PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (FTP)

Protocolo de transferencia de archivos entre sistemas conectados a una red TCP/IP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él, o para enviarle nuestros propios archivos; independientemente del sistema operativo utilizado en cada equipo.

FTP (file Transfer Protocol)

- Utiliza el puerto
  - 20: Para transferencia de datos al cliente
  - 21: Para escuchar las peticiones del cliente

En Linux se cuenta con varias opciones para instalar un servidor FTP como: proftpd, vsftpd, pure-ftpd, muddleftpd, tftp, y otras

TFTPD (Trivial FTP Daemon)

- Protocolo de transferencia simple (versión básica)
- Conexiones UDP
- No existe mecanismo de autenticación o cifrado

VSFTPD (Very secure FTP daemon)

- Sus valores por defecto son muy seguros
- Puede ejecutarse en los modos standalone o inetd
- Considerado el servidor FTP más seguro
- Conexiones TCP
- Encriptación por medio de SSL (Secure Socket Layer)
- Permite establecer usuarios enjaulados

ProFTPD(Professional FTP daemon)

- Es configurable y seguro
- Puede ejecutarse en los modos standalone o inetd
- Conexiones TCP
- Permite escribir extensiones como cifrado SSL (Secure Socket Layer), TLS (Transport Layer Security), LDAP (lightweight Directory Access Protocol), SQL (Structured Query Language)
- Permite configurar servicios virtuales

ProFTPD(Professional FTP daemon)

Instalación:

Apt-get install proftpd	Servidor Ftp
Apt-get install ftp	Cliente Ftp

Administrar el servicio ftp: ***service proftpd (start|stop|restart …)***
systemctl (start|stop|restart …) proftpd

Para Acceder desde un cliente Ftp a un servidor Ftp: ***ftp <Ip del servidor Ftp>***

Archivos básicos de configuración

- */etc/proftpd.conf* *:Configuración general*
- */etc/ftpusers* *:Usuarios para negar el acceso*
- */var/log/proftpd.log, /var/log/xferlog* *:Mensajes de Conexiones ProFTP*

Comandos de Gestión

- *Ftpcount: muestra la cantidad de conexiones actuales*
- *Ftptop: muestra el estado de ejecución de las conexiones*

- *Ftpwho: muestra información de los procesos actuales para cada sesión*
- *Ftpshut: baja el servicio de FTP, y no permite nuevas conexiones*

Un servidor Proftpd permite configurar el servicio mediante bloques de directivas, que permiten personalizar con de forma estructurada y ordenada la parametrización el servicio.

Bloques de Directivas

<Limit LOGIN> Order Allow, Dny Allow from 192.168.1.2, … Deny from all DenyUser pedro, juan </Limit>	Limitar a quienes pueden intentar entrar al servidor ftp
<Directory /mnt/datos> <Limit CWD DIRS … RETR> AllowAll DenyAll </Limit> </Directory>	Especificar las propiedades de una carpeta del sitio ftp
<Anonymous /home/ftp> </Anonimous>	Definición de un sitio anónimo. Se puede realizar dentro del bloque "Directory"

Servidores Virtuales

<global> </global>	Parámetros globales que afectan a todos los directorios virtuales
<VirtualHost Nombre o IP> </VirtualHost>	Parámetros de un directorio virtual

Parámetros de Configuración

ServerName "Nombrer"	Nombre del Servidor, aparece en el programa cliente
ServerType standalone ServerType inetd	Tipo de inicio del servicio, Standalone (Se inicia como un servidor autónomo), Inetd (se inicia desde el superdemonio de inicio)
DeferWelcome off/on	Activa (On) o desactiva (Off) el mensaje de bienvenida del servidor.
ServerIdent on/off "nombre"	Activa o desactiva el nombre de la distribución que aparece en el cliente y que ejecuta el proftpd. Se puede personalizar con un nombre.
DefaultServer on/off	Para indicar que el servidor ejecute las opciones por defecto.
ShowSymlinks on/off	Muestra o no los links para saltar a las carpetas del sitio. Si los links son externos no funcionaran.
<Directory /*> AllowOverwrite on </Directory>	Especifica que en ese directorio se pueden sobrescribir los ficheros existentes.
TimeoutLogin <numero>	Número de segundos que espera el servidor en recibir nombre de usuario y contraseña antes de desconectar al cliente.
TimeoutNoTransfer <numero>	Número de segundos que puede estar conectado un cliente, sin realizar una transferencia de información.
TimeoutStalled <numero>	Número de segundos que puede estar el servidor sin recibir información de una transferencia del cliente (atascado).

TimeoutIdle <numero>	Número de segundos que puede estar un cliente sin hacer nada.
Port <numero>	Puerto por el que escucha el proceso servidor.
MaxInstances <numero>	Número de conexiones que se pueden hacer a la vez al servidor.
MaxClients <numero> "mensage"	Número de clientes que pueden estar conectados a la vez en el servidor. **"Mensaje"** es el texto que envía al cliente si no permite la conexión.
MaxClientsPerHost <numero> "mensage"	Número de sesiones por Host (ip) que se pueden conectar al servidor. **"Mensaje"** es el texto que envía al cliente si no permite la conexión.
MaxClientsPerUser <numero> "mensage"	Número de sesiones por usuario. **"Mensaje"** es el texto que aparece en el cliente si no permite la conexión.
User nobody	Usuario que usa el servidor. Es el que se debe usar en los permisos de carpetas y ficheros.
Group nogroup	Grupo que usa el servidor. Es el que se debe usar en los permisos de carpetas y ficheros.
Umask 022	Evita que los nuevos directorios y ficheros se creen con permisos de escritura para el grupo y otros.
AccessGrantMsg "mensage"	Mensaje que se envía a los clientes que acceden al servidor con una identificación correcta.
AccessDenyMsg "mensage"	Mensaje que se envía a los clientes que acceden al servidor con una identificación incorrecta.
DisplayLogin <fichero>	Fichero de texto con el mensaje de bienvenida a los clientes que accedan al servidor.
DisplayFirstChdir <fichero>	Fichero de texto con el mensaje de explicación del contenido del directorio al que se han accedido.
TransferLog /var/log/proftpd/transfer	Fichero de texto donde se almacena la auditoria (Log) de Transferencias del servidor.
SystemLog /var/log/proftpd.log	Fichero de texto donde se almacenan las respuestas del servidor.
DefaultRoot <Ruta>	Directorio donde se envía a los usuarios registrados en el servidor.
AuthUserFile "/etc/passwd"	Localización del fichero de los usuarios.
AuthGroupFile "/etc/group"	Localización del fichero de los grupos de usuarios.
<Limit LOGIN> Order Allow,Deny Allow from 212.155.209.139, pepito.com Deny from all DenyUser pedro,juana </Limit>	Limitamos a quienes pueden intentar entrar en el servidor. Con la etiqueta ORDER le decimos el orden de lectura de la información, 1º A quien aceptamos y 2º A quien denegamos La etiqueta Allow from marca los host que queremos acptar separados por una coma. La etiqueta Deny from a quien vamos a rechazar, en este caso all que representa a todas las ip's. La etiqueta DenyUser especifica los usuarios a los que queremos restringir el acceso.
<Directory /datos/subir> <Limit CWD DIRS READ WRITE MKD RMD DELE STOR RETR> AllowAll DenyAll </Limit> </Directory>	Especifica las propiedades en una carpeta del sitio ftp. Estos permisos se complementan con los permisos que localmente tiene la carpeta. CWD: Cambiar de Directorio. DIRS: Conocer el contenido de un directorio. READ: Lectura WRITE: Escritura MKD: Crear Directorios RMD: Borrar Directorios DELE: Borrar ficheros. STOR: Enviar ficheros al servidor. RETR: Recuperar ficheros del servidor.
<global> </global>	Parámetros globales que afectarán a todos los directorios virtuales.

<VirtualHost Nombre o IP> </VirtualHost>	Definición de un directorio virtual.
<Anonymous Directorio> </Anonymous>	Definición del sitio Anónimo
UserAlias anonymous proftpd	Alias de nombres definidos para acceder al servidor como usuario anónimo.

VSFTPD (Very secure FTP daemon)

Archivos básicos de configuración

- */etc/vsftpd.conf : Configuración general*
- */etc/vsftpd.chroot_list : Lista de usuarios enjaulados*
- */etc/vsftpd.user_list : Lista de usuario que se les niega o se les permite el servicio FTP*
- */etc/vsftpd.banned_emails : Direcciones de correo que se niega el servicio FTP*
- */var/log/vsftpd.log : Mensajes de conexiones de servicio vsftpd*

Parámetros de Configuración: Parámetros que permiten personalizar el servicio VsFtpd

anonymous_enable=YES	Permite que los usuarios anónimos se conecten. Se aceptan los nombres de usuario anonymous y ftp
cmds_allowed	Especifica una lista delimitada por comas de los comandos FTP que permite el servidor. Se rechaza el resto de los comandos
write_enable=YES	Determina si se permite el mandato write (escritura) en el servidor
local_enable=YES	Este parámetro es particularmente atractivo si se combina con la función de jaula. Establece si se van a permitir los accesos autenticados de los usuarios locales del sistema
listen_port=2121 listen=YES connect_from_port_20=YES	*listen_port* permite cambiar el puerto por el que escucha el servidor. por defecto es el puerto 21. *listen=YES* permite configurar el servidor en modo standalone. Se puede configurar el puerto 20 que es el original del servidor ftp para transferencia de datos
ftp_data_port=20	Puerto utilizado por las conexiones de datos
userlist_enable=YES userlist_deny = YES userlist_file= /etc/vsftpd.user_list	El fichero vsftpd.user_list contiene una lista de usuarios. Si la directiva *serlist_deny=NO* contiene la lista de usuarios que únicamente se le permite el acceso. Si *userlist_deny=YES* contiene la lista de usuarios que no se le permiten hacer ftp
chroot_local_user=YES	Hace que el usuario no pueda navegar por el árbol completo de directorios, se enjaula al usuario autenticado en su directorio $HOME
chroot_local_user=YES chroot_list_enable=YES chroot_list_file=/etc/vsftpd/vsftpd.chroot_list	Si se desea que los usuarios solo poedan utilizar su propio directorio personal, puede hacerse con el parámetro *chroot_local_user* que habilitará la función de *chroot()* y los parámetros chroot_list_enable y chroot_list_file para establecer el fichero con la lista de usuarios que quedarán excluidos de la función *chroot()*
deny_email_enable = YES banned_email_file= /etc/vsftpd.chroot_list	Negar el acceso a las direcciones de correo, especificadas en la directriz banned_list_file
ftpd_banner=Bienvenido al servidor FTP	Establece el banderín de bienvenida que será mostrado cada vez que un usuario acceda al servidor.
port_enable=YES	Especifica las conexiones de FTP, en modo activo (existen dos modos Activo y Pasivo)

Gestión de Red

anon_max_rate=5120	Limitar la tasa de transferencia en bytes por segundo, para los usuarios

	anónimos
local_max_rate=5120	Limitar la tasa de transferencia en bytes por segundo, para los usuarios locales del servidor
max_clients=5	Número máximo de clientes simultáneos que tienen permitido conectarse al servidor (0 es ilimitado)
max_per_ip=5	Máximo número de clientes que tienen permitido conectarse desde la misma dirección IP
connect_timeout=60	Cantidad máxima de tiempo que un cliente tiene para responder a una conexión de datos, en segundos (valor predeterminado 60 segundos)
data_connection_timeout	Cantidad máxima de tiempo que las conexiones se pueden aplazar en segundos (valor predeterminado 300 segundos)
idle_session_timeout	Cantidad máxima de tiempo entre comandos desde un cliente remoto (valor predeterminado 300)
listen_address	Dirección IP en la cual vsftpd escucha por las conexiones de red

Otros Criterios del servicio FTP

anon_mkdir_write_enable =YES	los usuarios anónimos pueden crear nuevos directorios, dentro del directorio que tienen permiso de escritura
anon_upload_enable= NO	Cuando se usa con la directriz write_enable, los usuarios anónimos pueden cargar archivos al directorio padre que tiene permisos de escritura
anon_world_readable_only=YES	los usuarios anónimos solamente pueden descargar archivos legibles por todo el mundo
no_anon_password=YES	No se le pide una contraseña al usuario anónimo
chmod_enable=YES	Permite que los usuarios cambien los permisos en los archivos
guest_enable=YES	Todos los usuarios anónimos se conectan como guest
guest_username=User	Especifica el nombre de usuario al cual guest está asignado
local_umask=022	Valor de umask para la creación de archivos
dirlist_enable=YES	Los usuarios pueden ver los listados de directorios.
hide_ids =YES	Todos los listados de directorios muestran ftp como el usuario y grupo para cada archivo
text_userdb_names=YES	Se utilizan los nombres de usuarios y grupos en lugar de sus entradas UID o GID
use_localtime=YES	Los listados de directorios revelan la hora local para el computador
download_enable=YES	Se permiten las descargas de archivos
chown_uploads=YES	Todos los archivos cargados por los usuarios anónimos pertenecen al usuario especificado en la directriz chown_username
chown_username=User	Especifica la propiedad de los archivos cargados anónimamente (valor predeterminado es root)
ls_recurse_enable = YES	Habilitar Listado recursivo
syslog_enable	En conjunto con xferlog_enable, todos los registros que se escriben al archivo estándar especificado en la directriz vsftpd_log_file, se envían al registro del sistema.
xferlog_enable=YES vsftpd_log_file= /var/log/vsftpd.log	Activa el registro de las conexiones Especifica el archivo gestión de registro del servicio VsFtp