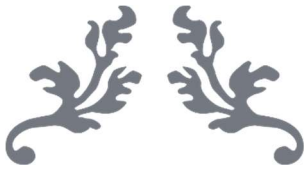


GUIA DE DESPLIEGUE

RETO DAW

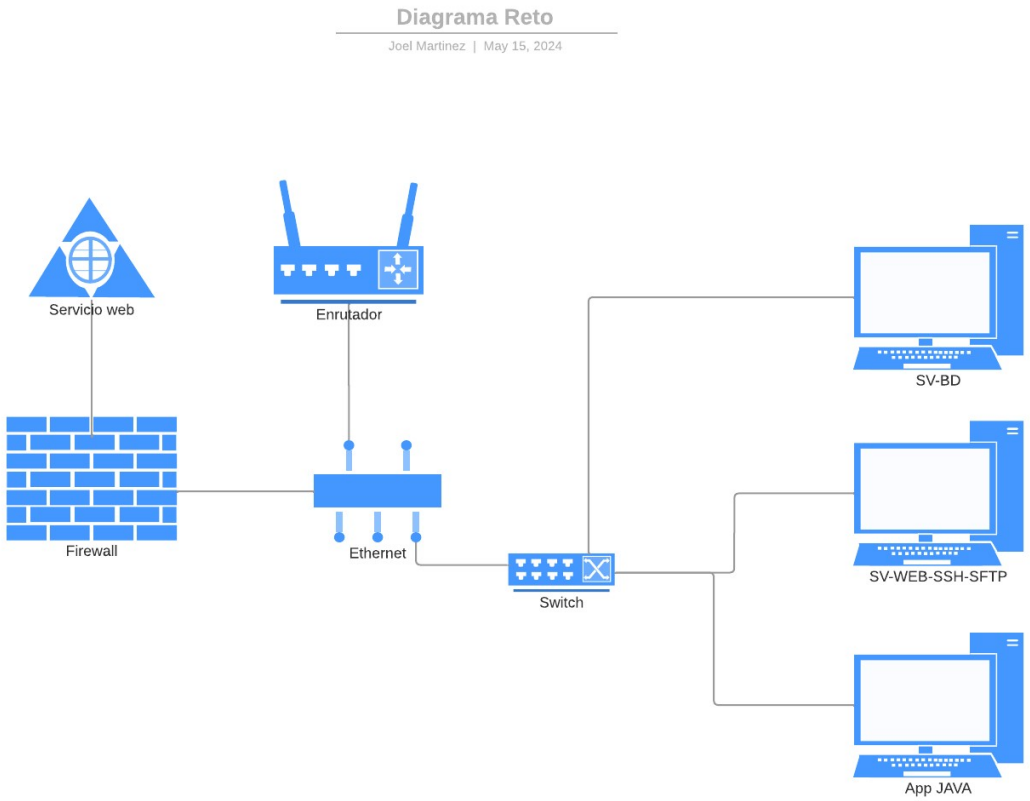
17 DE MAYO DE 2024

ACEX

Contenido

Diagrama de Red de la Arquitectura de la Aplicación. 1
Sistema Operativo. 1
Servidor de Base de Datos. 2
Servidor Web. 5
Servidor SSH. 6
Servidor SFTP. 7
Bibliografía/ Webgrafía/ Fuentes. 9

Diagrama de Red de la Arquitectura de la Aplicación.



Sistema Operativo.

Al elegir el sistema operativo para nuestros servidores, consideramos cuidadosamente varias opciones para garantizar un despliegue eficiente y confiable. Después de evaluar diferentes alternativas, decidimos optar por Ubuntu como nuestra elección principal. Esta decisión se basa en una serie de factores clave que consideramos fundamentales para nuestro entorno de servidor.

Primero y, ante todo, la estabilidad y confiabilidad de Ubuntu fueron aspectos cruciales en nuestra decisión. Sabemos que podemos confiar en Ubuntu para ofrecer un rendimiento consistente y sin problemas, lo que es fundamental para mantener la disponibilidad de nuestros servicios.

Además, la gran comunidad de usuarios y desarrolladores detrás de Ubuntu fue un factor importante. Esta comunidad activa proporciona un valioso apoyo, recursos y conocimientos que pueden ser invaluable cuando enfrentamos desafíos o necesitamos orientación en la configuración y administración de nuestros servidores.

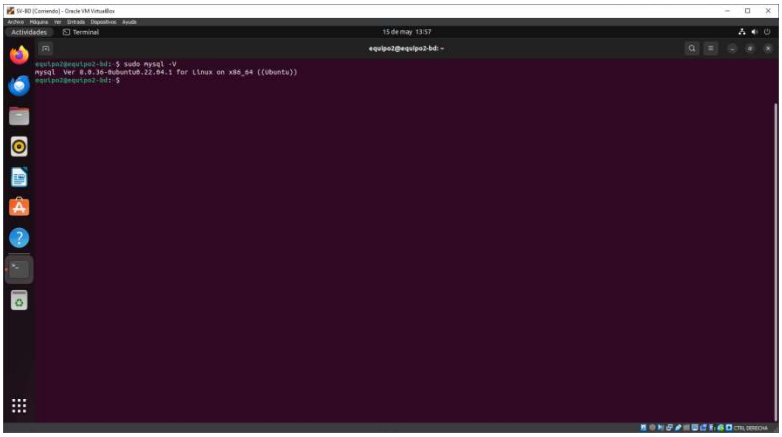
La facilidad de uso y configuración de Ubuntu también influyó en nuestra elección. La instalación es simple y directa, y el sistema operativo viene con una amplia gama de

herramientas y utilidades que facilitan la gestión de nuestros servidores sin requerir una curva de aprendizaje pronunciada.

Servidor de Base de Datos.

- **Descripción y Justificación de la Elección:**
  Se eligió una infraestructura de servidor de base de datos físico debido a los requisitos de rendimiento y seguridad de la aplicación. Un servidor físico ofrece un mayor control sobre los recursos y una mayor seguridad al estar menos expuesto a amenazas externas que un servidor virtual.

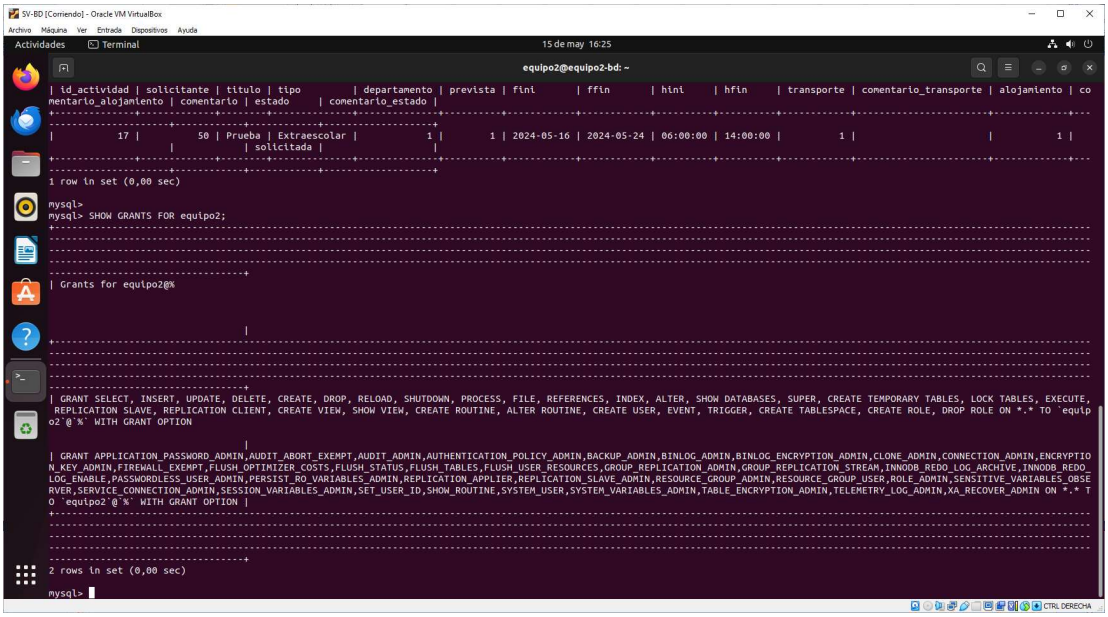
- **Versión de MySQL:**
  Se utiliza MySQL versión 8.0.36, la última estable al momento del despliegue. Esta elección se basa en su robustez y amplia compatibilidad, lo que garantiza un rendimiento óptimo y la compatibilidad con las tecnologías actuales y futuras.



- **Proceso de Instalación, Configuración y Despliegue:**
  - **Instalación de MySQL:**
    - Descargar el paquete de instalación de MySQL con el comando sudo apt install mysql. Después de una evaluación exhaustiva, optamos por MySQL como nuestra solución de base de datos principal. Esta elección se basa en una serie de razones clave que consideramos cruciales para nuestras necesidades específicas.

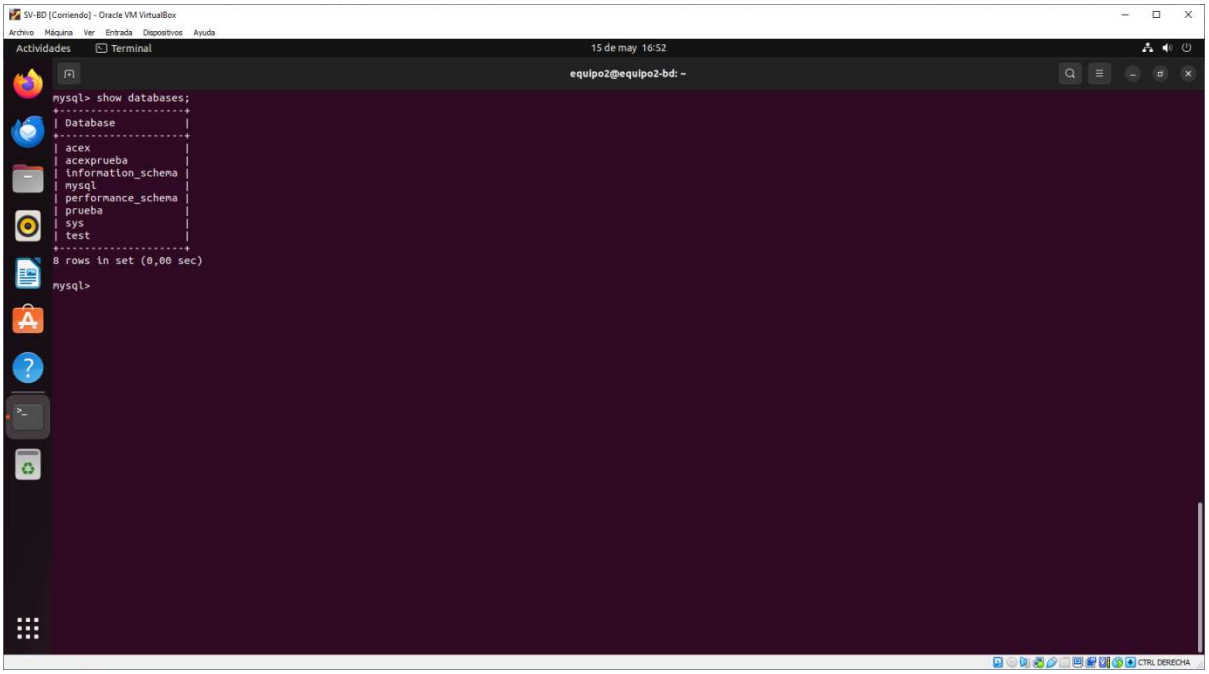
      En primer lugar, la robustez y confiabilidad de MySQL fueron factores determinantes en nuestra decisión. Sabemos que MySQL es ampliamente utilizado en la industria y ha demostrado ser un servidor de base de datos sólido y estable en una variedad de entornos. Su capacidad para manejar grandes volúmenes de datos y cargas de trabajo intensivas nos da la confianza de que podemos satisfacer nuestras demandas de almacenamiento de datos sin comprometer el rendimiento.
  - **Configuración de MySQL:**

- Establecer la contraseña de administrador.
- En nuestro caso hemos creado un usuario propio llamado equipo2 para acceder a MySQL, a este usuario le hemos dado todos los privilegios tanto de SELECT,DELETE etc para poder gestionar la base de datos sin problema.

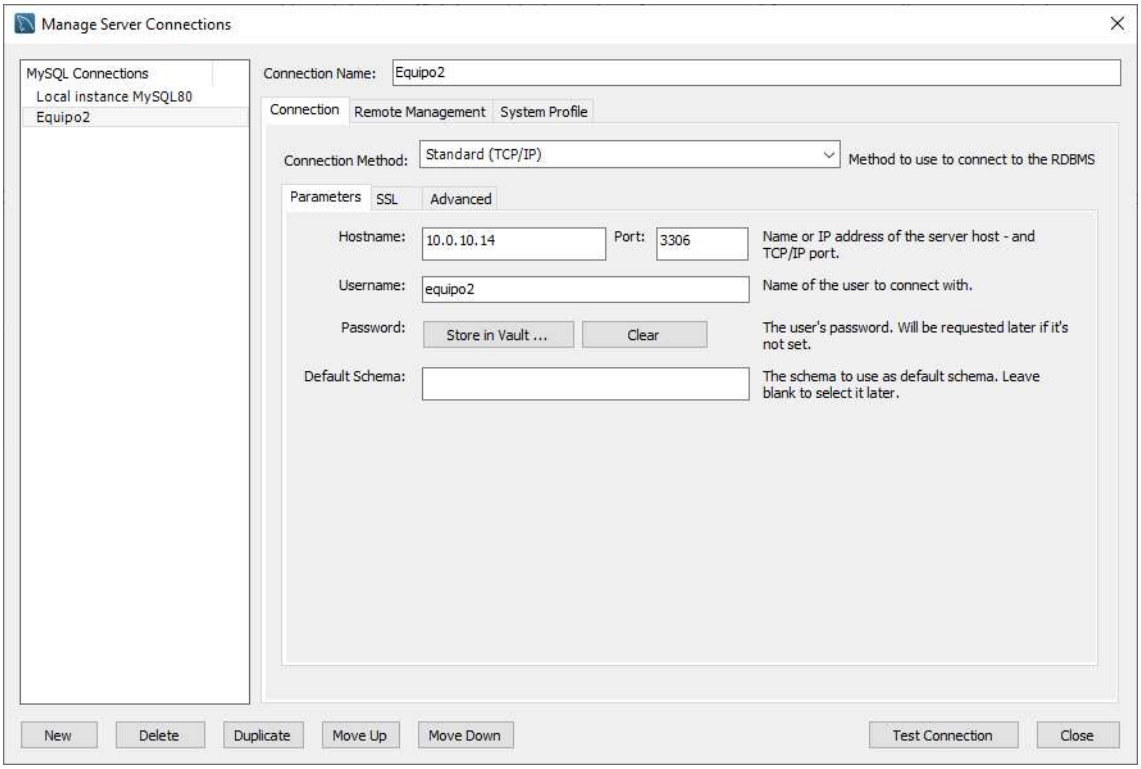


  - **Despliegue del Servidor:**
    - Iniciar el servicio de MySQL para que esté disponible para la aplicación. En nuestro caso el comando a utilizar para iniciar el servidor es **“sudo mysql –u equipo2 -p”. “-u”** es una variable que sirve para indicar el usuario con el que quieres entrar al servidor y **“-p”** se trata de una variable para que pida una contraseña al entrar.

- **Creación de la base de datos:**
  Para la creación de la base de datos podemos hacerlo de distintas maneras:
  - Desde el propio servidor, utilizando el comando **“CREATE DATABASE acex;”**



- Desde MySQL Workbench creando una nueva conexión con el servidor.



- **Carga de datos:** Para la carga de datos se hizo mediante CSV cargándolos desde la conexión hecha con MySQL Workbench mediante una opción que tiene el propio programa para importar datos

- **Acceso desde la Aplicación:**
  La aplicación accede al servidor de base de datos utilizando la dirección IP del servidor y el puerto MySQL especificado, lo que garantiza una comunicación segura y eficiente entre la aplicación y la base de datos.

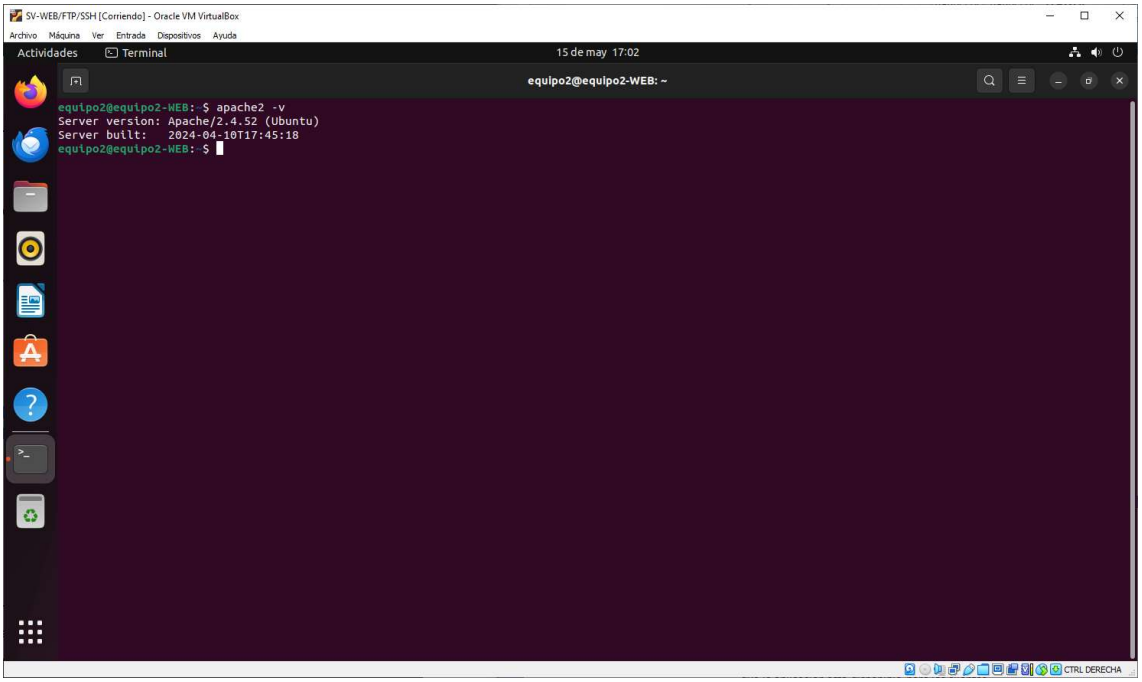
Servidor Web.

- **Descripción y Justificación de la Elección:**
  Se optó por Apache2 como servidor web debido a su amplia adopción y robustez en entornos de producción. Apache2 es conocido por su estabilidad, seguridad y capacidad para manejar un gran volumen de solicitudes web, lo que lo convierte en una opción confiable para hospedar aplicaciones web.

- **Proceso de Instalación, Configuración y Despliegue:**

  1. **Instalación de Apache2:**

     - Utilizando el gestor de paquetes del sistema operativo (por ejemplo, apt en sistemas basados en Debian), instalar el paquete apache2 mediante el comando **“sudo apt install apache2”**.



  2. **Configuración de Apache2:**

     - Establecer los permisos adecuados y las directivas de seguridad adecuadas para que el usuario pueda acceder, leer e insertar archivos en el directorio /var/www/html que es donde se meten los archivo de la pagina web para poder subirla al servidor.

  3. **Despliegue del Servidor:**

     - Reiniciar el servicio de Apache2 para aplicar los cambios y asegurar que la aplicación esté disponible para los clientes.

- **Acceso desde Clientes:**
  Los clientes acceden al servidor web ingresando la dirección IP pública del servidor y el puerto especificado en el navegador web. La configuración adecuada de Apache2 garantiza una experiencia de usuario segura y sin problemas al acceder a la aplicación.

Servidor SSH.

- **Descripción y Justificación de la Elección:**
  Se implementó un servidor SSH en el mismo servidor físico para permitir el acceso remoto seguro al servidor. SSH es un protocolo de red que proporciona un canal seguro a través de una conexión no segura, lo que garantiza la confidencialidad y la integridad de los datos durante la comunicación.

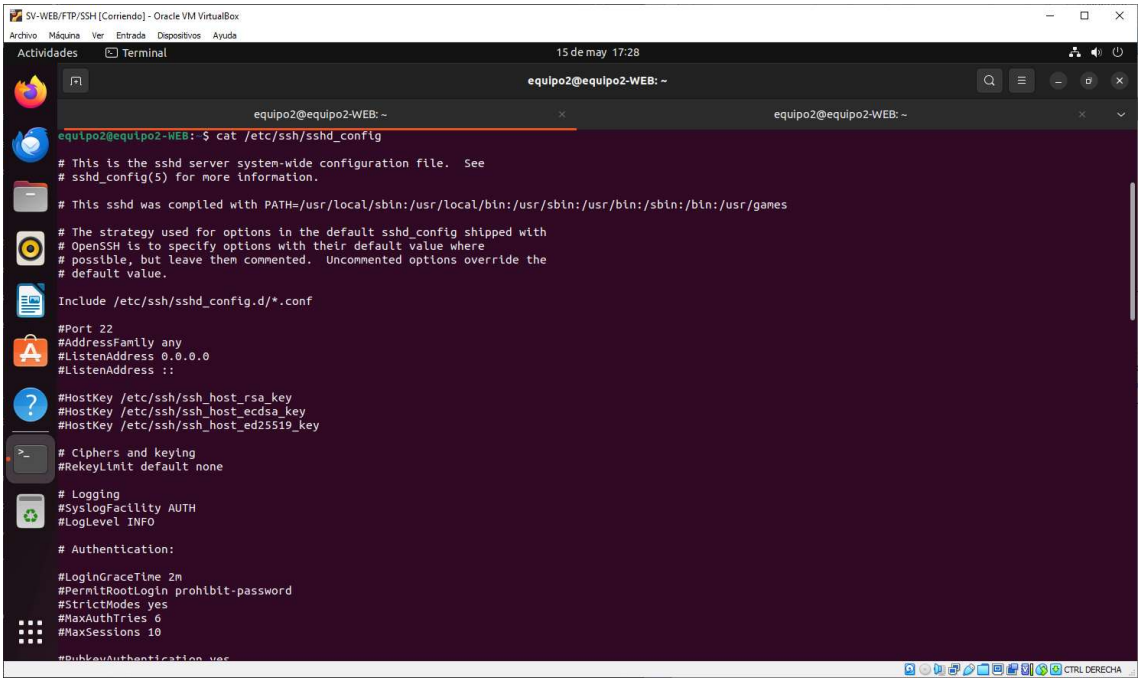
- **Proceso de Instalación, Configuración y Despliegue:**

  1. **Instalación de un Servidor SSH:**

     - Utilizando el gestor de paquetes del sistema operativo, instalar el servidor SSH (por ejemplo, OpenSSH) con el comando **"sudo apt install openssh-server"**.

  2. **Configuración de Opciones de Seguridad:**

     - Configurar las opciones de seguridad del servidor SSH para restringir el acceso no autorizado y proteger contra posibles ataques editando el fichero **"sshd_config"** y reiniciar el servicio para que se apliquen los cambios.

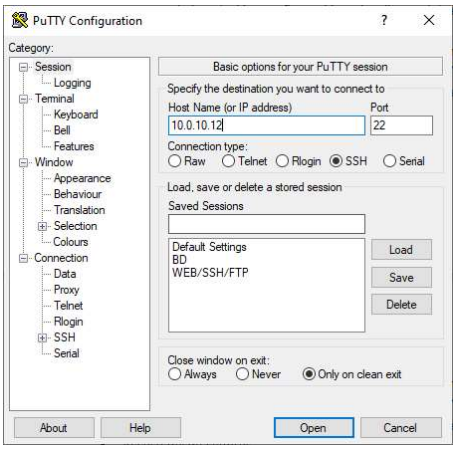


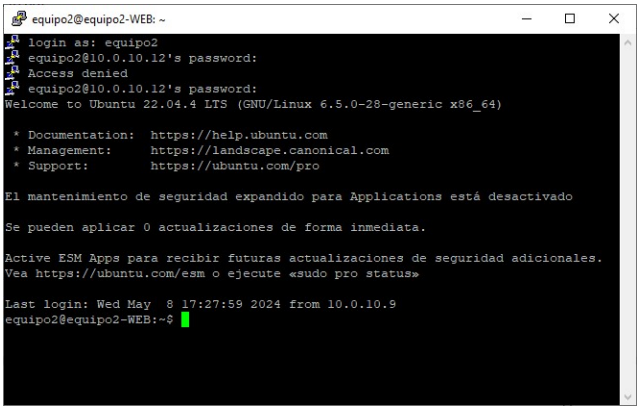
- **Despliegue del Servidor:**

- Iniciar el servicio SSH para que esté disponible para los usuarios remotos.

- **Acceso desde Clientes:**
  Los usuarios pueden acceder al servidor SSH utilizando un cliente SSH como PuTTY, ingresando la dirección IP del servidor y las credenciales de inicio de sesión. El uso de SSH proporciona una conexión segura y

cifrada que protege la información confidencial durante la transmisión.





Servidor SFTP.

- **Descripción y Justificación de la Elección:**

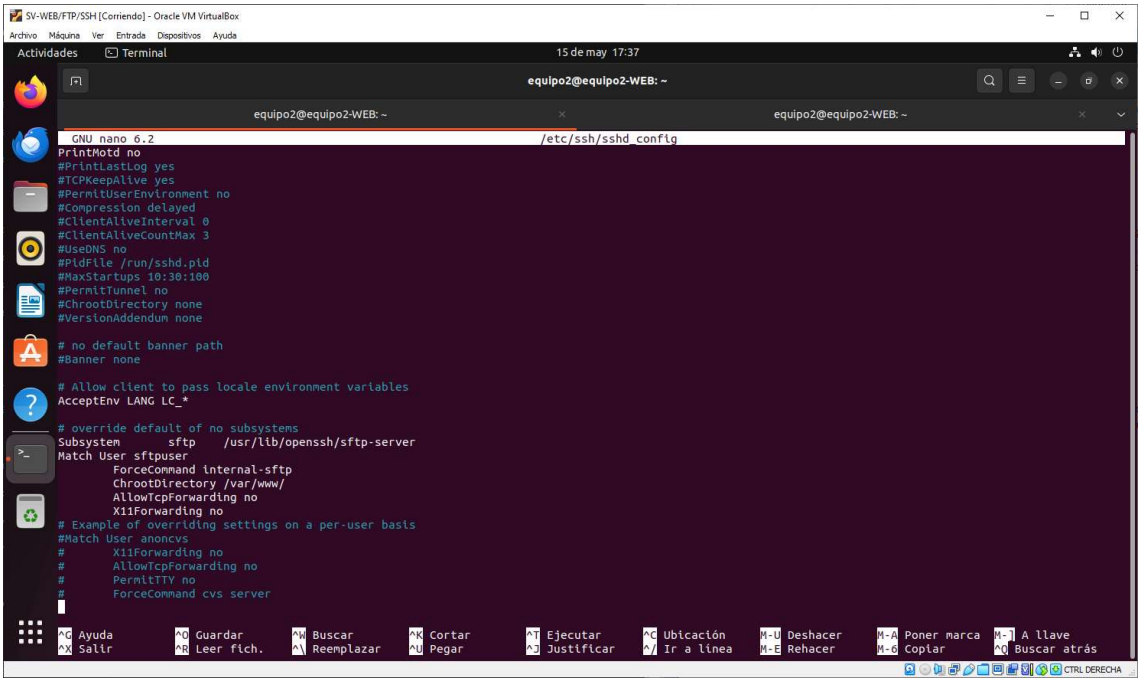
SFTP (SSH File Transfer Protocol) es una alternativa segura al FTP tradicional que utiliza SSH para cifrar todas las comunicaciones entre el cliente y el servidor. Esto proporciona una capa adicional de seguridad al transferir archivos sobre la red. La elección de SFTP se basa en la necesidad de garantizar la confidencialidad e integridad de los datos transferidos, así como la autenticación segura de los usuarios. Además, al aprovechar la infraestructura existente de SSH, SFTP se integra fácilmente en entornos donde se necesita una solución de transferencia de archivos segura.

- **Infraestructura:**

El servidor SFTP se ha montado en una máquina virtual (VM) con Ubuntu Server como sistema operativo. Esta elección se basa en la flexibilidad y la amplia compatibilidad de Ubuntu, así como en su robustez y seguridad en entornos de servidor.

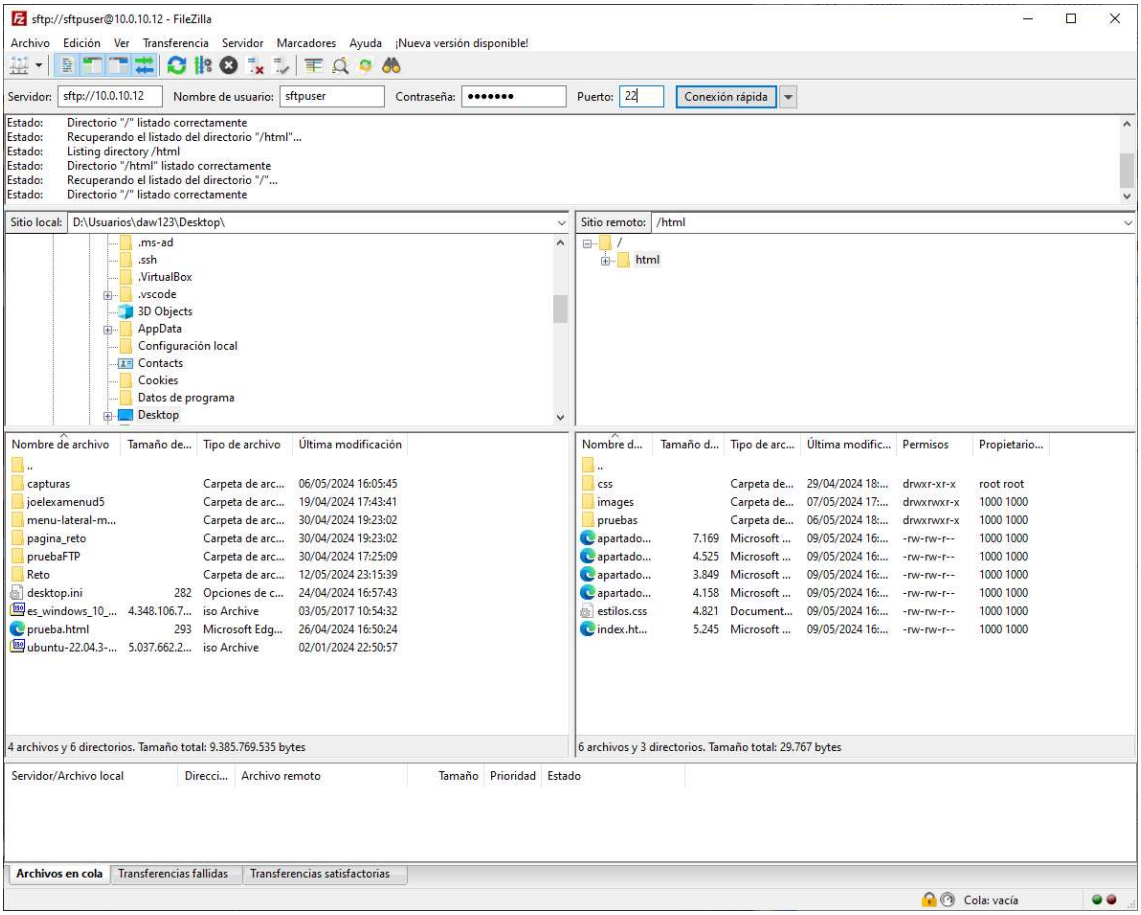
- **Proceso de Instalación, Configuración y Despliegue del Servidor:**
    - **Instalación de OpenSSH Server:** El primer paso es instalar el servidor SSH en la máquina virtual. Esto esta explicado anteriormente.
    - **Configuración de SFTP:** Una vez instalado OpenSSH Server, SFTP estará habilitado de forma predeterminada. Sin embargo, es posible que desees ajustar algunas configuraciones según tus necesidades específicas. El archivo de configuración principal de SSH se encuentra en **/etc/ssh/sshd_config**.

      En nuestro caso hemos creado un usuario nuevo para poder acceder al SFTP llamado sftpuser y hemos modificado el archivo sshd_config para que el usuario solo pueda acceder al directorio /var/www/html para poder mover los archivos de la pagina web.



- **Reiniciar el Servicio SSH:** Después de realizar cambios en la configuración de SSH, es importante reiniciar el servicio para que los cambios surtan efecto. Puedes hacerlo ejecutando el siguiente comando: **“sudo systemctl restart ssh”.**

  Una vez hecho esto ya podremos usar un cliente SFTP como FileZilla, que es el que hemos usado en nuestro caso. Para ello solo hay que indicar la IP del servidor el nombre de usuario la contraseña y el puerto.



Bibliografía/ Webgrafía/ Fuentes.

- ChatGPT
- Ionos.es
- Apuntes de CFGM de Sistemas Microinformáticos y Redes.