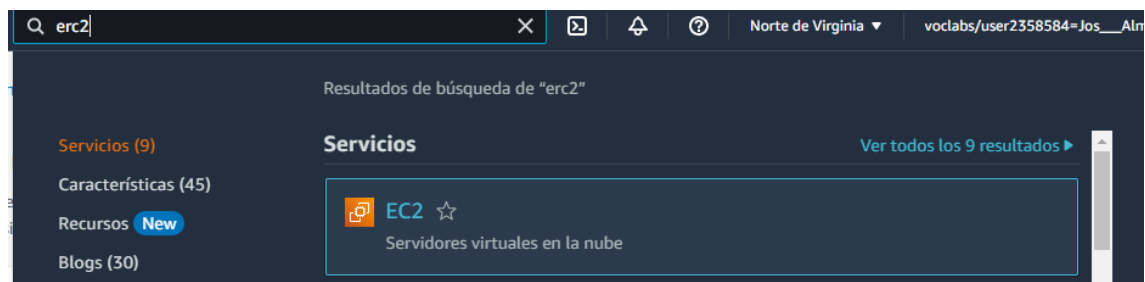
## Acceso AWS y creación de instancia AWS EC2

El repositorio de GitHub donde está el proyecto es [projectAWS](#)

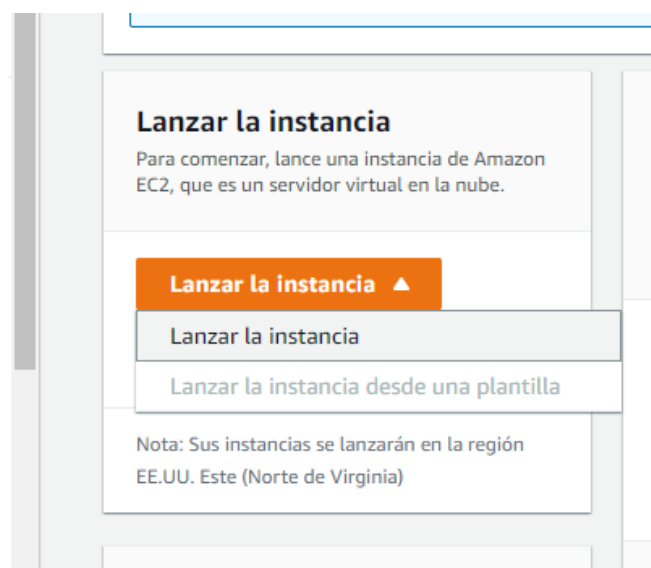
Una vez hemos accedido a la plataforma de AWS nos dirigiremos a Modules > Learner Lab, con esto iniciaremos el laboratorio de prueba, le daremos click a start Lab si fuera necesario



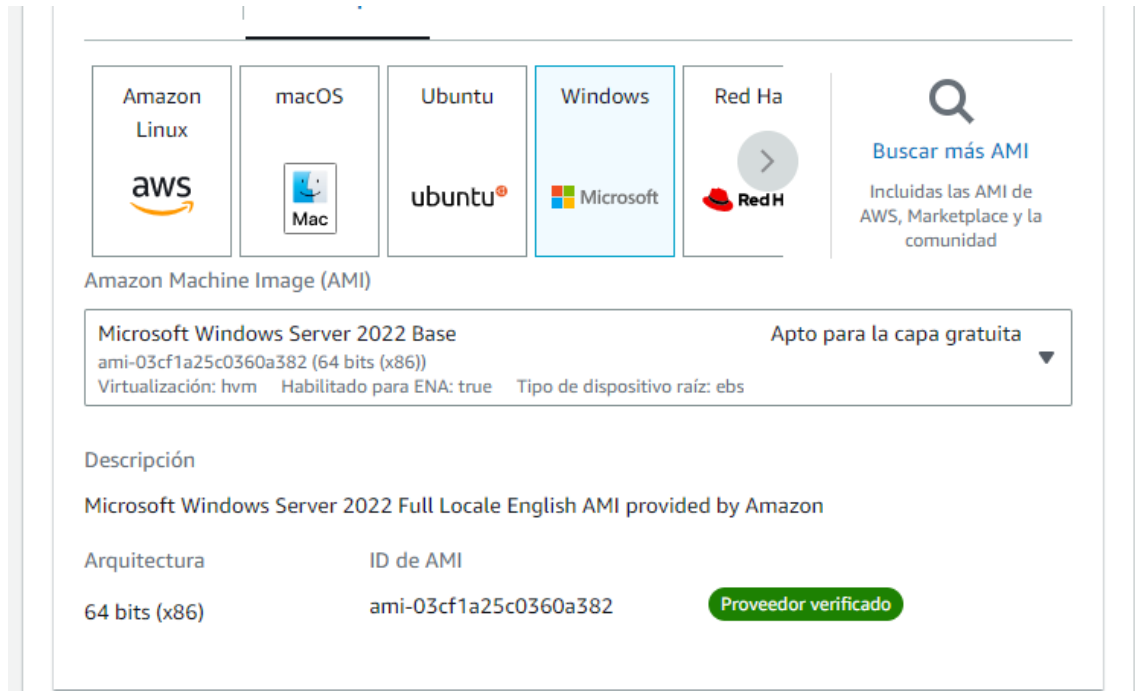
Pulsando en las letras AWS que salen encima de la terminal nos redirige a una web de administración de la consola, bajamos hasta la opción de crear una solución y pulsamos en lanzar una máquina virtual. En la barra de búsqueda buscamos EC2



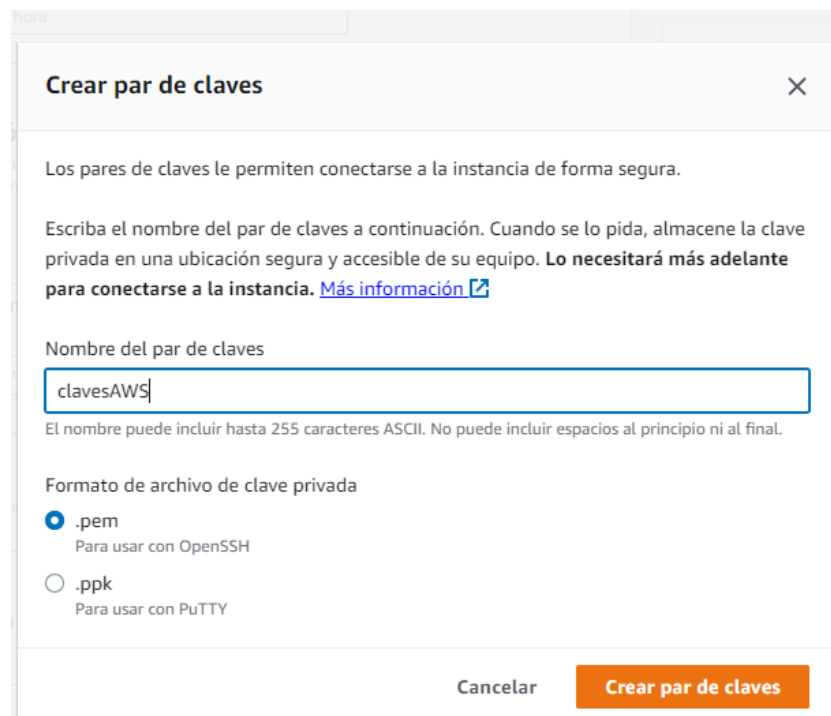
Buscamos la opción de lanzar instancia



Nos saldrá una lista de opciones entre ellas el nombre de la instancia, que la llamaremos Sistema operativo. En selección de imagen seleccionáramos un Windows server 2022 con la capa gratuita



Pulsamos sobre crear par de claves y generaremos un par de claves .pem



Quedando de la siguiente manera

**▼ 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*

[Crear un nuevo par de claves](#)

Para las instancias de Windows, utilice un par de claves para descifrar la contraseña del administrador y, a continuación, utilice la contraseña descifrada para conectarse a la instancia.

En la configuración de red confirmamos que la subred está habilitada y asignar automáticamente IP pública, en las reglas de seguridad habilitamos rdp, ssh, httpy https, dejamos la configuración de almacenamiento

Reglas de entradaReglas de salidaEtiquetas

Ahora puede comprobar la conectividad de red con Reachability Analyzer

Ejecutar Reachability Analyzer

Reglas de entrada (5)

Filtrar reglas de grupo de seguridad

<1>

| <input type="checkbox"/> | Name | ID de la regla del g... | Versión de IP | Tipo          | Protocolo | Intervalo de |
|--------------------------|------|-------------------------|---------------|---------------|-----------|--------------|
| <input type="checkbox"/> | -    | sgr-03d0dad3c90a8fc5d   | IPv4          | SSH           | TCP       | 22           |
| <input type="checkbox"/> | -    | sgr-0b7542c2fb302a3c4   | IPv4          | HTTP          | TCP       | 80           |
| <input type="checkbox"/> | -    | sgr-0c08cfbe45fe421d2   | IPv4          | HTTPS         | TCP       | 443          |
| <input type="checkbox"/> | -    | sgr-0299792b8c4bc39...  | IPv4          | RDP           | TCP       | 3389         |
| <input type="checkbox"/> | -    | sgr-0dd046844b5d4d...   | IPv4          | Todos los TCP | TCP       | 0 - 65535    |

Una vez realizadas todas las configuraciones procedemos a lanzar la instancia

awsServiciosBúsqueda[Alt+S]Norte de Virginiavoclabs/user2358584=Jos\_\_\_Almir\_n @ 7806-3954-7360

EC2 > Instancias > Lanzar una instancia

✓ Correcto

El lanzamiento de la instancia se inició correctamente (i-Ofc69e3b5610a4cf6)

▼ Registro de lanzamiento

Inicialización de solicitudes

Se realizó correctamente

Creación de grupos de seguridad

Se realizó correctamente

Creación de reglas de grupo de seguridad

Se realizó correctamente

Inicio del lanzamiento

Se realizó correctamente

Detalles de la instancia

## Despliegue de aplicación web en Servidor AWS

The screenshot shows the 'Resumen de instancia de i-080a1c3ad0f5531d6 (Sistema operativo)' page in the AWS Management Console. The instance is in the 'En ejecución' (Running) state. Key details include:

- ID de la instancia:** i-080a1c3ad0f5531d6 (Sistema operativo)
- Dirección IPv4 pública:** 3.83.114.51 | [dirección abierta](#)
- Direcciones IPv4 privadas:** 172.31.93.89
- DNS de IPv4 pública:** ec2-3-83-114-51.compute-1.amazonaws.com | [dirección abierta](#)
- Tipo de instancia:** t2.micro
- ID de VPC:** vpc-026ef1e01c2301c1d
- ID de subred:** subnet-0286d90d5a487a065

At the bottom, there are tabs for 'Detalles', 'Seguridad', 'Redes', 'Almacenamiento', 'Comprobaciones de estado', 'Monitoreo', and 'Etiquetas'.

Ejecutamos la instancia pulsando sobre el menú de acciones y damos en conectar, vamos a la pestaña de cliente DRP y descargamos el archivo de escritorio remoto, obtenemos el usuario y la contraseña que nos saldrá más debajo de la pagina

The screenshot shows the 'Tipo de conexión' (Connection type) page in the AWS Management Console. It provides instructions on how to connect to the instance:

- Conectarse mediante el cliente de RDP:** Descargue un archivo para usarlo con el cliente de RDP y recupere la contraseña.
- Conectarse mediante Fleet Manager:** Para conectarse a la instancia mediante el escritorio remoto de Fleet Manager, SSM Agent debe estar instalado y en ejecución en la instancia. Para obtener más información, consulte [Trabajo con SSM Agent](#).

Para conectarse a la instancia de Windows, puede utilizar el cliente de escritorio remoto que elija, así como descargar y ejecutar el archivo de acceso directo de RDP que se indica a continuación:

[Descargar archivo de escritorio remoto](#)

Cuando se lo pidan, conéctese a la instancia utilizando los siguientes datos:

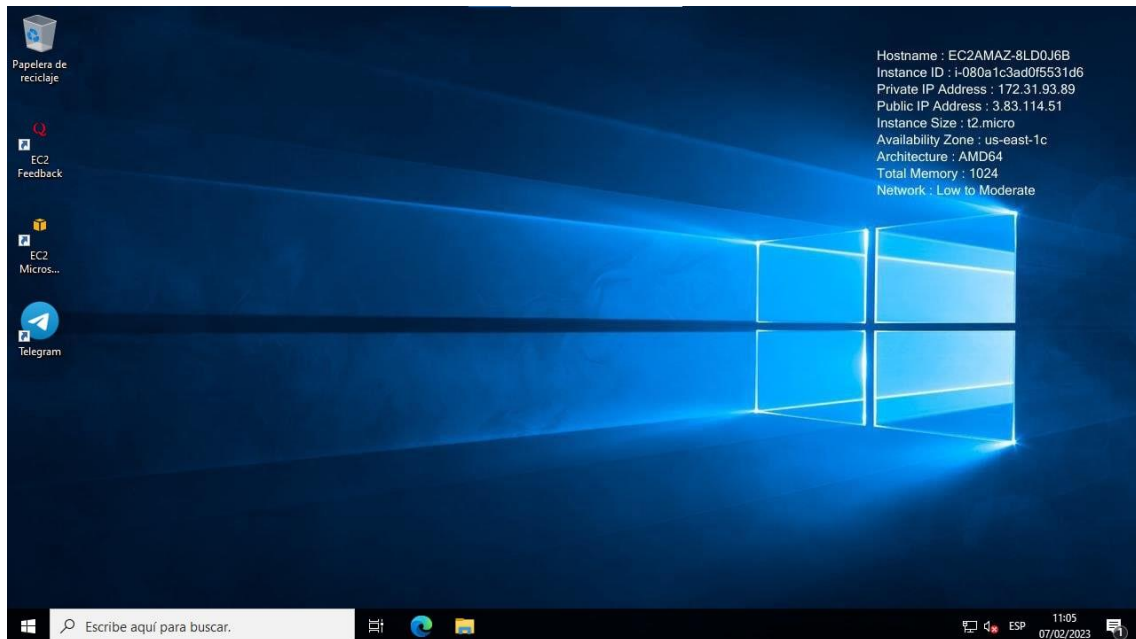
| Public DNS                              | Nombre de usuario |
|---|-------------------|
| ec2-3-83-114-51.compute-1.amazonaws.com | Administrator     |

Contraseña [Obtener contraseña](#)

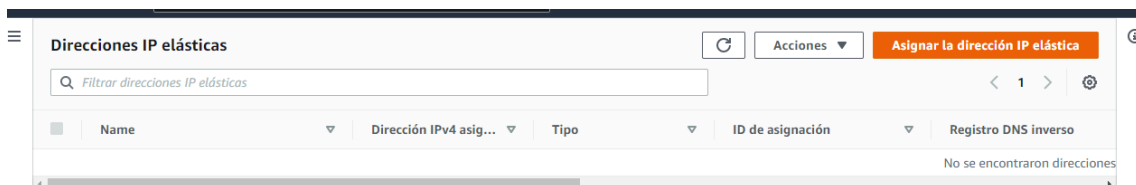
Si ha unido su instancia a un directorio, puede utilizar las credenciales del directorio para conectarse a la instancia.

[Cancelar](#)

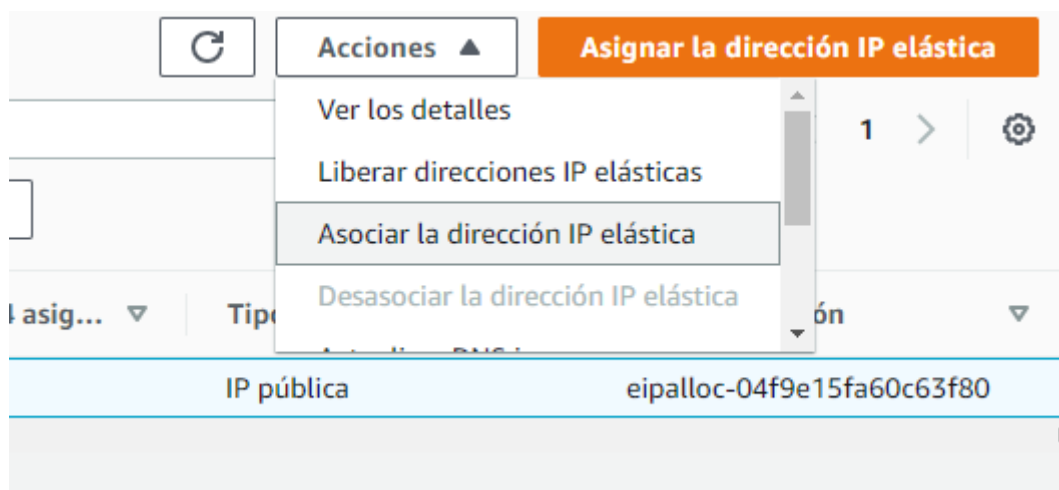
Una vez estemos en obtener contraseña, cargamos el fichero .pem que contiene las claves y pulsamos sobre el botón descifrar. Una vez hecho esto desde la aplicación que se nos ha descargado de escritorio remoto, rellenaremos los datos de login y se nos lanzara la máquina virtual de Windows server



Creamos una IP elástica, esto lo encontraremos en la configuración de red



Dejamos todo por defecto y la asociamos a la instancia que habíamos creado anteriormente



## Asociar la dirección IP elástica

Elegir la instancia o la interfaz de red que se desea asociar a esta dirección IP elástica (52.202.26.54)

### Dirección IP elástica: 52.202.26.54

#### Tipo de recurso

Elija el tipo de recurso al que desea asociar la dirección IP elástica.

- ☒ Instancia  
☐ Interfaz de red

**⚠** Si asocia una dirección IP elástica a una instancia que ya tiene asociada una dirección de este tipo, esa dirección IP elástica anterior se desasociará, pero aun así se asignará a su cuenta. [Más información](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

#### Instancia

#### Dirección IP privada

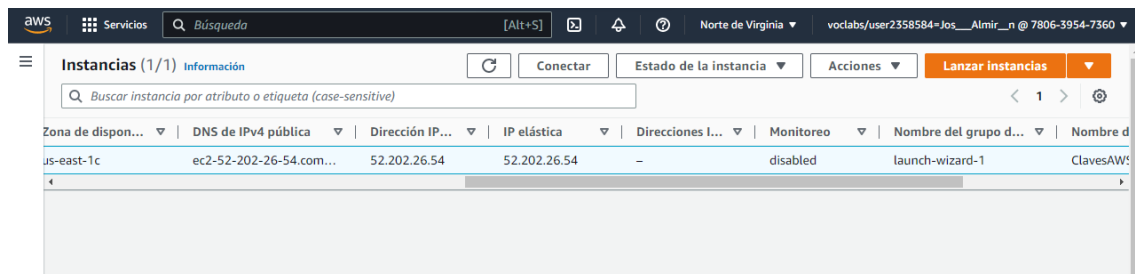
La dirección IP privada a la que desea asociar la dirección IP elástica.

#### Nueva asociación

Especifique si la dirección IP elástica se puede volver a asociar a un recurso diferente en el caso de que ya exista otra asociación.

☐ Permitir que se vuelva a asociar esta dirección IP elástica

Como podemos ver ya tenemos la IP elástica asociada a la instancia



| Zona de dispon... | DNS de IPv4 pública     | Dirección IP... | IP elástica  | Direcciones I... | Monitoreo | Nombre del grupo d... | Nombre d  |
|-------------------|-------------------------|-----------------|--------------|------------------|-----------|-----------------------|-----------|
| us-east-1c        | ec2-52-202-26-54.com... | 52.202.26.54    | 52.202.26.54 | -                | disabled  | launch-wizard-1       | ClavesAW! |

Para configurar el firewall local, nos dirigimos al servidor y una vez en el panel de control > sistema y seguridad > firewall de Windows defender > configuración avanzada. Aquí podremos gestionar tanto las reglas de entrada como de salida. Podemos abrir puertos tanto de forma gráfica o por comandos de PowerShell, abrimos los puertos 80, 443 y 22, el puerto RDP viene abierto por defecto

***New-NetFirewallRule -DisplayName "ALLOW TCP PORT 80" -Direction inbound -Profile Any -Action Allow -LocalPort 80 -Protocol TCP***



## Despliegue de aplicación web en Servidor AWS

```
Administrador: Windows PowerShell
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName "ALLOW TCP PORT 22" -Direction inbound -Profile Any -Action Allow -LocalPort 22 -Protocol TCP

Name
: {a0e19712-4011-4042-b000-cc85052ff359}
DisplayName
: ALLOW TCP PORT 22
Description
:
DisplayGroup
:
Group
:
Enabled
: True
Profile
: Any
Platform
: {}
Direction
: Inbound
Action
: Allow
EdgeTraversalPolicy
: Block
LooseSourceMapping
: False
LocalOnlyMapping
: False
Owner
:
PrimaryStatus
: OK
Status
: Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus
: NotApplicable
PolicyStoreSource
: PersistentStore
PolicyStoreSourceType
: Local
RemoteDynamicKeywordAddresses
: {}

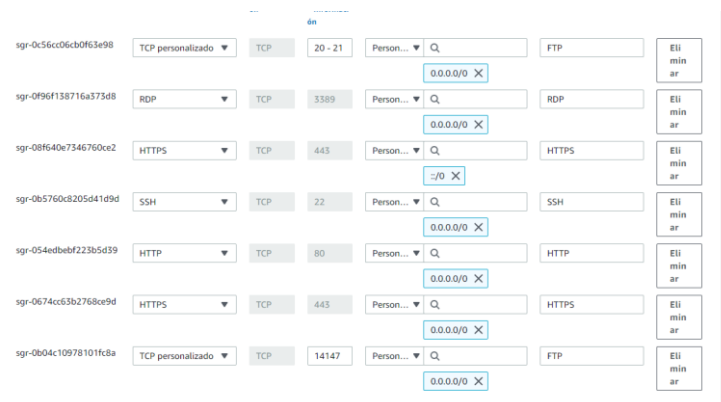
PS C:\Users\Administrator>
```



## Instalación de componentes para el despliegue, prueba local y gestión de posibles errores

Tenemos que instalar XAMPP desde su web oficial, la instalación es como cualquier instalación de Windows con todo por defecto, una vez termine configuraremos el acceso por FTP para poder subir los ficheros de la web

Para poder conectar por medio de FTP debemos modificar las reglas de seguridad nos dirigimos a la instancia, seguridad buscamos grupos de seguridad y nos saldrá una web donde modificar las reglas de entrada, añadiremos para el puerto 14147 y el rango de 20-21, que son los puertos en los que escucha FTP

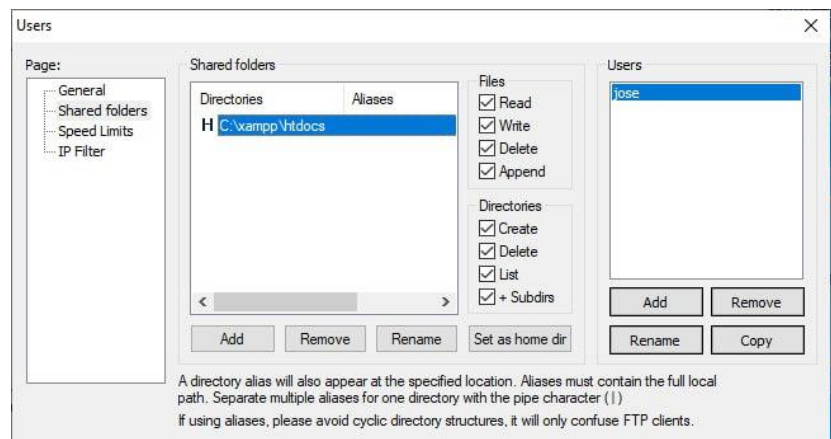
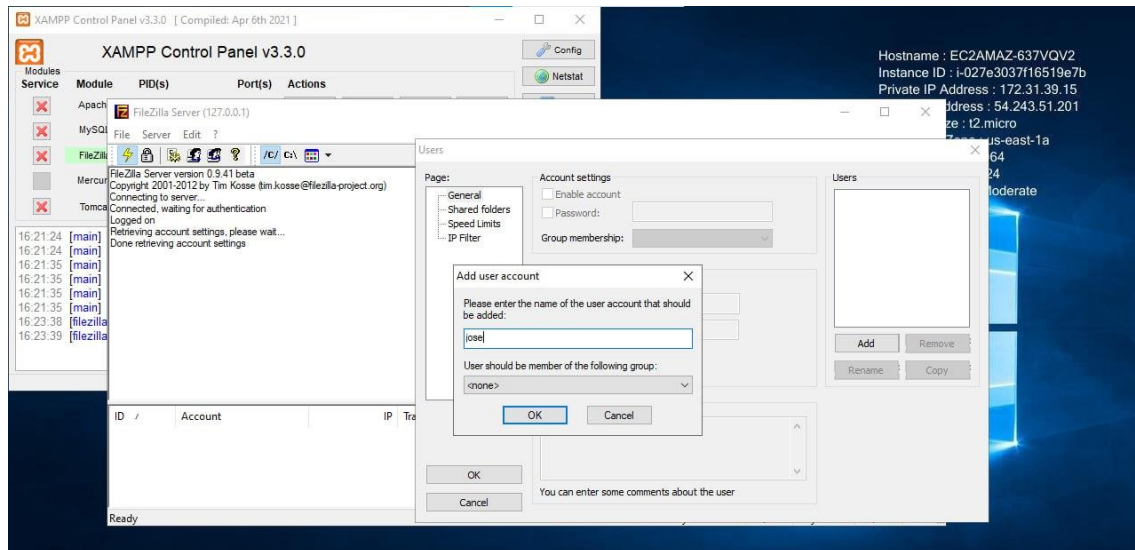


En el servidor también debemos abrir esos puertos como ya vimos anteriormente

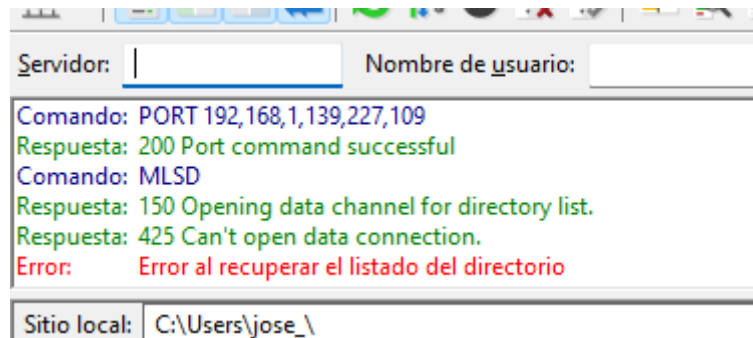
## Despliegue de aplicación web en Servidor AWS



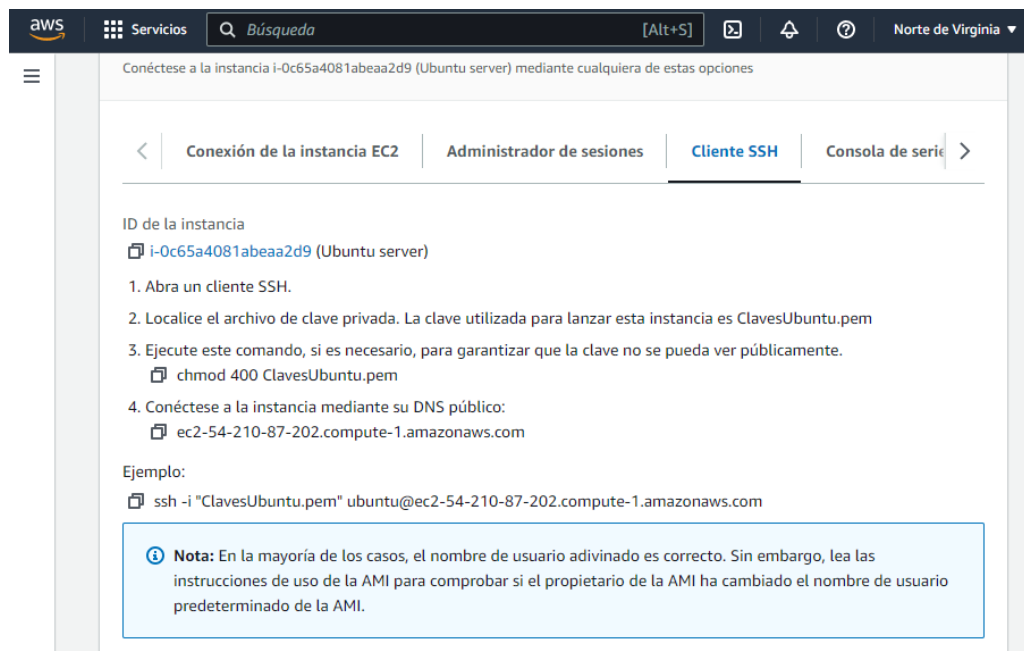
Una vez abiertos los puertos, ejecutamos XAMPP, activamos el servicio de FileZilla que nos proporciona y creamos un usuario que será el que tenga acceso por medio de FTP a la carpeta htdocs de ZAMPP donde se alojaran los ficheros de la web



Cuando intento probar la conexión desde el local no he tenido problema, pero desde mi equipo no he podido conectarme



He tenido problemas usando la instancia de Windows server, he abierto los puertos desde el firewall de Windows y desde AWS, pero no he conseguido conectarme por SSH y FTP, solo he podido acceder al puerto 80. He creado una instancia esta vez usando Ubuntu siguiendo los pasos anteriores, creando otro par de claves y asignándole otra dirección ip elástica, una vez realizado todo esto ya podremos conectar por SSH



Probamos la conexión por medio de SSH

## Despliegue de aplicación web en Servidor AWS

```
ubuntu@ip-172-31-84-116: ~  
C:\Users\jose_\Downloads>ssh -i "ClavesUbuntu.pem" ubuntu@ec2-54-210-87-202.compute-1.amazonaws.com  
The authenticity of host 'ec2-54-210-87-202.compute-1.amazonaws.com (54.210.87.202)' can't be established.  
ED25519 key fingerprint is SHA256:fb28IY2qTSqP9yXgtSwIZyQ4TIkCI1QqCW6AqsoC3+s.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'ec2-54-210-87-202.compute-1.amazonaws.com' (ED25519) to the list of known hosts.  
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1028-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Tue Feb  7 12:28:48 UTC 2023  
  
System load:  0.658203125      Processes:            102  
Usage of /:   19.6% of 7.57GB   Users logged in:     0  
Memory usage: 20%             IPv4 address for eth0: 172.31.84.116  
Swap usage:   0%  
  
0 updates can be applied immediately.  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

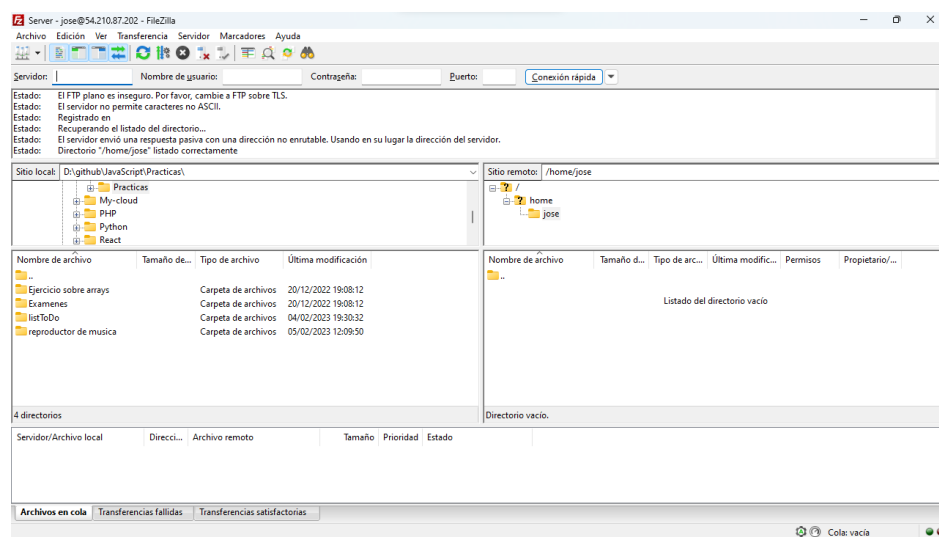
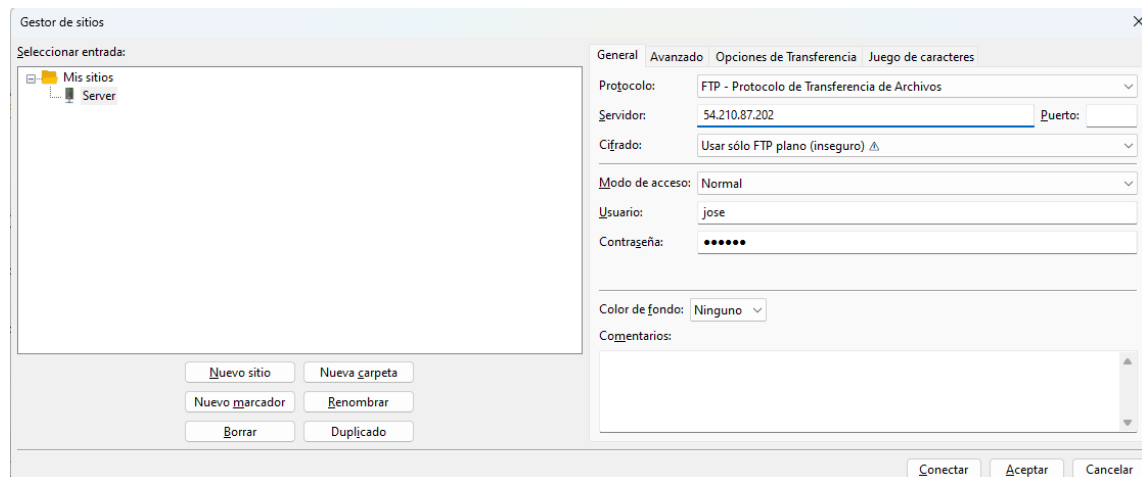
Lo primero que hare será crear un usuario, este usuario será el que tenga acceso a FTP

```
ubuntu@ip-172-31-84-116: ~  
ubuntu@ip-172-31-84-116:~$ sudo useradd -m jose  
ubuntu@ip-172-31-84-116:~$ sudo passwd jose  
New password:  
Retype new password:  
passwd: password updated successfully  
ubuntu@ip-172-31-84-116:~$ sudo usermod -aG sudo jose  
ubuntu@ip-172-31-84-116:~$ |
```

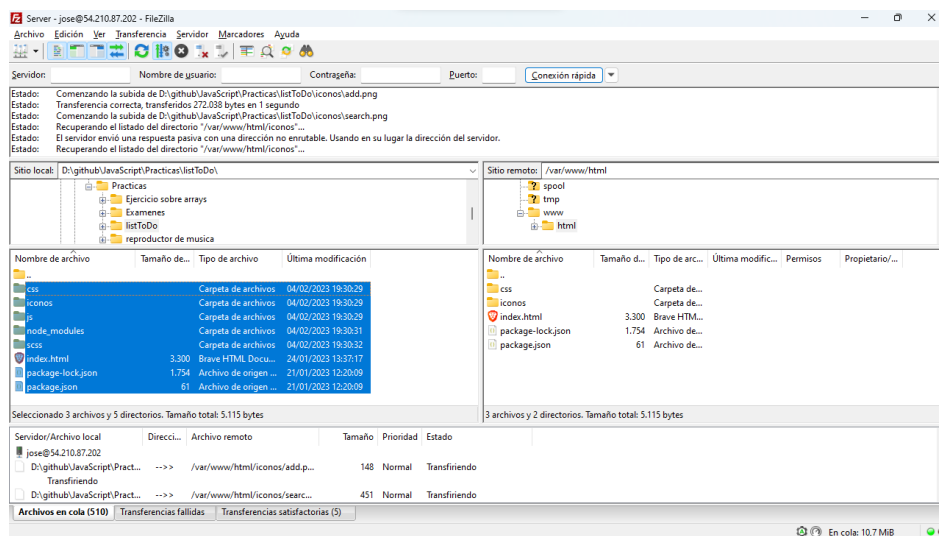
Instalare el servidor apache siguiendo los pasos de la anterior práctica, instalare también el servidor FTP

```
ubuntu@ip-172-31-84-116:~$ sudo apt install vsftpd  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  vsftpd  
0 upgraded, 1 newly installed, 0 to remove and 6 not upgraded.  
Need to get 123 kB of archives.  
After this operation, 326 kB of additional disk space will be used.  
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 vsftpd amd64 3.0.5-0ubuntu1 [123 kB]  
Fetched 123 kB in 0s (6453 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 64340 files and directories currently installed.)  
Preparing to unpack .../vsftpd_3.0.5-0ubuntu1_amd64.deb ...  
Unpacking vsftpd (3.0.5-0ubuntu1) ...  
Setting up vsftpd (3.0.5-0ubuntu1) ...  
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.  
Processing triggers for man-db (2.10.2-1) ...  
Scanning processes...  
Scanning candidates...  
Scanning linux images...
```

Descimentamos la línea write\_enable y comprobamos la conexión desde filezilla

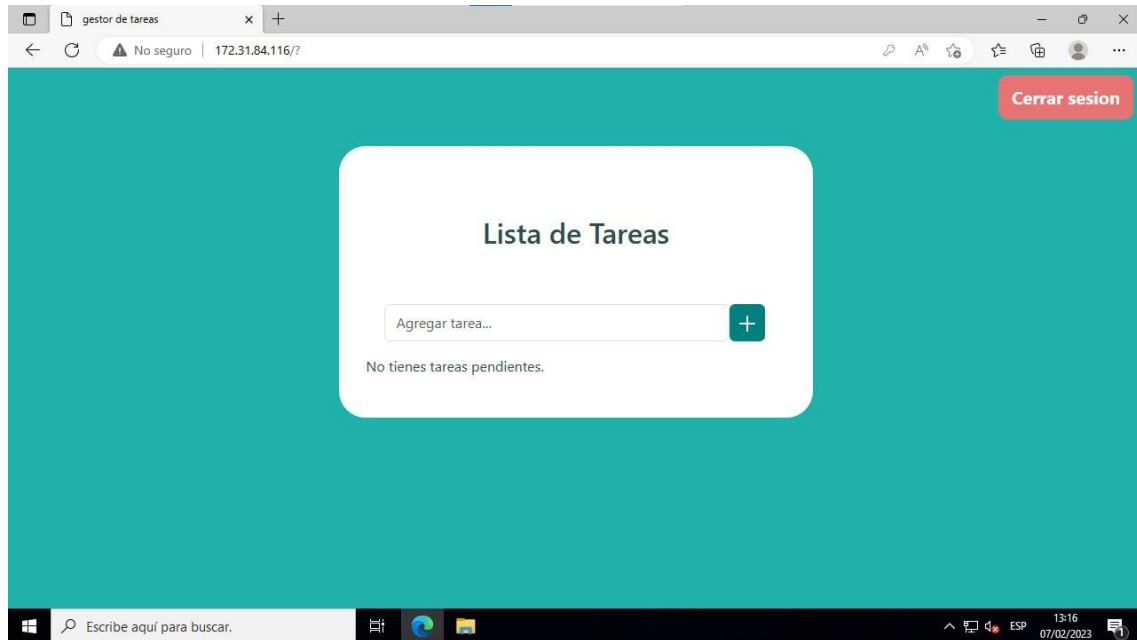


Una vez realizada la conexión transferiremos el proyecto al servidor

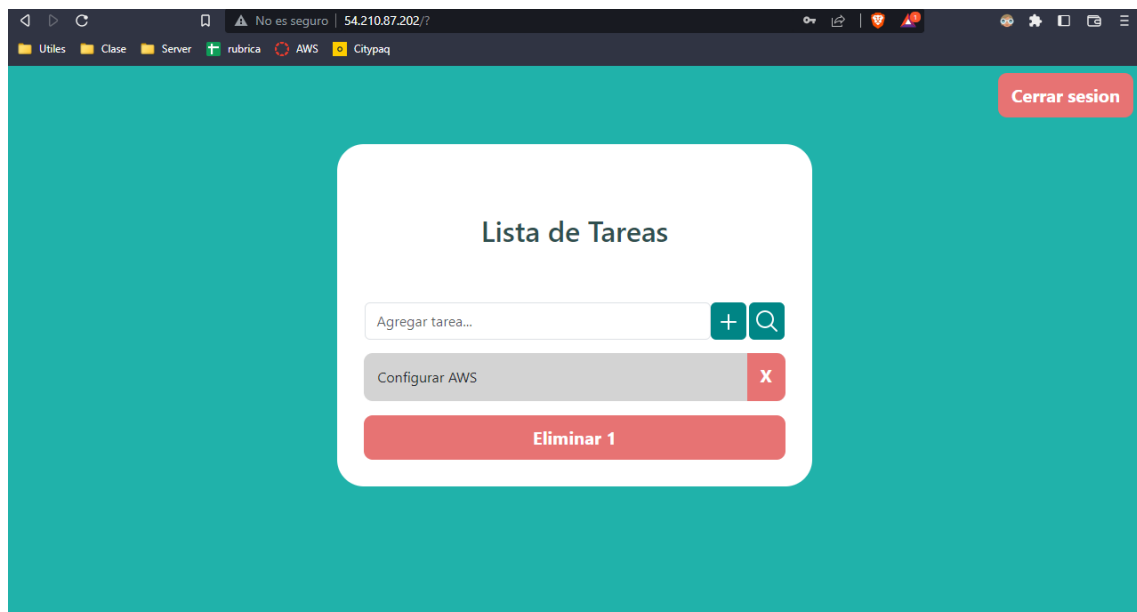


## Configuraciones de acceso remoto y pruebas de autenticación al Servidor AWS

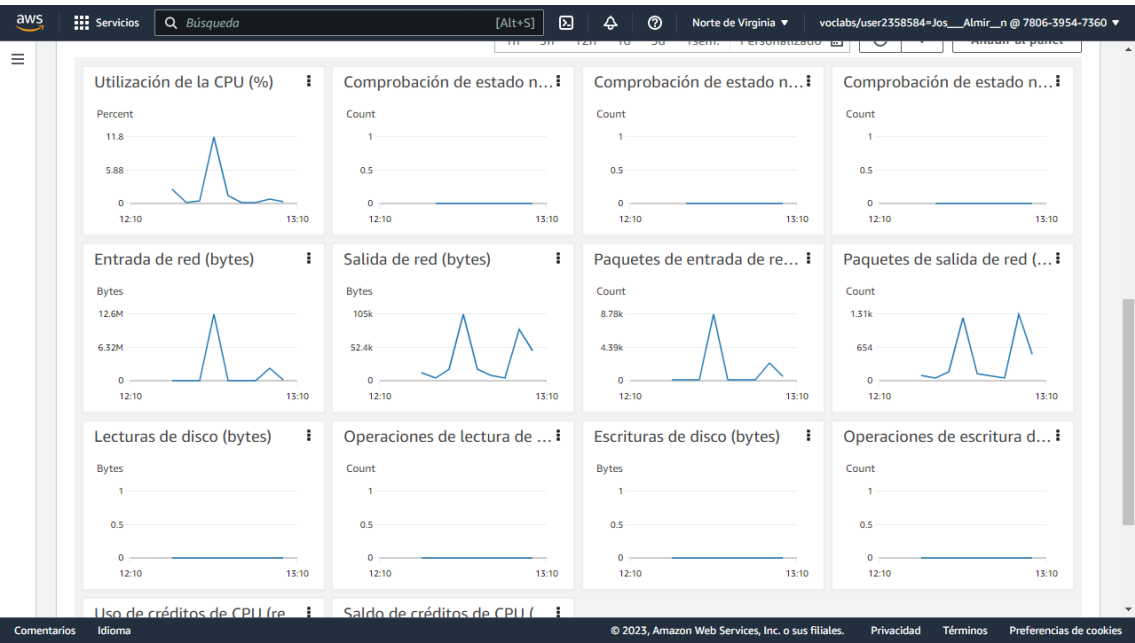
Comprobación de carga de la web desde la instancia de Windows ya que esta en la misma subred que la de Ubuntu



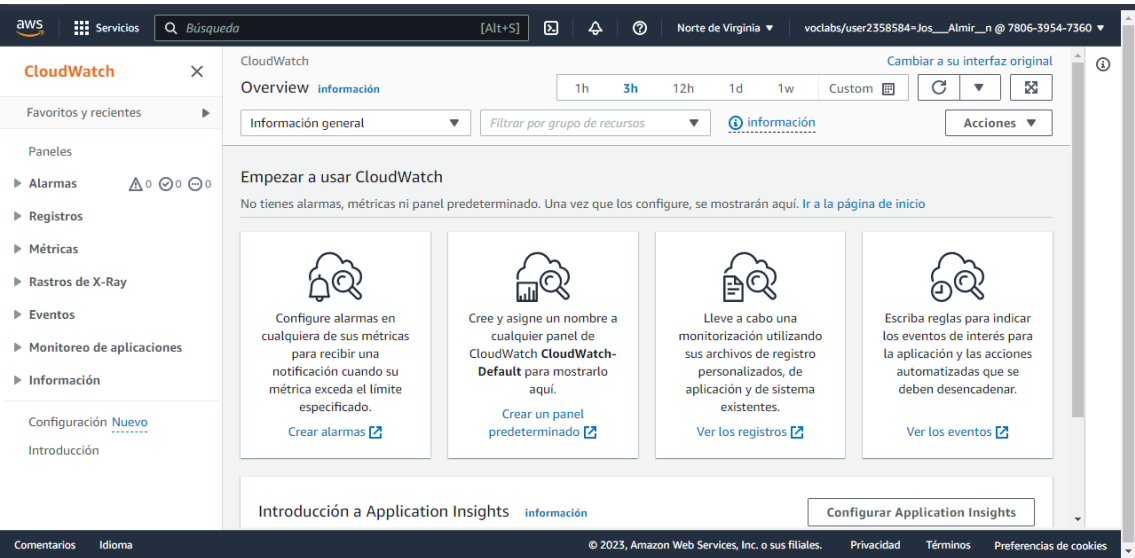
Comprobación desde mi propio equipo accediendo con la IP publica (elástica)



Muestra del monitoreo

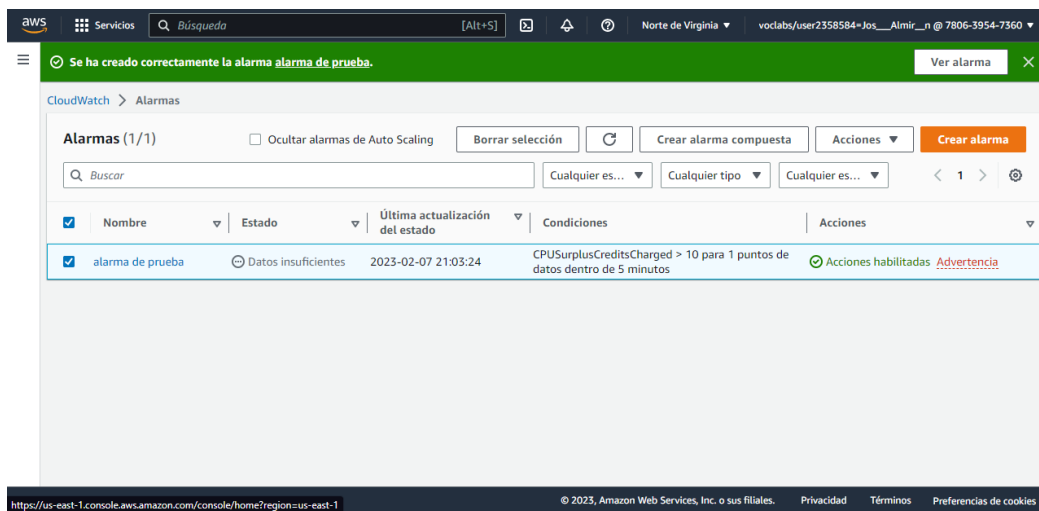
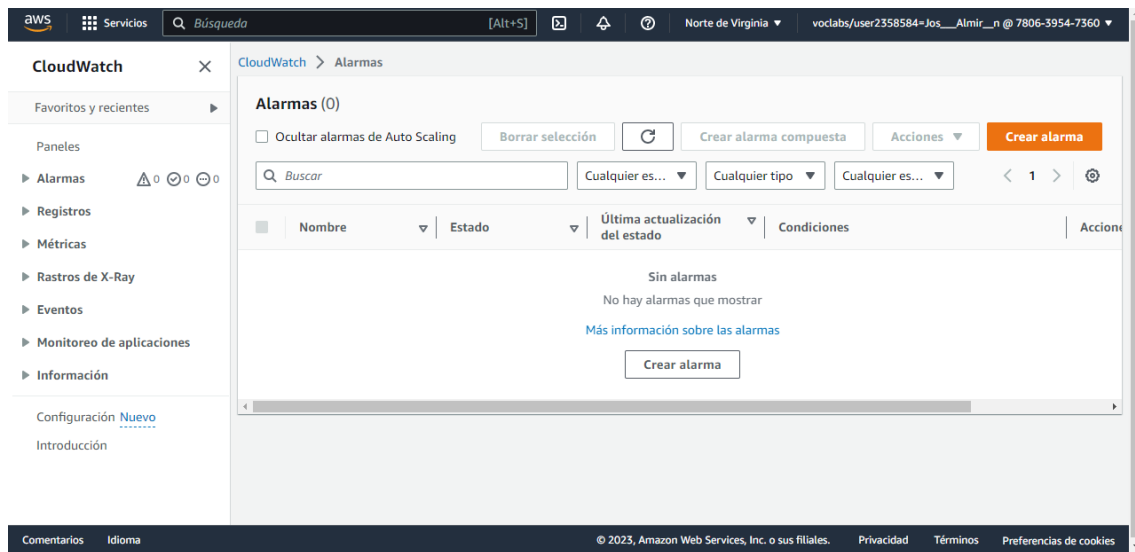


Para configurar [CloudWatch](#) accederemos a la web



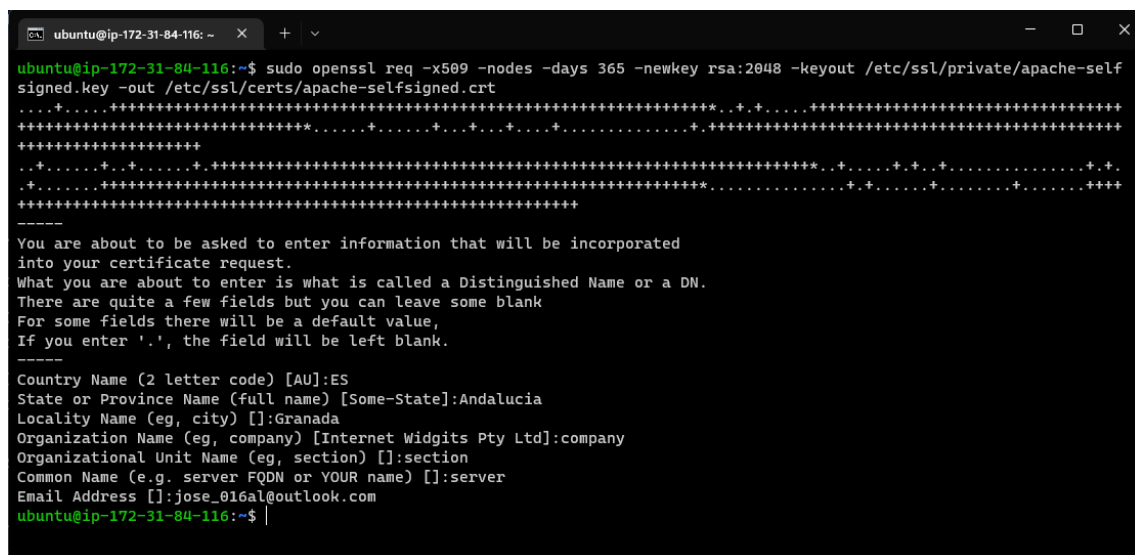
## Despliegue de aplicación web en Servidor AWS

Para ver un ejemplo, vamos a crear una alarma



## Extra: creación del certificado SSL para mejorar la seguridad

Creamos un par de claves SSL





Primero, crearemos un fragmento de configuración de Apache para definir algunos ajustes de SSL

- ***sudo nano /etc/apache2/conf-available/ssl-params.conf***

Quedando de la siguiente manera

```
ubuntu@ip-172-31-84-116: ~  
GNU nano 6.2 /etc/apache2/conf-available/ssl-params.conf  
SSLCipherSuite ECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH  
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1  
SSLHonorCipherOrder On  
# Disable preloading HSTS for now. You can use the commented out header line that includes  
# the "preload" directive if you understand the implications.  
# Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"  
Header always set X-Frame-Options DENY  
Header always set X-Content-Type-Options nosniff  
# Requires Apache >= 2.4  
SSLCompression off  
SSLUseStapling on  
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"  
# Requires Apache >= 2.4.11  
SSLSessionTickets Off
```

Modificar el archivo de host virtual de Apache SSL predeterminado

```
GNU nano 6.2 /etc/apache2/sites-available/default-ssl.conf *  
<IfModule mod_ssl.c>  
    <VirtualHost _default_:443>  
        ServerAdmin jose_016al@outlook.com  
        ServerName 172.31.84.116  
  
        DocumentRoot /var/www/html  
  
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,  
        # error, crit, alert, emerg.  
  
        # A self-signed (snakeoil) certificate can be created by installing  
        # the ssl-cert package. See  
        # /usr/share/doc/apache2/README.Debian.gz for more info.  
        # If both key and certificate are stored in the same file, only the  
        # SSLCertificateFile directive is needed.  
        SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt  
        SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key  
  
        # Server Certificate Chain:  
        # Point SSLCertificateChainFile at a file containing the  
        # concatenation of PEM encoded CA certificates which form the  
        # certificate chain for the server certificate. Alternatively  
        # the referenced file can be the same as SSLCertificateFile  
        # when the CA certificates are directly appended to the server
```

Modificar el archivo de host HTTP para el redireccionamiento a HTTPS

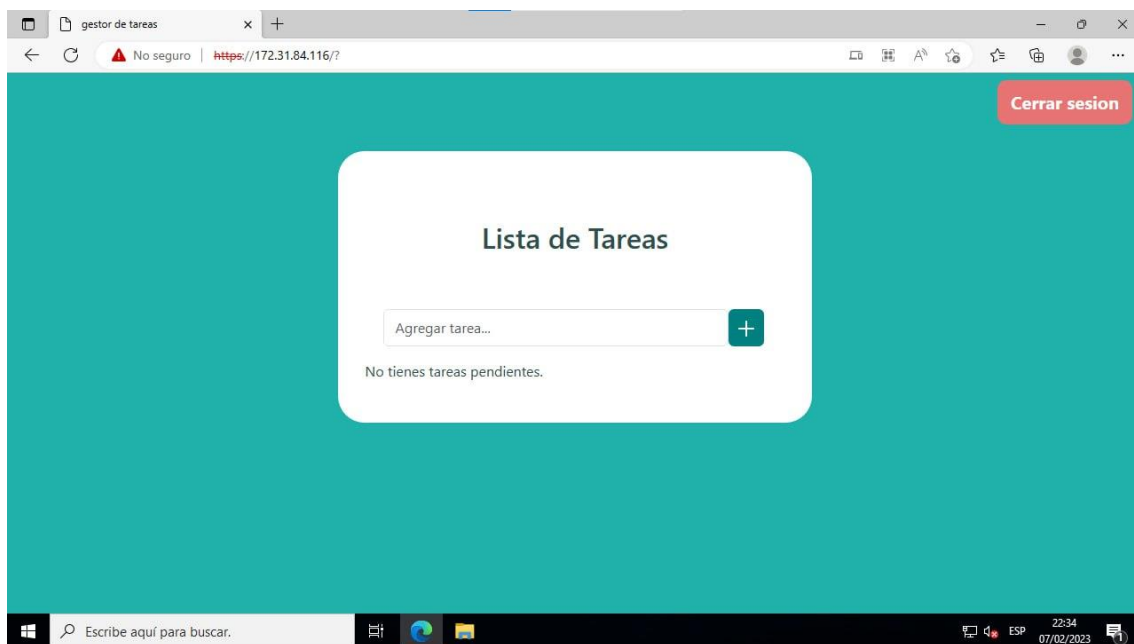
```
GNU nano 6.2 /etc/apache2/sites-available/000-default.conf *  
<VirtualHost *:80>  
    # The ServerName directive sets the request scheme, hostname and port that  
    # the server uses to identify itself. This is used when creating  
    # redirection URLs. In the context of virtual hosts, the ServerName  
    # specifies what hostname must appear in the request's Host: header to  
    # match this virtual host. For the default virtual host (this file) this  
    # value is not decisive as it is used as a last resort host regardless.  
    # However, you must set it for any further virtual host explicitly.  
    #ServerName www.example.com  
  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html  
    Redirect "/" "https://172.31.84.116/"  
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,  
    # error, crit, alert, emerg.  
    # It is also possible to configure the loglevel for particular
```

### Habilitar los cambios en Apache

```
ubuntu@ip-172-31-84-116:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
ubuntu@ip-172-31-84-116:~$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
    systemctl restart apache2
ubuntu@ip-172-31-84-116:~$ |
```

```
ubuntu@ip-172-31-84-116:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
ubuntu@ip-172-31-84-116:~$ sudo a2enconf ssl-params
Enabling conf ssl-params.
To activate the new configuration, you need to run:
    systemctl reload apache2
ubuntu@ip-172-31-84-116:~$ |
```

### Comprobación desde el local con la IP privada



Por ultimo comprobamos la conexión desde la ip Publica (elástica)

