

Manual para la configuración del servidor FTP

Índice

- Introducción ----- 1-4
- Configuración del servidor ----- 5-7
- Configuración de clientes ----- 7-14
- Configuración de puerto de operación -----16
- Certificados de operación -----16-18

Introducción

¿Qué es FTP?

FTP es otro protocolo de este tipo, y viene a significar “Protocolo de transferencia de archivos” (“File Transfer Protocol”). Es uno de los protocolos más antiguos en uso hoy en día, y es una forma conveniente de mover archivos. Un servidor FTP ofrece acceso a un directorio con subdirectorios. Los usuarios se conectan a estos servidores con un cliente FTP, una pieza de software que les permite descargar archivos del servidor, así como cargar archivos en él.

¿Qué es Vsftpd?

Vsftpd significa “Very Secure FTP Daemon” (Demonio FTP muy seguro), y es un servidor FTP para Linux y otros sistemas operativos UNIX. Como el nombre indica, se trata de un servidor de este tipo mucho más seguro que los estándares, además de que ofrece varias opciones interesantes.

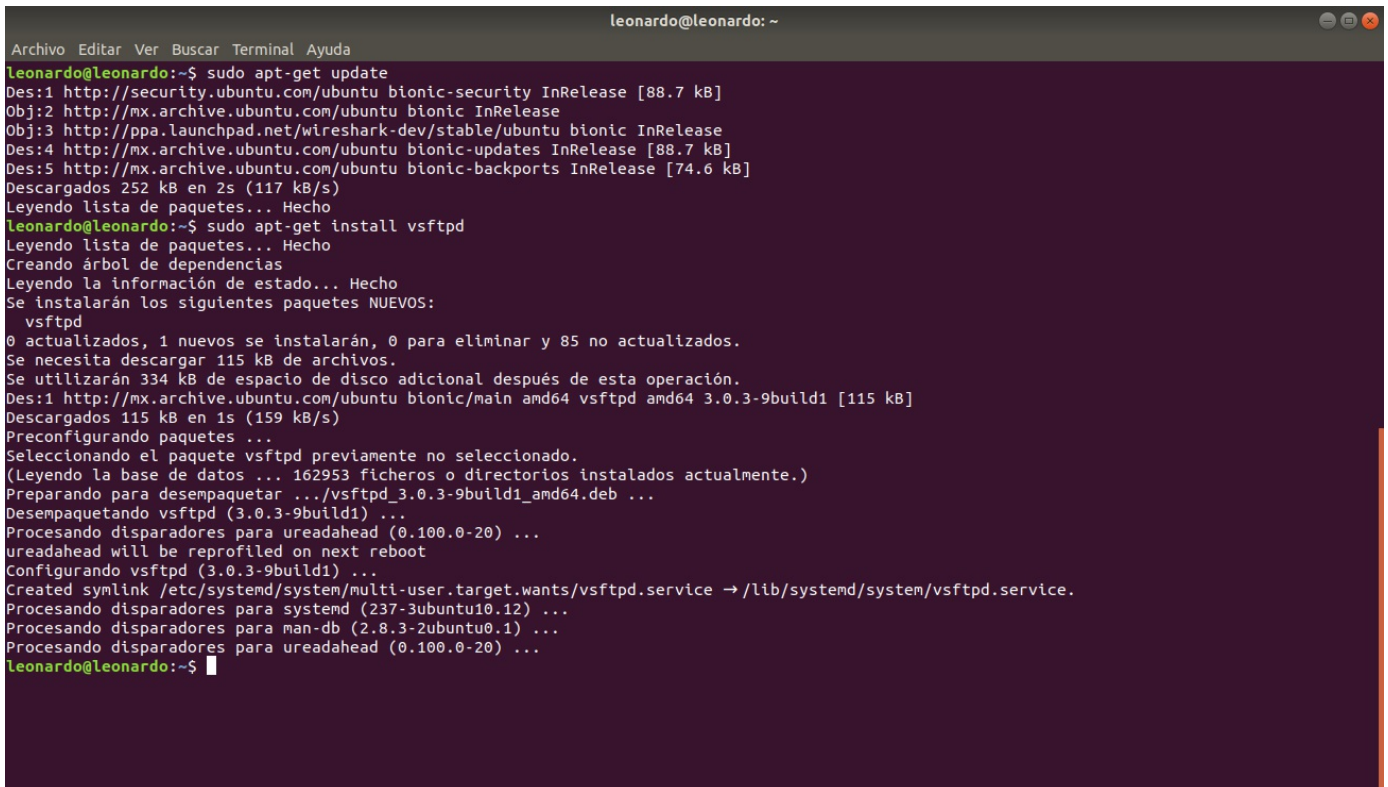
Requisitos

- Ubuntu 18.04
- Vsftpd versión 3.0.5

Instalación

1. Necesitamos instalar el servidor vsftpd y para esto utilizaremos el comando:

```
sudo apt-get install vsftpd
```

A terminal window titled 'leonardo@leonardo: ~' showing the installation of vsftpd. The user first runs 'sudo apt-get update', which updates the package lists. Then, they run 'sudo apt-get install vsftpd'. The terminal output shows that vsftpd is being installed along with its dependencies. It indicates that 115 kB of space is needed and that the package will be installed. The installation process includes downloading the package, preparing it for installation, and creating a symlink for the service. The terminal output is as follows:

```
leonardo@leonardo:~$ sudo apt-get update
Des:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Obj:2 http://mx.archive.ubuntu.com/ubuntu bionic InRelease
Obj:3 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic InRelease
Des:4 http://mx.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Des:5 http://mx.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Descargados 252 kB en 2s (117 kB/s)
Leyendo lista de paquetes... Hecho
leonardo@leonardo:~$ sudo apt-get install vsftpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  vsftpd
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 85 no actualizados.
Se necesita descargar 115 kB de archivos.
Se utilizarán 334 kB de espacio de disco adicional después de esta operación.
Des:1 http://mx.archive.ubuntu.com/ubuntu bionic/main amd64 vsftpd amd64 3.0.3-9build1 [115 kB]
Descargados 115 kB en 1s (159 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete vsftpd previamente no seleccionado.
(Leyendo la base de datos ... 162953 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../vsftpd_3.0.3-9build1_amd64.deb ...
Desempaquetando vsftpd (3.0.3-9build1) ...
Procesando disparadores para ureadahead (0.100.0-20) ...
ureadahead will be reprofiled on next reboot
Configurando vsftpd (3.0.3-9build1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Procesando disparadores para systemd (237-3ubuntu10.12) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
Procesando disparadores para ureadahead (0.100.0-20) ...
leonardo@leonardo:~$
```

2. Después de que instalamos los paquetes y componentes necesarios debemos ejecutar el servidor con el comando:

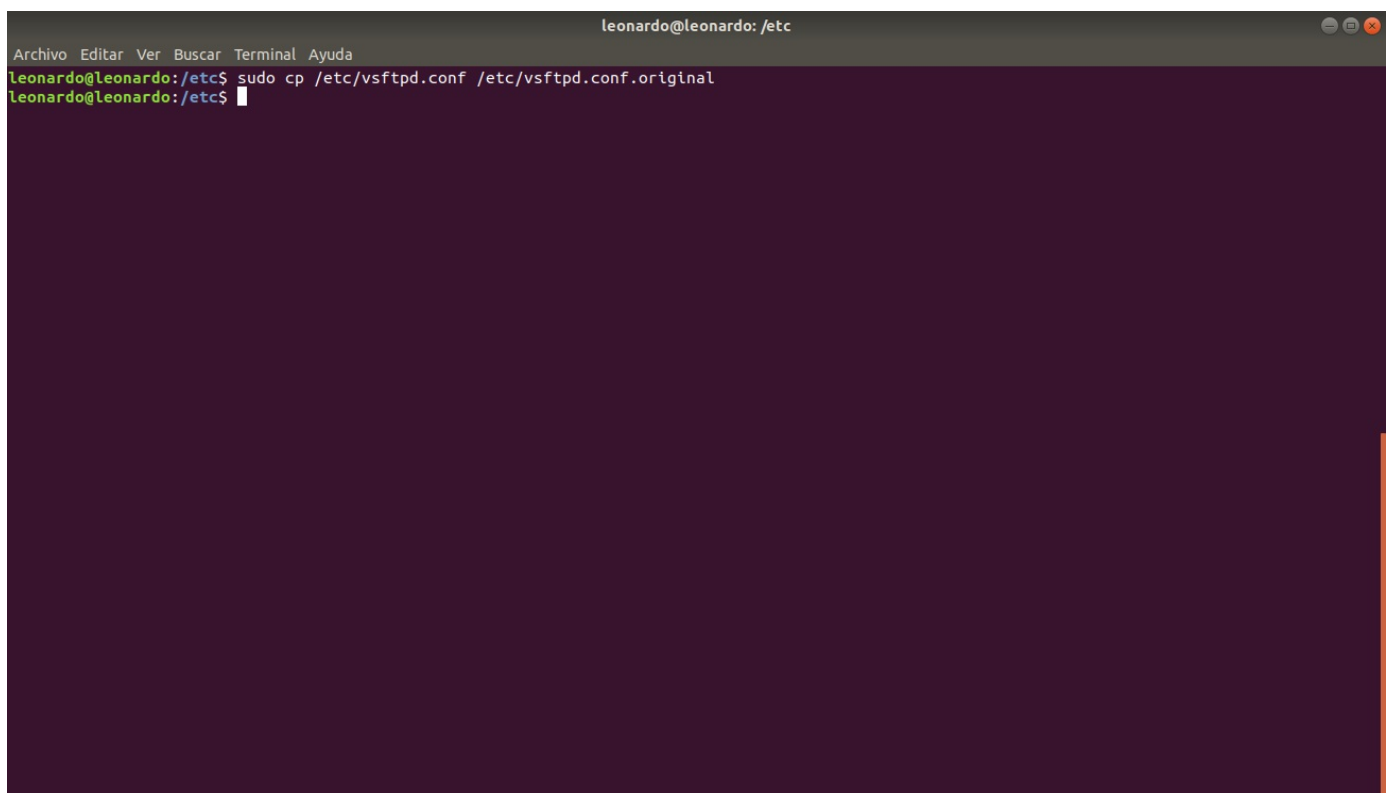
```
sudo service vsftpd start
```

Antes de empezar a modificar nuestro archivo de configuración, por seguridad es necesario que hagamos una copia de respaldo.

Para poder hacer esto, escribimos en consola:

```
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original
```

Aquí es la ruta donde se encuentra nuestro archivo.

A screenshot of a terminal window titled 'leonardo@leonardo: /etc'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal shows the command 'sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original' being executed. The prompt changes from 'leonardo@leonardo:/etc\$' to 'leonardo@leonardo:/etc\$' after the command is run, with a cursor at the end. The terminal background is dark purple.

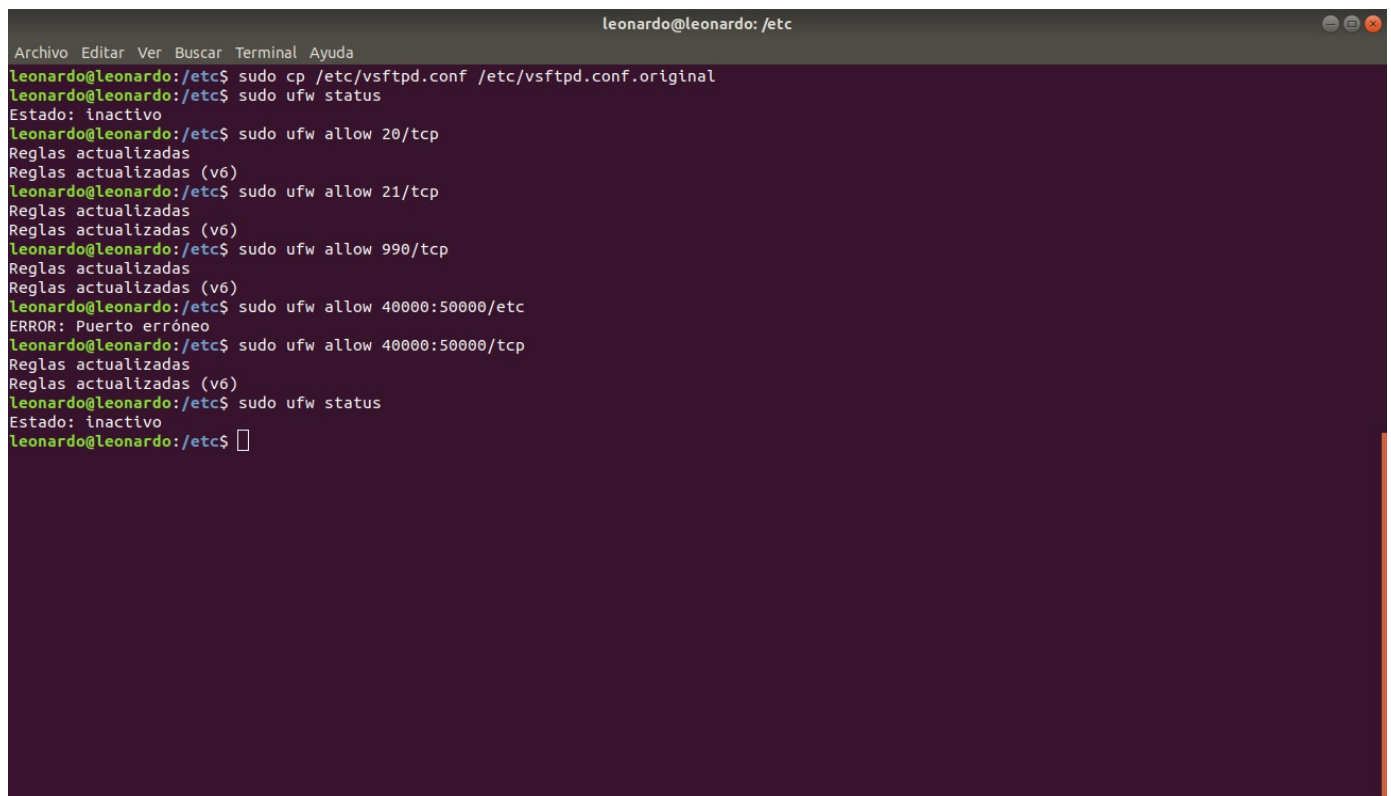
Antes de revisar el estado de nuestro servidor es necesario que verifiquemos si los puertos que vamos a ocupar están abiertos, o que no hay problema con el Firewall de ubuntu.

```
sudo ufw status <-- Con este comando nos permite saber si  
nuestro cortafuegos está activo
```

Para poder abrir los puertos que utilizaremos escribimos:

```
sudo ufw allow 20/tcp
```

```
sudo ufw allow 21/tcp
```

A terminal window titled 'leonardo@leonardo: /etc' with a menu bar (Archivo, Editar, Ver, Buscar, Terminal, Ayuda). The terminal shows the following commands and output:

```
leonardo@leonardo:/etc$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original
leonardo@leonardo:/etc$ sudo ufw status
Estado: inactivo
leonardo@leonardo:/etc$ sudo ufw allow 20/tcp
Reglas actualizadas
Reglas actualizadas (v6)
leonardo@leonardo:/etc$ sudo ufw allow 21/tcp
Reglas actualizadas
Reglas actualizadas (v6)
leonardo@leonardo:/etc$ sudo ufw allow 990/tcp
Reglas actualizadas
Reglas actualizadas (v6)
leonardo@leonardo:/etc$ sudo ufw allow 40000:50000/etc
ERROR: Puerto erróneo
leonardo@leonardo:/etc$ sudo ufw allow 40000:50000/tcp
Reglas actualizadas
Reglas actualizadas (v6)
leonardo@leonardo:/etc$ sudo ufw status
Estado: inactivo
leonardo@leonardo:/etc$
```

Para poder revisar el estado de nuestro servidor, si está activo, es necesario que ingresemos el siguiente comando:

```
sudo service vsftpd status
```

```
leonardo@leonardo: /etc
Archivo Editar Ver Buscar Terminal Ayuda
leonardo@leonardo:/etc$ sudo systemctl start vsftpd
leonardo@leonardo:/etc$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2019-03-07 18:30:43 CST; 17min ago
     Main PID: 5805 (vsftpd)
       Tasks: 1 (limit: 4424)
    CGroup: /system.slice/vsftpd.service
            └─5805 /usr/sbin/vsftpd /etc/vsftpd.conf

mar 07 18:30:43 leonardo systemd[1]: Starting vsftpd FTP server...
mar 07 18:30:43 leonardo systemd[1]: Started vsftpd FTP server.
leonardo@leonardo:/etc$
```

Configuración del archivo vsftpd

Nuestro archivo vsftpd.conf en realidad es muy simple de configurar, ya que cada línea es un comentario o directiva, para poder diferenciar si es una directiva o un comentario, los comentarios inician con el siguiente simbolo: #

Una directiva línea directiva tiene el formato:

Opción = valor.

Es muy importante tomar en cuenta que es un error colocar cualquier espacio entre la opción, = y el valor.

La especificación de todas las opciones las podemos consultar en la liga: “Directivas de vsftpd.conf”

Las directivas que utilizaremos para nuestro servidor, son las siguientes:

1. `listen_port=20`
2. `listen=N0`
3. `listen_ipv6=YES`
4. `anonymous_enable=N0`
5. `local_enable=YES`
6. `write_enable=YES`
7. `dirmessage_enable=YES`
8. `use_localtime=YES`
9. `chown_uploads=YES`
10. `ascii_upload_enable=YES`
11. `ftpd_banner=Mensaje de Bienvenida`
12. `chroot_local_user=YES`
13. `secure_chroot_dir=/var/run/vsftpd/empty`
14. `pam_service_name=vsftpd`

1. Este es el puerto en el que se escuchará las conexiones entrantes de FTP. Por defecto es el puerto 21.
2. Permite que vsftpd se ejecute de manera independiente, es decir, no debe ejecutarse desde un **inetd** de algún tipo.
3. Ejecutará el servidor de manera independiente, con la diferencia de que con esta directiva el servidor escuchara en un socket IPv6 en lugar de un IPv4.
4. Controla si los inicios de sesión anónimos están permitidos o no. Si esta habilitado, los nombres de usuario ftp y Anonymous se reconocen como inicios de sesión anónimos.
5. Si esta habilitado, las cuentas de usuario normales que se encuentran en el archivo /etc/passwd se pueden usar para

iniciar sesión.

6. Controla si se permiten o no los comandos FTP que cambian el sistema de archivos.
7. Permite que los usuarios del servidor FTP puedan mostrar mensajes cuando ingresan por primera vez a un nuevo directorio.
8. Permite que las listas de los directorios sean mostrados con la hora de la zona horaria local.
9. Todos los archivos cargados de manera anónima cambiarán la propiedad al usuario que se especifiquen en `chown_username`.
10. Es importante habilitar esta directiva para la carga de archivos en clientes Windows.
11. Es importante habilitar esta directiva para la descarga de archivos en clientes Windows.
12. Esto habilita el mensaje de bienvenida para los clientes que se conecten al servidor.
13. Esto permite el manejo de jaulas para los usuarios que indiquemos.
14. Este directorio se usa como una jaula segura de **chroot()**
15. Es el nombre del servicio PAM

Para poder acceder al archivo `vsftpd.conf` ejecutamos el siguiente comando:

```
sudo nano /etc/vsftpd.conf
```

Después cada cambio que hagamos a nuestro servidor es necesario que reiniciemos el servidor de esta manera:

```
sudo service vsftpd restart
```

Configuración de clientes

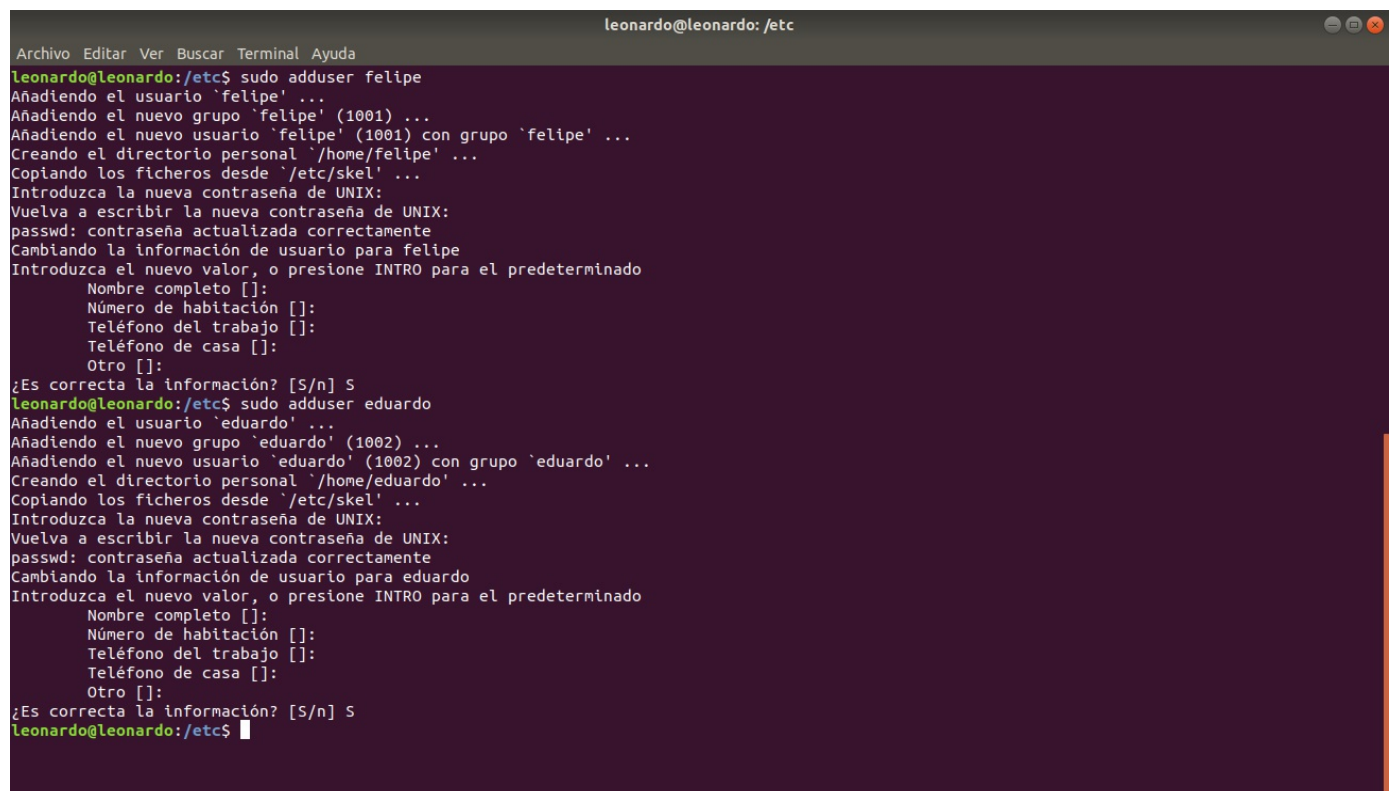
Para poder agregar usuarios en nuestra terminal escribimos:

sudo adduser usuario

```
sudo adduser felipe
```

```
sudo adduser eduardo
```

Se les va a asignar un directorio a cada usuario, en este caso `/home/usuario`, el cual también se le conoce como chroot del usuario.



```
leonardo@leonardo: /etc
Archivo Editar Ver Buscar Terminal Ayuda
leonardo@leonardo:/etc$ sudo adduser felipe
Añadiendo el usuario 'felipe' ...
Añadiendo el nuevo grupo 'felipe' (1001) ...
Añadiendo el nuevo usuario 'felipe' (1001) con grupo 'felipe' ...
Creando el directorio personal '/home/felipe' ...
Copiando los ficheros desde '/etc/skel' ...
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para felipe
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []:
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] S
leonardo@leonardo:/etc$ sudo adduser eduardo
Añadiendo el usuario 'eduardo' ...
Añadiendo el nuevo grupo 'eduardo' (1002) ...
Añadiendo el nuevo usuario 'eduardo' (1002) con grupo 'eduardo' ...
Creando el directorio personal '/home/eduardo' ...
Copiando los ficheros desde '/etc/skel' ...
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para eduardo
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []:
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] S
leonardo@leonardo:/etc$
```

Enjaular a los usuarios

Es muy importante que realizemos este procedimiento para poder

mantener la seguridad en los archivos del resto de usuarios y del servidor, debido a que si los usuarios son agregados al servidor como en el paso anterior tendrán acceso a diversas carpetas que se encuentren en el.

Al utilizar jaulas nos garantizará que los usuarios solo podrán hacer uso de ciertos directorios.

Para poder enjaular a nuestros usuarios usaremos la siguiente sentencia:

sudo chown root:root /home/usuario/

```
sudo chown root:root /home/eduardo
sudo chown root:root /home/felipe
```

De esta manera indicamos que ahora el dueño de la carpeta es el usuario root, después procedemos a crear un directorio nuevo para el usuario, para subir y descargar sus archivos, solo en esta carpeta podrá hacer dichas acciones.

```
sudo mkdir /home/felipe/nuevo
sudo mkdir /home/eduardo/nuevo
```

Después tenemos que asignar un dueño a la carpeta que creamos, para ello utilizamos el comando:

sudo chown usuario:usuario /home/usuario/nuevo

```
sudo chown felipe:felipe /home/felipe/nuevo/
sudo chown eduardo:eduardo /home/eduardo/nuevo/
```

```
leonardo@leonardo: /etc
Archivo Editar Ver Buscar Terminal Ayuda
leonardo@leonardo:/etc$ sudo chown root:root /home/felipe/
leonardo@leonardo:/etc$ sudo chown root:root /home/eduardo/
leonardo@leonardo:/etc$ sudo mkdir /home/felipe/nuevo/
leonardo@leonardo:/etc$ sudo mkdir /home/eduardo/nuevo/
leonardo@leonardo:/etc$ sudo chown felipe:felipe /home/felipe/nuevo/
leonardo@leonardo:/etc$ sudo chown eduardo:eduardo /home/eduardo/nuevo/
leonardo@leonardo:/etc$
```

Por seguridad es importante quitar el acceso al interprete de comandos (shell) del usuario, nos generaría un problema al momento de acceder al servicio FTP, el usuario no tendría una shell válida, por lo tanto le creamos una.

```
** sudo nano /bin/shellusuario**
```

```
sudo nano /bin/felipe
sudo nano /bin/eduardo
```

Una vez que se ha creado la shell, debemos dar los permisos de ejecución a la shell.

```
** sudo chmod a+x /bin/usuario**
```

```
sudo chmod a+x /bin/felipe
sudo chmod a+x /bin/eduardo
```

```
leonardo@leonardo: /etc
Archivo Editar Ver Buscar Terminal Ayuda
leonardo@leonardo:/etc$ sudo nano /bin/felipe
leonardo@leonardo:/etc$ sudo nano /bin/eduardo
leonardo@leonardo:/etc$ sudo chmod a+x /bin/felipe
leonardo@leonardo:/etc$ sudo chmod a+x /bin/eduardo
leonardo@leonardo:/etc$
```

Se debe agregar la shell que se ha creado para cada usuario en la lista de shells del sistema.

```
sudo nano /etc/shells
```

Nos debe quedar como esto:

```
leonardo@leonardo: /etc
GNU nano 2.9.3 /etc/shells

/etc/shells: valid login shells
/bin/sh
/bin/bash
/bin/rbash
/bin/dash
/bin/felipe
/bin/eduardo

[ 7 líneas leídas ]
^G Ver ayuda  ^O Guardar  ^W Buscar  ^K Cortar Texto  ^J Justificar  ^C Posición  ^M-U Deshacer  ^M-A Marcar text  ^M-] A llave
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar txt  ^T Ortografía  ^_ Ir a línea  ^M-E Rehacer  ^M-G Copiar txt  ^M-W Siguiente
```

Finalmente tenemos que asignar la shell creada a los usuarios, mediante.

```
sudo usermod usuario -s /bin/usuario
sudo usermod felipe -s /bin/felipe
```

```
leonardo@leonardo: /etc
Archivo Editar Ver Buscar Terminal Ayuda
leonardo@leonardo:/etc$ sudo nano /bin/felipe
leonardo@leonardo:/etc$ sudo nano /bin/eduardo
leonardo@leonardo:/etc$ sudo chmod a+x /bin/felipe
leonardo@leonardo:/etc$ sudo chmod a+x /bin/eduardo
leonardo@leonardo:/etc$ sudo nano /etc/shells
leonardo@leonardo:/etc$ sudo nano /etc/shells
leonardo@leonardo:/etc$ sudo usermod felipe -s /bin/felipe
leonardo@leonardo:/etc$ sudo usermod eduardo -s /bin/eduardo
leonardo@leonardo:/etc$
```

Restricciones de acceso

Para poder restringir el acceso, es necesario acceder al archivo `host.deny`, se encuentra en:

```
sudo nano /etc/hosts.deny
```

Donde vamos a escribir la siguiente línea:

vsftpd: 192.168.45.36

La ip es la del cliente a la cual se le denegará el servicio

```
leonardo@leonardo: /etc
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3 /etc/hosts.deny Modificado

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example: ALL: some.host.name, .some.domain
# ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
vsftpd: 192.168.100.8
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar ^C Posición ^M-U Deshacer ^M-A Marcar text ^M-J A llave
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^ Ir a línea ^M-E Rehacer ^M-G Copiar txt ^M-W Siguiente
```

Restringir acceso al recurso por usuario

Para poder hacer esto, es necesario habilitar algunas directivas en nuestro archivo vsftpd.conf, las cuales son:

userlist_enable=YES

Con esto activa la lista de usuarios para que la configuración del servidor la reconozca.

userlist_deny=YES

Habilitamos la lista de usuarios contendrá los usuarios a los que se les va a restringir el acceso

userlist_file=/etc/vsftpd.denied_users

Establece el archivo en el cual se escribirá el nombre de los usuarios que no tendrán acceso al servicio.

Por último creamos el archivo vsftpd.denied_users

```
sudo nano /etc/vsftpd.denied_users
```

```
leonardo@leonardo: /etc
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3 /etc/vsftpd.conf

# default.
#
# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
userlist_enable=YES
userlist_deny=YES
userlist_file=/etc/vsftpd.denied_users
#
#
#
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES

```

Identificación requerida



ftp://192.168.1.83 está solicitando tu usuario y contraseña.

Nombre de usuario:

Contraseña:

Restringir el acceso al recurso por grupo de usuarios

Debemos crear un grupo, con el siguiente comando:

```
sudo groupadd group
```

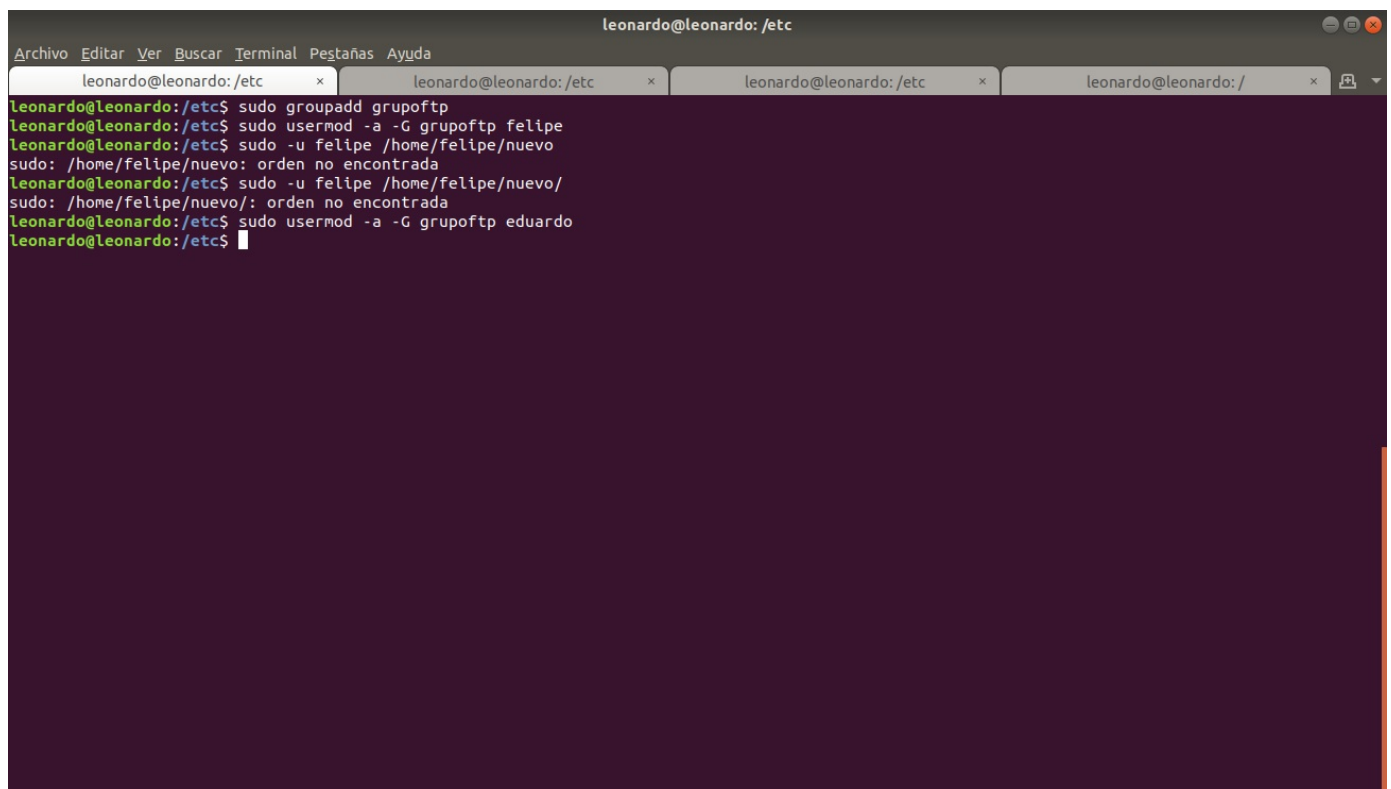
Procedemos a crear el grupo con nuestros usuarios que tenemos.

```
sudo groupadd grupoftp
sudo usermod -a -G grupoftp felipe
sudo -u felipe /home/felipe/nuevo/
```

Después editamos el siguiente archivo `/etc/pam.d/vsftpd` y agregamos la siguiente línea:

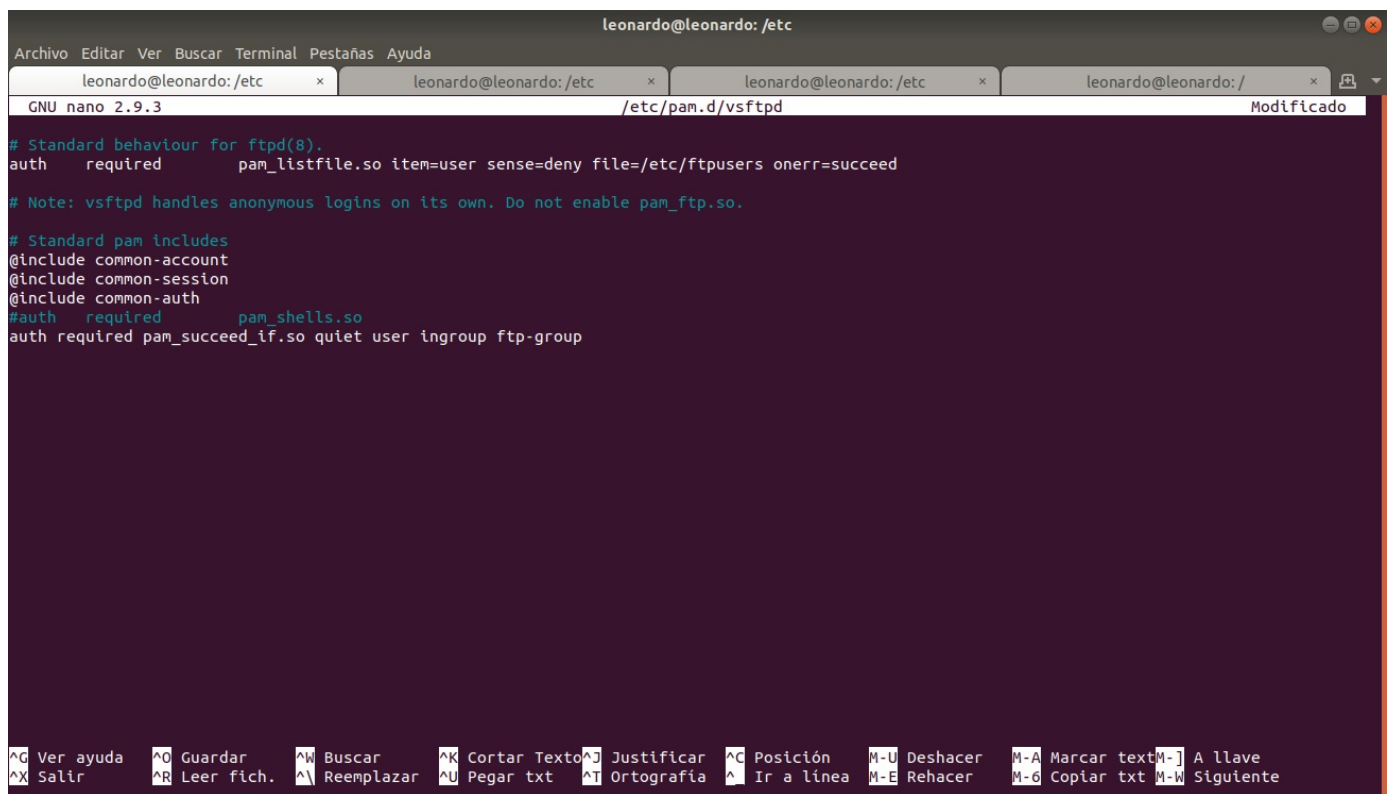
```
auth required pam_succeed_if.so quiet user ingroup ftp-group
```

Tomando en cuenta que el último parámetro es el nombre del grupo

A screenshot of a terminal window titled 'leonardo@leonardo: /etc'. The terminal shows the following commands and output:

```
leonardo@leonardo:/etc$ sudo groupadd grupoftp
leonardo@leonardo:/etc$ sudo usermod -a -G grupoftp felipe
leonardo@leonardo:/etc$ sudo -u felipe /home/felipe/nuevo
sudo: /home/felipe/nuevo: orden no encontrada
leonardo@leonardo:/etc$ sudo -u felipe /home/felipe/nuevo/
sudo: /home/felipe/nuevo/: orden no encontrada
leonardo@leonardo:/etc$ sudo usermod -a -G grupoftp eduardo
leonardo@leonardo:/etc$
```

The terminal window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', 'Pestañas', and 'Ayuda'. There are three tabs open, all titled 'leonardo@leonardo: /etc'. The terminal background is dark purple with light green text.



```
leonardo@leonardo: /etc
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
leonardo@leonardo: /etc x leonardo@leonardo: /etc x leonardo@leonardo: /etc x leonardo@leonardo: /etc x
GNU nano 2.9.3 /etc/pam.d/vsftpd Modificado

# Standard behaviour for ftpd(8).
auth required pam_listfile.so item=user sense=deny file=/etc/ftpusers onerr=succeed

# Note: vsftpd handles anonymous logins on its own. Do not enable pam_ftp.so.

# Standard pam includes
@include common-account
@include common-session
@include common-auth
#auth required pam_shells.so
auth required pam_succeed_if.so quiet user ingroup ftp-group

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar ^C Posición M-U Deshacer M-A Marcar text M-J A llave
^X Salir ^R Leer fich. ^Y Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea M-E Rehacer M-6 Copiar txt M-W Siguiente
```

Configuración de puerto de operación

Para la configuración del puerto, tenemos la directiva

listen_port=21

Por default nuestro puerto de configuración es el 21, para agregar esta directiva accedemos al archivo vsftpd.conf y la escribimos al inicio del archivo.

Sin olvidar que tenemos que reiniciar el servidor cada que hagamos un cambio.

```
sudo service vsftpd restart
```

Certificados de operación

Para garantizar la seguridad de la transmisión de datos en cargas y descargas de archivos de los usuarios, es importante manejar certificados cifrados que permitan encriptar los archivos en el transporte.

Para configurar los certificados se hace lo siguiente:

Se debe realizar la petición de certificado por medio de OpenSSL con el siguiente comando:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -  
keyout  
/etc/ssl/private/ftps_vsftpd.pem -out  
/etc/ssl/private/ftps_vsftpd.pem
```

Una vez que se ha realizado la petición se solicitarán una serie de datos, los cuales pueden ser los que el usuario desee.

Ya con el certificado firmado, se deben de agregar al archivo vsftpd.conf las siguientes directivas:

ssl_enable=YES

Habilita el uso de certificados SSL.

ssl_tlsv1=YES

Habilita el cifrado con TLS version 1, el cual es el cifrado que se recomienda en la documentación y de mayor seguridad, además de tener alto grado de compatibilidad.

force_local_data_ssl=YES

Permite que las operaciones en el servidor, como lo son carga, descarga, creación, entre

otras, sean bajo el cifrado que especificamos.

force_local_logins_ssl=YES

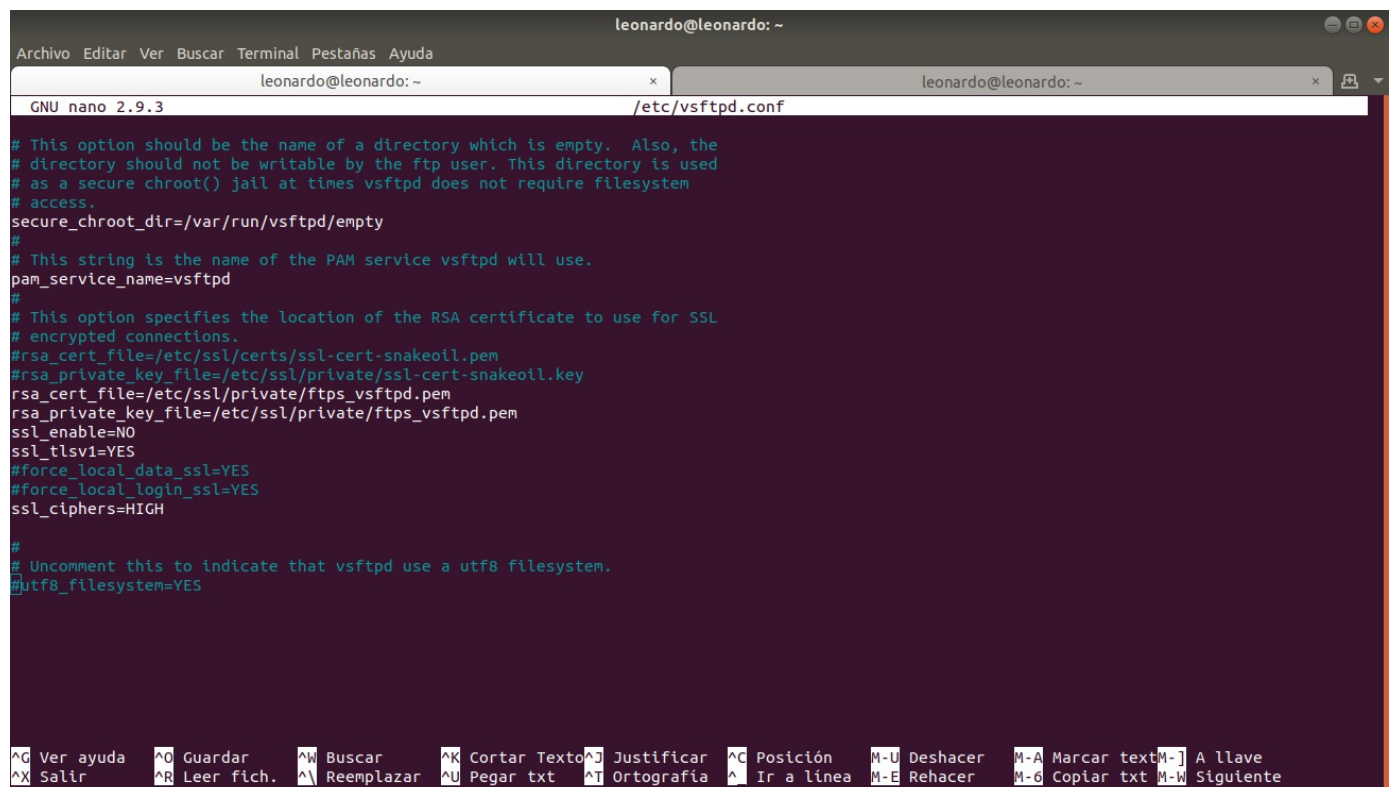
Permite que los inicios de sesión en el servidor sean forzados a usar el cifrado que se

especificó.

ssl_ciphers=HIGH

Especifica el nivel de seguridad que requerimos tanto para las sesiones, como para las

operaciones que se realicen en el servidor. En este caso usaremos el nivel más alto.

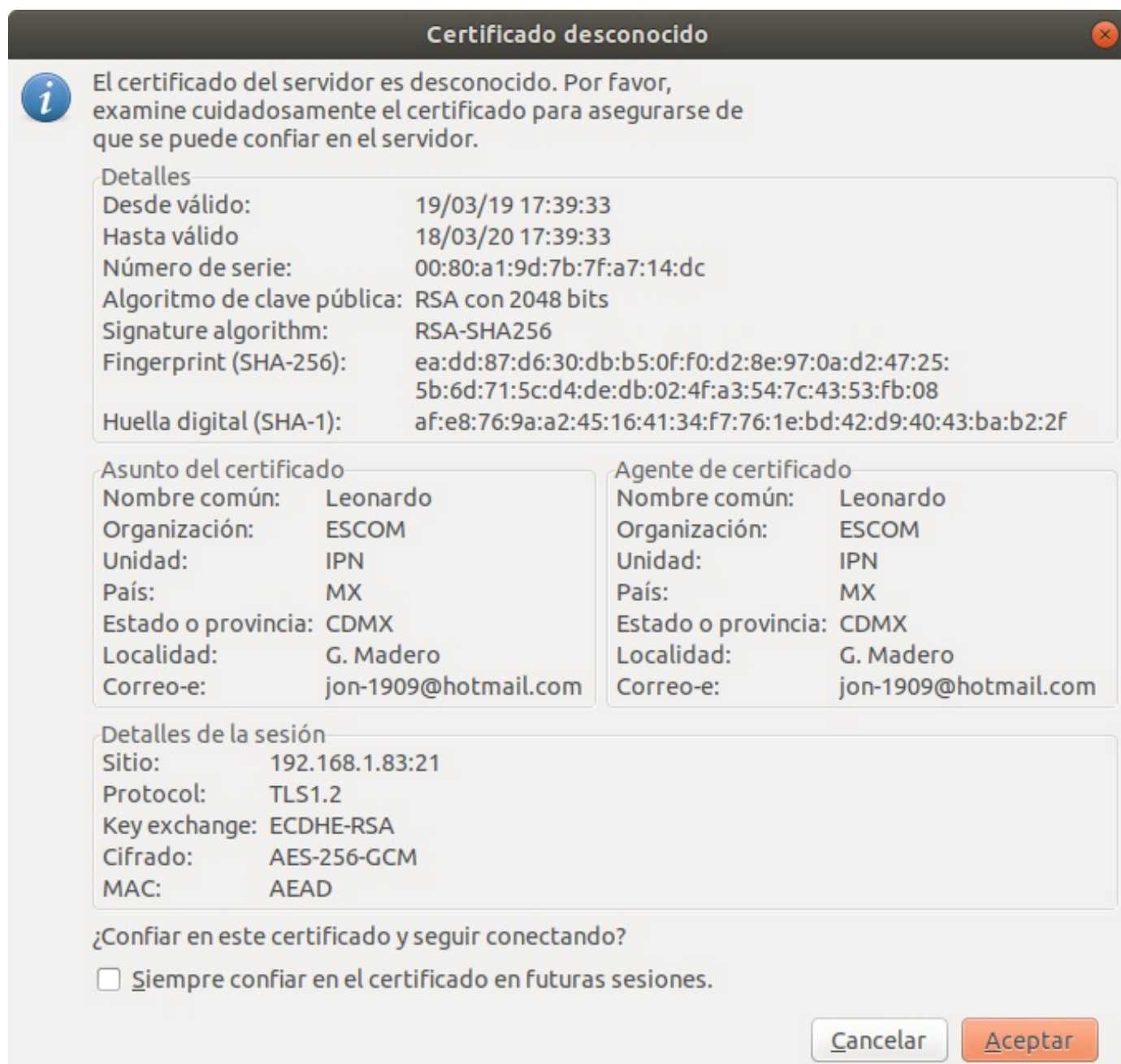


```
leonardo@leonardo: ~
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
leonardo@leonardo: ~ /etc/vsftpd.conf
GNU nano 2.9.3

# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
rsa_cert_file=/etc/ssl/private/ftps_vsftpd.pem
rsa_private_key_file=/etc/ssl/private/ftps_vsftpd.pem
ssl_enable=NO
ssl_tlsv1=YES
#force_local_data_ssl=YES
#force_local_login_ssl=YES
ssl_ciphers=HIGH

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar ^C Posición M-U Deshacer M-A Marcar text M-J A llave
^X Salir ^R Leer fich. ^Y Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea M-E Rehacer M-6 Copiar txt M-W Siguiete
```



Configuración de los sistemas de registro de acceso al sistema.

El registro que se tiene de las operaciones que ejecuta el servidor FTP con vsftpd tiene 3 niveles de operación de bitácoras principales. A continuación, se explicará que registra cada uno de estos niveles, la configuración para habilitarlos y que diferencia a un

nivel del otro.

Al termino de cada configuración se debe de reiniciar y revisar el estado del servicio.

vsftpd.log

Este archivo es el que la mayoría de las veces se utiliza, ya que permite registrar la conexión

de los usuarios, la carga y descarga de archivos, la información acerca del certificado (si se

configura en el archivo vsftpd.log y si se ha configurado el certificado), así como las

operaciones fallidas que usuarios intentaron hacer y estas fueron denegadas o canceladas.

Para poder configurar este nivel de bitácora es necesario configurar las siguientes directivas

xferlog_enable=YES

Directiva que habilitara el registro en el archivo.

vsftpd_log_file=/var/log/vsftpd.log

Archivo donde se realizará el registro.

debug_ssl=YES

Si se ha configurado el certificado SSL, esta directiva permitirá registrar las

operaciones que se realizan con el certificado.

// Imagen sobre el log aquí.

xferlog

A diferencia del nivel de bitacora mencionado en el inciso anterior, este nivel solo registrara

el manejo de los archivos por parte de los usuarios, asi como las

operaciones que se realicen
entre ellos, como lo son la carga y la descarga.

Para configurar este nivel de bitácora es necesario configurar las
siguientes directivas en el

archivo vsftpd.conf

xferlog_enable=YES

Se le da el mismo uso que en el nivel de bitácora anterior.

xferlog_std_format=YES

Esta directiva habilitara el archivo xferlog con el formato estándar.

xferlog_file=/var/log/xferlog.log

Archivo donde se realizará el registro.

// inserte imagen aquí

syslog

En el caso de ubuntu 18.04 se existe el archivo syslog donde se
registran todas las
operaciones que se realizan en el sistema. En este archivo registran las
operaciones que se
realizan en el servidor FTP.

Para configurarlo se debe agregar siguiente directiva:

syslog_enable=YES

Indica que todo el registro de operación del servidor, se enviara al
archivo

syslog ubicado en el directorio /var/log. Es importante mencionar que, si
se

habilita esta directiva en conjunto con las directivas para los niveles de
bitácora anteriores, el registro se realizara en syslog y no en los
archivos

vsftpd.log y xferlog.

```
leonardo@leonardo: ~
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
leonardo@leonardo: ~ x leonardo@leonardo: ~
GNU nano 2.9.3 /etc/vsftpd.conf

connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
xferlog_file=/var/log/vsftpd.log
debug_ssl=YES
syslog_enable=YES
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_enable=YES
xferlog_std_format=YES
xferlog_file=/var/log/xferlog.log
#
# You may change the default value for timing out an idle session.
idle_session_timeout=60
#1 minuto sin hacer nada, desconecta
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar ^C Posición M-U Deshacer M-A Marcar text M-J A llave
^X Salir ^R Leer fich. ^A Reemplazar ^U Pegar txt ^T Ortografía ^I Ir a línea M-E Rehacer M-6 Copiar txt M-W Sigulente
```

```
leonardo@leonardo: ~
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
leonardo@leonardo: ~ x leonardo@leonardo: ~
GNU nano 2.9.3 /var/log/syslog

Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: Reply with serial 23
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Request successful
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Requesting busy
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: Reply with serial 24
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Request successful, cookie is 938851567
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Requesting idle
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: Reply with serial 25
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Request successful
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Requesting busy
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: Reply with serial 26
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Request successful, cookie is 1408505174
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Requesting idle
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: Reply with serial 27
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Request successful
Mar 22 20:37:38 leonardo filezilla.desktop[2373]: wxD-Bus: CPowerManagementInhibitor: Requesting busy
Mar 22 20:37:38 leonardo vsftpd[3187]: [alejandro] OK LOGIN: Client "::ffff:192.168.1.83"
Mar 22 20:39:04 leonardo vsftpd[3199]: [alejandro] OK LOGIN: Client "::ffff:192.168.1.83"
Mar 22 20:39:04 leonardo vsftpd[3201]: [alejandro] OK UPLOAD: Client "::ffff:192.168.1.83", "/nuevo/10.png", 164292 bytes, 23353.92Kbyte/sec
Mar 22 20:39:06 leonardo vsftpd[3201]: [alejandro] OK UPLOAD: Client "::ffff:192.168.1.83", "/nuevo/12.png", 119103 bytes, 10752.66Kbyte/sec
Mar 22 20:39:08 leonardo vsftpd[3201]: [alejandro] OK UPLOAD: Client "::ffff:192.168.1.83", "/nuevo/13.png", 126288 bytes, 10263.66Kbyte/sec
Mar 22 20:39:10 leonardo org.gnome.Shell.desktop[1287]: Window manager warning: Window 0x3803490 (El archivo) sets an MWM hint indicating it $
Mar 22 20:39:10 leonardo org.gnome.Shell.desktop[1287]: message repeated 2 times: [ Window manager warning: Window 0x3803490 (El archivo) set$
Mar 22 20:39:25 leonardo vsftpd[3211]: [alejandro] OK LOGIN: Client "::ffff:192.168.1.83"
Mar 22 20:39:25 leonardo vsftpd[3213]: [alejandro] OK DELETE: Client "::ffff:192.168.1.83", "/nuevo/13.png"
Mar 22 20:40:51 leonardo gvfsd-metadata[2221]: g_udev_device_has_property: assertion 'G_UDEV_IS_DEVICE (device)' failed
Mar 22 20:40:51 leonardo gvfsd-metadata[2221]: message repeated 7 times: [ g_udev_device_has_property: assertion 'G_UDEV_IS_DEVICE (device)' $
Mar 22 20:40:51 leonardo gvfsd[1249]: mkdir failed on directory /var/cache/samba: Permiso denegado
Mar 22 20:40:51 leonardo gvfsd[1249]: message repeated 6 times: [ mkdir failed on directory /var/cache/samba: Permiso denegado]
Mar 22 20:40:51 leonardo systemd-resolved[573]: Using degraded feature set (UDP) for DNS server 192.168.1.254.
Mar 22 20:40:56 leonardo gvfsd[1249]: mkdir failed on directory /var/cache/samba: Permiso denegado

```

Referencias

[Directivas de vsftpd.conf](#)

[Uso del Firewall en Ubuntu](#)

[Configuración del servidor vsftpd](#)

[Vsftpd log](#)

[Opciones de configuración vsftpd](#)

[How to View System Log Files on Ubuntu 18.04 LTS](#)

Glosario

- `inetd` <-- Inetd es un **demonio** presente en la mayoría de sistemas tipo Unix, conocido como el “Super Servidor de Internet”, ya que gestiona las conexiones de varios demonios.
- `demonio` <-- Es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario.