geekland.eu

https://geekland.eu/crear-servidor-sftp-enjaulado/

Crea nuestro propio servidor SFTP enjaulado para los usuarios

20-25 minutes

Después de la lectura de este post, los lectores sabrán que es un servidor SFTP, las ventajas que nos da respecto un servidor FTP, los usos que pueden dar a un servidor SFTP y finalmente aprenderán a crear y configurar su propio servidor SFTP.

¿QUÉ ES UN SERVIDOR SFTP?

Un servidor SFTP es aquel que utiliza el protocolo de red SFTP para establecer una conexión segura entre servidor y cliente con la finalidad de transferir y modificar archivos y carpetas de forma segura entre cliente y servidor. El medio del que se vale el protocolo SFTP para conseguir una conexión y transmisión segura entre cliente y servidor acostumbra a ser SSH.

No se debe confundir un servidor SFTP con un servidor FTP. Aunque ambos servidores tienen la misma utilidad, el protocolo SFTP es completamente diferente e independiente del protocolo FTP. Los protocoles SFPT y FTP no tienen relación alguna entre ellos. Si precisan información adicional sobre el protocolo SFTP pueden consultar el siguiente enlace.

VENTAJAS DE UN SERVIDOR SFTP RESPECTO A UN FTP

Las 2 principales ventajas que el servidor SFTP ofrece sobre un servidor FTP son las siguientes:

1. En un servidor SFTP, el proceso de **autentificación entre el cliente y el servidor se realiza con una capa de cifrado**. Por lo tanto nadie debería poder averiguar nuestro usuario y nuestra contraseña de forma sencilla.
2. En un servidor SFTP, **la totalidad de información y tráfico que se envía entre el cliente y el servidor está cifrado**. Por lo tanto un atacante no podrá interceptar ni modificar la información que se transmite entre el cliente y el servidor.

En contraposición con un servidor FTP, un servidor SFTP es un medio excelente y seguro para la transferencia de datos locales o remotos.

Nota: En este apartado solo comento las principales ventajas del servidor SFPT respecto al FTP. En cuanto a inconvenientes, pienso que prácticamente no hay ninguno. Si hay que buscar alguno podemos decir que a día de hoy hay apps de teléfono o software que no permiten conectarnos a servidores SFTP. No obstante parece que Windows 10 soportará el protocolo de encriptación SSH. Sin duda esto ayudará que se extienda el uso de este protocolo.

USOS QUE PODEMOS DAR A UN SERVIDOR SFTP

Usos comunes que hoy en día se acostumbran a dar a los servidores SFTP son los que se describen a continuación:

1. Una solución corporativa para **transferir archivos de gran tamaño** de forma segura a los clientes, a los diseñadores gráficos, a los empleados, etc.
2. Una solución segura para **subir información y realizar copias de seguridad en un servidor Web**.
3. Crear nuestra propia **nube personal para almacenar información**. De este modo estemos donde estemos podemos acceder a nuestra información almacenada en nuestro servidor y no dependemos de servicios que puedan comprometer nuestra privacidad como Google Drive, Dropbox, iCloud etc.

CARACTERÍSTICAS DEL SERVIDOR SFTP QUE VAMOS A INSTALAR Y CONFIGURAR

Las principales características del servidor que vamos a instalar y configurar son las siguientes:

1. El servidor será **accesible de forma local y de forma remota**. No tiene mucho sentido que un servidor SFTP únicamente esté accesible de forma local.
2. Por cuestiones obvias de seguridad el servidor **estará enjaulado**. Por lo tanto los usuarios que accedan al servidor sftp, solo tendrán acceso a las carpetas que nosotros queramos.
3. **Controlaremos los permisos que tendrán los usuarios que accedan a nuestro servidor SFTP**. Por lo tanto podremos seleccionar si los usuarios del servidor tienen permisos lectura, escritura y ejecución.
4. El **proceso de autentificación será mediante usuario y contraseña**. Si lo deseamos también seria posible implementar un sistema de autenticación de dos factores mediantes contraseñas y claves SSH.
5. El servidor ftp que configuraremos en este post **dispondrá** únicamente **de 2 clientes**. Vosotros podéis configurar los clientes que queráis.
6. En el caso de usar un cliente adecuado, **los clientes serán capaces de modificar los permisos de los archivos que suben al servidor SFTP**.

¿QUÉ NECESITAMOS PARA MONTAR NUESTRO SERVIDOR?

Para seguir los pasos de este tutorial no necesitamos prácticamente nada. Simplemente necesitamos **un simple ordenador con un sistema operativo Linux** que actuará de servidor.

ASEGURAR QUE EL SERVIDOR SFTP TENGA IP LOCAL FIJA

Es muy importante asegurar que nuestro servidor SFTP disponga de una IP interna fija en la red local. El motivo de esta afirmación es simple. Sí la IP del servidor es dinámica, nuestro servidor no estará localizable porqué no sabremos cual es su IP.

Para conseguir disponer de un servidor con ip interna fija tan solo hay que seguir los pasos que se detallan en el siguiente enlace:

https://geekland.eu/configurar-ip-fija_o_estatica_ipv4/

Nota: El método descrito en el enlace es válido en el caso que estéis usando un servidor sin entorno gráfico. En el caso que el servidor que uséis disponga de entorno gráfico tendréis que configurar este aspecto a través de las interfaces visuales de vuestro gestor de red que probablemente será network manager o wicd.

Una vez terminados la totalidad de pasos mi servidor tendrá una IP fija que en mi caso será la 192.168.1.188. Esta IP es la que deberemos usar para localizar y conectar con nuestro servidor SFTP de forma local. Esta también será la IP que tenemos que usar para que nuestro Router redireccione las peticiones de los clientes SFTP remotos al servidor SFTP.

HACER QUE NUESTRO SERVIDOR SFTP ESTE ACCESIBLE DESDE EL EXTERIOR

Cuando tengamos nuestro servidor SFTP funcionando, lo más probable es que tengamos clientes remotos que quieran conectarse a nuestro servidor SFTP.

Los clientes remotos necesitaran nuestra IP Pública para poderse conectar al servidor SFTP. Desafortunadamente en la gran mayoría de casos la IP que tenemos es dinámica. Por lo tanto se puede dar perfectamente el caso que en el momento de conectarnos no sepamos la IP Pública de nuestro servidor.

Para solucionar este problema **tenemos que asociar la IP Pública de nuestro servidor a un dominio. Para poder realizar este paso tan solo tienen que seguir las indicaciones del siguiente enlace**:

https://geekland.eu/encontrar-servidor-con-dns-dinamico/

Una vez realizados estos pasos tendréis vuestra IP Pública asociada a un dominio. En mi caso mi IP Pública está asociada al dominio **geekland.sytes.net**

LOGUEARNOS COMO USUARIO ROOT

Todo el proceso de instalación y configuración del servidor se realizará siendo root. Por lo tanto el primer paso es loguearnos como usuario root. Para ello **en la terminal ejecutamos el siguiente comando**:

```
su root
```

Al ejecutar el comando nos preguntaran la contraseña del usuario root. La introducimos y presionamos **Enter**.

INSTALAR EL SERVIDOR SFTP

El segundo paso para disponer de nuestro servidor SFTP es asegurar que tengamos la totalidad de paquetes necesarios instalados. Para ello abrimos una terminal y **ejecutamos el siguiente comando para actualizar los repositorios de nuestro sistema operativo**:

```
apt-get update
```

Seguidamente tenemos que instalar los paquetes openssh-server y openssh-client. Para ello **ejecutamos el siguiente comando en la terminal**:

```
apt-get install openssh-server openssh-client
```

Nota: La mayoría de distros linux instalan los paquetes openssh-server y openssh-client en el momento de la instalación de la distro. Por lo tanto es posible que ya tengan estos paquetes previamente instalados.

Nota: En caso de usar un gestor de paquetes diferente a apt-get, deberán adaptar los comandos de este apartado al gestor de paquetes correspondiente.

CREACIÓN DE LAS CARPETAS EN LAS QUE LOS CLIENTES UBICARAN LA INFORMACIÓN

Seguidamente hay que crear las carpetas en las que los clientes del servidor SFTP ubicarán su información.

En mi caso he decidido que la totalidad de información del servidor SFTP se almacene en la ubicación /home/sftpserver. Por lo tanto el primer paso es **crear la carpeta sftpserver dentro de la ubicación home ejecutando el siguiente comando en la terminal**:

```
mkdir /home/sftpserver
```

Seguidamente, **dentro de la ubicación** /home/sftpserver **creamos una carpeta para cada uno de los usuarios** del servidor SFTP. Como los usuarios son jccall80 y ramon, hay **introducir los siguientes comandos en la terminal** para crear las carpetas:

```
mkdir /home/sftpserver/jccall80

mkdir /home/sftpserver/ramon
```

A continuación, dentro de cada una de las carpetas de los usuarios, crearé otra serie de carpetas para que el usuario del servidor SFTP pueda almacenar sus archivos y su información. Para ello hay que **ejecutar los siguientes comandos en la terminal**:

```
mkdir /home/sftpserver/jccall80/archivos

mkdir /home/sftpserver/jccall80/compartir

mkdir /home/sftpserver/ramon/archivos

mkdir /home/sftpserver/ramon/compartir
```

CREAR UN GRUPO QUE CONTIENE LA TOTALIDAD DE USUARIOS DEL SERVIDOR SFTP

En mi caso he decidido crear un grupo llamado SFTP que contendrá la totalidad de usuarios del servidor SFTP. **Para crear el grupo tenemos que teclear el siguiente comando en la terminal**:

```
groupadd sftpserver
```

El hecho de crear un grupo que contenga la totalidad de usuarios del servidor SFTP nos será de gran utilidad a la hora de configurar los permisos y enjaular a los usuarios de nuestro servidor.

CREAR LOS USUARIOS Y EL GRUPO DE NUESTRO SERVIDOR SFTP

Una vez creado el grupo sftpserver, ahora hay que crear los usuarios de nuestro servidor SFTP. **Para crear** un usuario, que en mi caso será **jccall80**, es necesario teclear y **ejecutar el siguiente comando en la terminal**:

```
useradd -g sftpserver -s /bin/false -d /home/sftpserver/jccall80 jccall80
```

El significado de cada una de las partes del comando que acabamos de ejecutar es el siguiente:

useradd: Comando principal empleado para la creación de un usuario.

-g sftpserver: Para indicar que el usuario que estamos creando pertenece al grupo sftpserver.

-s /bin/false: Para definir que el usuario del servidor SFTP que estamos creando, no tenga acceso a la terminal o interprete de comandos. Este aspecto es importante por temas de seguridad, ya que si un usuario del servidor tuviera acceso al interprete de comandos, podría ejecutar comandos que podrían comprometer la seguridad de nuestro servidor.

-d /home/sftpserver/jccall80: Para indicar la ruta home por defecto del usuario que estamos creando para el servidor SFTP.

jccall80: Es el nombre del usuario que queremos crear.

Del mismo modo que hemos creado el usuario jccall80, también **crearemos el usuario ramon ejecutando el siguiente comando en la terminal**:

```
useradd -g sftpserver -s /bin/false -d /home/sftpserver/ramon ramon
```

CREAR UN PASSWORD PARA CADA USUARIO

Seguidamente asignaremos un password a los usuarios que acabamos de crear. **Para asignar un password al usuario jccall80 abriremos una terminal y ejecutaremos el siguiente comando**:

```
passwd jccall80
```

El significado de este comando es el siguiente:

passwd: Comando para fijar o modificar la contraseña de un usuario.

jccall80: Es el usuario el cual queremos cambiar/definir su contraseña.

Después de ejecutar el comando, se nos preguntará 2 veces el password que queremos que tenga el usuario. Lo introducimos, presionamos Enter y el proceso ha terminado.

Del mismo modo que hemos generado el password para usuario jccall80, **también generaremos un password para el usuario ramon introduciendo el siguiente comando en la terminal**:

```
passwd ramon
```

ASIGNAR UN USUARIO Y UN GRUPO A LAS CARPETAS DEL SERVIDOR SFTP

A estas alturas ya hemos creado los grupos y los usuarios de nuestro servidor SFPT. El siguiente paso será definir el grupo y el usuario al que pertenecen cada una de las carpetas de los usuarios del servidor SFTP.

Las carpetas /home/sftpserver/jccall80/archivos y /home/sftpserver/jccall80/compartir, **queremos que pertenezcan el usuario jccall80 y al grupo sftpserver. Para ello ejecutamos los siguientes comandos en la terminal**:

```
chown jccall80:sftpserver /home/sftpserver/jccall80/archivos

chown jccall80:sftpserver /home/sftpserver/jccall80/compartir
```

El significado de cada uno de los parámetros del comando son los siguientes:

chown: Es el comando usado para modificar los permisos de archivos y carpetas.

jccall80:sftpserver: jccall80 es el nombre usuario al que queremos que pertenezca la carpeta jccall80. Sfptserver es el grupo al que queremos que pertenezca la carpeta jccall80

/home/sfptserver/jccall80/archivos: Es la ruta de la carpeta la cual queremos modificar el grupo y el usuario.

Las carpetas /home/sftpserver/ramon/archivos y /home/sftpserver/ramon/compartir, **queremos que pertenezcan el usuario ramon y al grupo sftpserver. Para ello ejecutamos los siguientes comandos en la terminal**:

```
chown ramon:sftpserver /home/sftpserver/ramon/archivos

chown ramon:sftpserver /home/sftpserver/ramon/compartir
```

Finalmente queremos que las carpetas /home/sftpserver, /home/sftpserver/jccall80 y /home/sftpserver/ramon pertenezcan al usario root y al grupo root. Por lo tanto ejecutaremos los siguientes comandos en la terminal:

```
chown root:root /home/sftpserver
```

```
chown root:root /home/sftpserver/jccall80

chown root:root /home/sftpserver/ramon
```

Nota: Es absolutamente indispensable que las carpetas /home/sftpserver, /home/sftpserver/jccall80 y home/sftpserver/ramon pertenezcan al usuario root. En caso contrario seria completamente imposible enjaular a los grupos o a los usuarios del servidor sftp. El propietario del directorio que usamos como jaula tiene que ser siempre root, y los permisos de la carpeta tienen que ser 755.

ASIGNAR PERMISOS A LAS CARPETAS DEL SERVIDOR SFTP

En apartados anteriores hemos creado las carpetas de nuestro servidor SFTP. A estas carpetas tenemos que asignarles los permisos que más nos convengan.

En mi caso **quiero que las carpetas** jccall80/archivos y ramon/archivos **solo sean accesibles/modificables por sus propietarios**, que son jccall80 y ramon respectivamente. **Para ello introduciré los siguientes comandos en la terminal**:

```
chmod 700 /home/sftpserver/jccall80/archivos

chmod 700 /home/sftpserver/ramon/archivos
```

Asignando los permisos 700, la carpeta jccall80/archivos únicamente será accesible y modificable por parte del usuario jccall80, y la carpeta ramon/archivos únicamente será accesible y modificable por el usuario ramón. El resto de usuarios no dispondrán de ningún permiso sobre estas carpetas. Por lo tanto asignar estos permisos es ideal para mantener la información de los usuarios del servidor privada.

También **quiero que cualquier usuario pueda acceder y visualizar el contenido de las carpetas** jccall80/compartir y ramon/compartir, **y que únicamente los propietarios de la carpetas** jccall80/compartir y ramon/compartir **puedan modificar su contenido. Para conseguir este propósito ejecutaré los siguientes comandos en la terminal**:

```
chmod 755 /home/sftpserver/jccall80/compartir

chmod 755 /home/sftpserver/ramon/compartir
```

Asignando los permisos 755 a estas carpetas, cualquier usuario podrá entrar en la carpeta jccall80/compartir y ramon/compartir y visualizar los archivos que hay dentro de esta ubicación, pero solo el propietario podrá crear, eliminar y modificar archivos. Por lo tanto estos permisos son ideales para compartir información con otros usuarios del servidor SFTP.

Finalmente **tenemos que asignar, sí o sí, los permisos 755 a las carpetas** /home/sftpserver, home/sftpserver/jccall80 y **home/sftpserver/ramon**. **Para ello ejecutamos los siguientes comandos en la terminal**:

```
chmod 755 /home/sftpserver/jccall80

chmod 755 /home/sftpserver/ramon

chmod 755 /home/sftpserver
```

Estas 3 carpetas deben tener los permisos 755, ya que en caso contrario, seria imposible enjaular a los usuarios del servidor SFTP. Recordamos de nuevo que el propietario del directorio que usamos como jaula debe ser root, y los permisos de la carpeta que usamos como jaula tienen que ser 755

ENJAULAR A LOS USUARIOS DEL SERVIDOR SFTP

Para enjaular a los usuarios disponemos de 2 opciones. Enjaular usuario por usuario, o enjaular a un grupo entero de usuarios. **Únicamente podéis seleccionar una de las 2 opciones**.

Opción 1: Enjaular a un grupo de usuarios

Si estáis leyendo este apartado es porqué habéis decidido enjaular a un grupo de usuarios. Para enjaular a un grupo de usuarios **hay que modificar la configuración del fichero** sshd_config. Antes de realizar cualquier modificación en la configuración de este fichero, **realizaremos una copia del fichero ejecutando el siguiente comando en la terminal**:

```
cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
```

Una vez realizada la copia de seguridad ya se puede **editar el fichero de configuración introduciendo el siguiente comando en la terminal**:

```
nano /etc/ssh/sshd_config
```

Después de ejecutar el comando se abrirá el editor de texto nano con el contenido del fichero sshd_config.

En el fichero de configuración **tenemos que buscar la siguiente línea**:

```
Subsystem sftp /usr/lib/openssh/sftp-server
```

Una vez encontrada, **la comentamos introduciendo # al inicio de la línea**. Por lo tanto quedará de la siguiente forma:

```
#Subsystem sftp /usr/lib/openssh/sftp-server
```

Para enjaular al grupo de usuarios del servidor, tenemos que **ir al final del fichero de configuración e introducir los siguientes parámetros**:

```
Subsystem sftp internal-sftp
Match group sftpserver
ChrootDirectory /home/sftpserver
ForceCommand internal-sftp
```

Nota: Únicamente hay que modificar las partes del código que están en color rojo. En el comando Match Group hay que poner el nombre del grupo que queremos enjaular que en mi caso es sftpserver. En el comando ChrootDirectory, tenemos que indicar la ubicación en que queremos enjaular a los usuarios que forman parte del grupo sftpserver.

Nota: Con esta configuración, los usuarios del servidor SFTP que pertenezcan al grupo sftpserver, solo podrán acceder al contenido de la carpeta /home/sftpserver en adelante.

Una vez realizados los cambios tan solo tenemos guardarlos y cerrar el fichero. Seguidamente tenemos que reiniciar el servidor SSH para que las modificaciones surjan efecto. Para **reiniciar el servidor tecleando el siguiente comando en la terminal**:

```
service ssh restart
```

Una vez reiniciado el servidor ssh, el servidor SFTP ya está plenamente operativo.

Opción 2: Enjaular usuario por usuario

Si estáis leyendo este apartado es porqué habéis decidido enjaular a cada uno de los usuarios de forma individual. Para enjaular a un usuario **hay que modificar la configuración del fichero** sshd_config. Antes de realizar cualquier modificación en la configuración de este fichero, **realizaremos una copia del fichero ejecutando el siguiente comando en la terminal**:

```
cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
```

Una vez realizada la copia de seguridad ya se puede **editar el fichero de configuración introduciendo el siguiente comando en la terminal**:

```
nano /etc/ssh/sshd_config
```

Después de ejecutar el comando se abrirá el editor de texto nano con el contenido del fichero sshd_config.

En el fichero de configuración **tenemos que buscar la siguiente línea**:

```
Subsystem sftp /usr/lib/openssh/sftp-server
```

Una vez encontrada, **la comentamos introduciendo # al inicio de la línea.** Por lo tanto quedará de la siguiente forma:

```
#Subsystem sftp /usr/lib/openssh/sftp-server
```

Para enjaular a los usuarios jccall80 y ramon, tenemos que **ir al final del fichero de configuración e introducir el siguiente texto**:

```
Subsystem sftp internal-sftp
Match user jccall80
ChrootDirectory /home/sftpserver/jccall80
ForceCommand internal-sftp

Match user ramon
ChrootDirectory /home/sftpserver/ramon
ForceCommand internal-sftp
```

Nota: Únicamente hay que modificar las partes del código que están en color rojo. En el comando Match user hay que poner el nombre del usuario que queremos enjaular. En el comando ChrootDirectory, tenemos que indicar la ubicación en que queremos enjaular cada uno de los usuarios.

Nota: Con esta configuración, el usuario jccall80 únicamente podrá acceder al contenido ubicado en la carpeta /home/sftpserver/jccall80 y en las carpetas de nivel superior a /home/sftpserver/jccall80. Por otra parte el usuario el usuario ramon solo podrá acceder al contenido ubicado en la carpeta /home/sftpserver/ramon y en las carpetas de nivel superior a /home/sftpserver/ramon.

Una vez realizados los cambios tan solo tenemos guardarlos y cerrar el fichero. Seguidamente tenemos que **reiniciar el servidor SSH** para que las modificaciones surjan efecto. Para reiniciar el servidor tecleamos el siguiente comando en la terminal:

```
service ssh restart
```

Una vez reiniciado el servidor ssh, el servidor SFTP ya está plenamente operativo.

FORTIFICAR NUESTRO SERVIDOR SFTP

Dentro del fichero de configuración **etc/ssh/sshd_config**, podemos modificar ciertos parámetros para fortificar la seguridad de nuestro servidor SFTP.

Quien esté interesado en este punto, tiene que saber que durante las próximas semanas escribiré un post en el que detallaré los parámetros que podemos modificar para fortificar nuestro servidor.

ELIMINAR GRUPOS USUARIOS Y EL GRUPO DEL SERVIDOR SFTP

Anteriormente hemos visto como crear un grupo y una serie de usuarios para nuestro servidor SFTP.

Si algún día **precisamos borrar algún usuario del servidor SFTP** lo podemos hacer de la siguiente forma:

Primero de todo **instalamos el paquete members** que nos servirá para ver los usuarios que tiene un determinado grupo. **Para ello ejecutamos el siguiente comando en la terminal**:

```
apt-get install members
```

Una vez dispongamos del paquete members instalado, **tecleamos la palabra members seguida del nombre del grupo que contiene los usuarios del servidor SFTP** en la terminal:

```
members sftpserver
```

Presionamos Enter y obtendremos la totalidad de usuarios del servidor SFTP. **Seleccionamos el usuario que queremos borrar** que en mi caso es ramon. Una vez seleccionado el usuario a borrar tan solo tenemos que **ejecutar el siguiente comando en la terminal**:

```
userdel -r ramon
```

Nota: La opción -r especifica que aparte de borrarse el usuario, también queremos que se borre el directorio home del usuario.

Una vez borrados todos los usuarios, si lo precisamos **también podemos borrar el grupo sftpserver**. Para ello tan solo tenemos que teclear el siguiente comando en la terminal:

```
groupdel sftpserver
```

CONECTARSE Y USAR EL SERVIDOR SFPT

Durante las próximas semanas escribiré una serie de post en el que detallaré que opciones tenemos para conectarnos a nuestro servidor SFTP. En los post detallaré como podemos usar nuestro servidor SFTP en prácticamente la totalidad de sistemas operativos existentes en la actualidad.