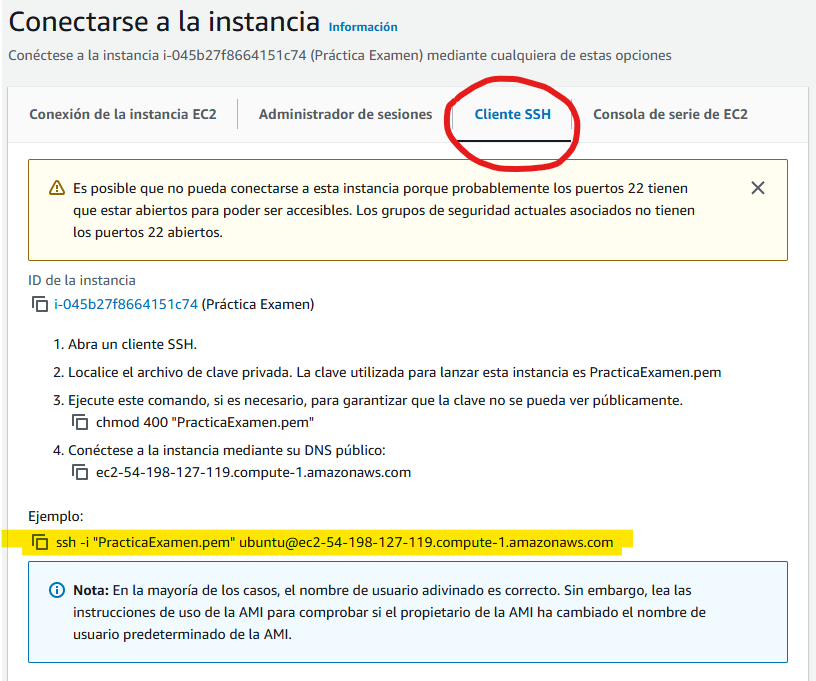
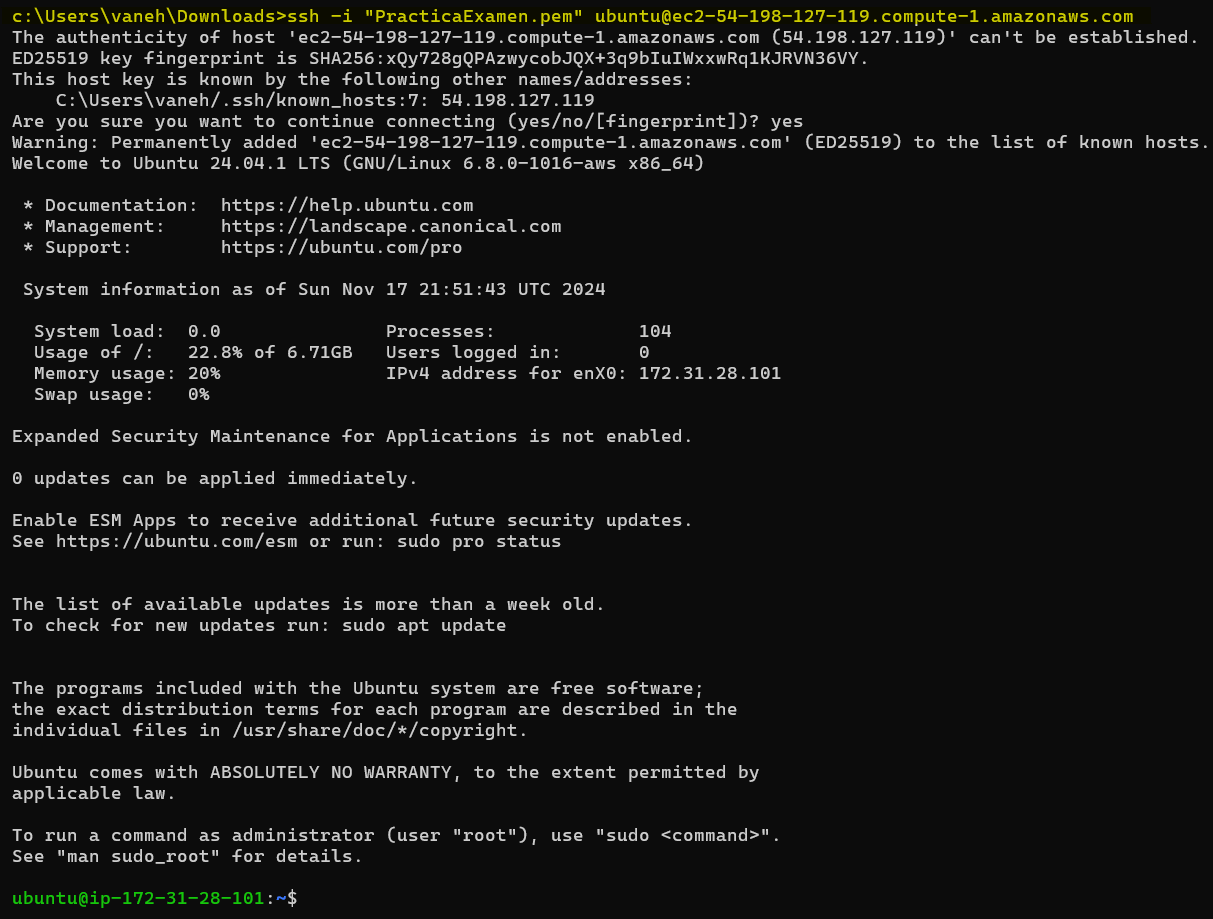
C:\Users\vaneh>dir //ls

C:\Users\vaneh>cd Downloads // Esto es Windows no linux



ssh -i "PracticaExamen.pem" [ubuntu@ec2-54-198-127-119.compute-1.amazonaws.com](mailto:ubuntu@ec2-54-198-127-119.compute-1.amazonaws.com)

Actualizar el sistema:  
**sudo apt update && sudo apt upgrade -y**

Instalar Apache2:  
**sudo apt install apache2 -y**

Configurar el firewall:  
**sudo ufw allow 'Apache'**

**Verificar el estado del servicio Apache2:  
sudo systemctl status apache2**

**sudo ufw allow 80**

**sudo ufw allow 443**

**sudo systemctl restart apache2**

INSTALAR WORDPRESS EN EL SERVIDOR

**wget<https://wordpress.org/latest.zip>**

**sudo apt install unzip**

**unzip latest.zip**

**sudo mkdir /var/www**

**sudo mv wordpress /var/www**

INSTALAR MYSQL EN EL SERVIDOR

**sudo apt install mysql-server**

2º Ponemos el siguiente comando para entrar directamente en MYSQL:

**sudo mysql**

3º Creamos la BD:

**CREATE DATABASE wordpress;**

**USE wordpress;**

**CREATE USER  ‘wordpress’@’localhost’ IDENTIFIED BY ‘1234’;**

**GRANT ALL PRIVILEGES ON wordpress.\* TO wordpress@'localhost' WITH GRANT OPTION;**

**FLUSH PRIVILEGES;**

**QUIT;**

4º Extension

SHOW DATABASES; (listar las bases de datos)

DROP DATABASE Nombre\_BD; (borrar BD) SHOW DATABASES; (confirmar el borrado)

SELECT User, Host FROM mysql.user; (lista los usuarios creados)

-INSTALAR DEPENDENCIAS EN UBUNTU

**sudo apt update**

**sudo apt install -y apache2 \**

**ghostscript \**

**libapache2-mod-php \**

**mysql-server \**

**php \**

**php-bcmath \**

**php-curl \**

**php-imagick \**

**php-intl \**

**php-json \**

**php-mbstring \**

**php-mysql \**

**php-xml \**

**php-zip**

**www-data ES EL USUARIO DE APACHE QUE TODOS PONEN POR DEFECTO**

**sudo chown -R** [**www-data**](http://www.data)**: /var/www/wordpress** (cambiar los permisos)

CONFIGURAR APACHE EN UBUNTU

PARA EDITAR EL FICHERO DE CONFIGURACION DE APACHE2

**sudo nano /etc/apache2/sites-available/wordpress.conf**

(también se puede hacer sin la ruta y ejecutarlo en esa ruta)

<VirtualHost \*:80>

    DocumentRoot /var/www/wordpress

    <Directory /var/www/wordpress>

        Options FollowSymLinks

        AllowOverride Limit Options FileInfo

        DirectoryIndex index.php

        Require all granted

    </Directory>

    <Directory /var/www/wordpress/wp-content>

        Options FollowSymLinks

        Require all granted

    </Directory>

</VirtualHost>

1.-luego hay que habilitarlo

**sudo a2ensite wordpress.conf** (habilitar sitio )

**sudo ls -l /etc/apache2/sites-enabled/** (para comprobar si está habilitado)

**sudo systemctl reload apache2**  (para reiniciar para los cambios)

**sudo systemctl status apache2** (para ver si está activo y escuchando por el puerto 80 que le hemos abierto)

**sudo a2enmod rewrite** (para habilitar la sobrescritura de URL)

**sudo a2dissite 000-default** (deshabilitar el sitio por defecto de apache)

**sudo systemctl reload apache2** (volver a recargar apache)

**sudo apache2ctl configtes**t (probar si funciona

2.- En pestaña seguridad de las instancias

editar las reglas de entrada, añadir una regla http que abra el puerto 80, en seguridad de aws, reglas de entrada

al poner la ip publica en el navegador deberia abrirse la pagina de wordpress pidiendo usuario y contraseña que son las que aparecen en el script, y conectarse con éxito.

SSH

TECNICA SALTS, PARA QUE EL HASHCODE NO SEA EL MISMO EN CADA SERVIDOR AUNQUE TENGA LA MISMA PASS SE AÑADE SALT SE AÑADE AL PASSWORD Y DEBE SER DISTINTO EN CADA SERVIDOR

Pasos para crear par de llaves , crear un usuario y autorizarlo en terminal local

1. ssh-keygen –help  //ver ayuda
2. ssh-keygen -t: la t sirve para especificar que se selecciona un tipo de par de claves, rsa o ED25519
3. ssh-keygen -t rsa: Genera un par de claves SSH usando el algoritmo RSA. //
4. ssh-keygen -t ed25519: Genera un par de claves SSH usando el algoritmo ED25519.
5. cd .ssh : Cambia el directorio a .ssh.
6. cat id\_ed25519.pub y cat id\_rsa.pub // mostramos la clave corta
7. ssh ubuntu@100.27.29.198 // estamos conectando nuestro pc al servidor (no hacer caso a la ip).
8. sudo adduser daw //creamos usuario daw
9. sudo -su daw //estamos dando permisos de super usuario a el usuario daw
10. ssh daw@100.27.29.198 //ahora conectamos el nuevo usuario al servidor tb

Terminal de aws

1. mkdir .ssh // crea directorio
2. cd .ssh/ : Cambia el directorio a .ssh.
3. ssh-keygen -t ed25519: Genera un par de claves SSH usando el algoritmo ED25519.
4. cat id\_ed25519.pub y cat id\_rsa.pub // mostramos la clave publica que es la que es .pub
5. cat authorized\_keys : muestra el contenido de authorized\_keys.
6. nano authorized\_keys // se abre authorized\_keysen el editor nano y pegamos la clave que nos ha generado el cat de consola el paso 4 y 6 del párrafo anterior.
7. sudo useradd daw : agrega un nuevo usuario nombrado daw con privilegios de superusuario.
8. sudo -su daw //estamos dando permisos de super usuario a el usuario daw

GESTION CONEXION REMOTA

[sgz.es/linux](http://sgz.es/linux) <- usuarios

[sgz.es/ssh](http://sgz.es/ssh)

BASICO

1. CREAR USUARIO,

2. DAR QUITAR PASS A UN USUARIO

3. GENENAR PAR DE CLAVES CON O SIN PASS

4. PERMISOS CORRECTOS EN CLAVE PUB/PRI

5. INSTALAR CLAVE PUBLICA EN EL SERVIDOR

-manual

-ssh-copy-id

CONFIGURACION CLIENTE

1. FICHERO LOCAL ~/.SSH/CONFIG

TRANSFERENCIA DE FICHEROS

1.- Subir y bajar ficheros y directorios

2.- Comandos scp

OTRAS COSAS

* **php -i y php -v** : Muestra la configuración y la versión de PHP.

**docker ps** : enumera los contenedores Docker en ejecución.

**ifconfig** : muestra la configuración de la red.

**dig -h** y **dig tiernogalvan.es** : comandos de búsqueda DNS.

adduser

cat etc/paswd

crear un usuario completo y darle un pass

con id vemos grupos etc de un usuario o proceso

sudo login tb con sudo su

dar y quitar password

md5sum .(fichero) lo hashea

man passwd

sudo passwd -d ubuntu (para quitar el pass)

sudo passwd -l bloquea el usuario

(con control+c salimos del comando que estemos usando)

tail

 AWS Details descargar ssh.pem

ssh -i ~Descargas/labsuser.pem  (asi se toma la clave privada

chmod  600 ~Descargas/labsuser.pem quitarle permisos de ejecucion