FTP SERVER LINUX

📙Descargar PDF

- Referencias

Guía completa de vsftpd en Debian 11 – Usuarios, Grupos y Carpetas Virtuales

Esta guía permite instalar y configurar **vsftpd** en Debian 11, incluyendo usuarios locales y virtuales, grupos, carpetas compartidas y virtuales, permisos, firewall, modo pasivo y FTPS básico.

Introducción a vsftpd

vsftpd (Very Secure FTP Daemon) es un servidor FTP para sistemas Linux/Unix conocido por su seguridad, estabilidad y buen rendimiento. Permite:

- Acceso anónimo y autenticado.
- Restricción de usuarios a sus directorios (chroot).
- Uso de usuarios locales y virtuales.
- Soporte de FTP sobre TLS/SSL (FTPS).
- Configuración de modos activo y pasivo.

Archivos principales de configuración

- `/etc/vsftpd.conf` : archivo principal con todas las directivas de configuración.
- `/etc/pam.d/vsftpd` : archivo PAM para autenticación de usuarios locales.
- `/etc/pam.d/vsftpd.virtual` : archivo PAM para usuarios virtuales.
- `/etc/vsftpd/virtual_users.txt` y `/etc/vsftpd/virtual_users.db` : usuarios virtuales y base de datos PAM.

La configuración de vsftpd se realiza modificando `vsftpd.conf` y reiniciando el servicio con `systemctl restart vsftpd` .

---

1. Instalación de vsftpd

Se actualiza el sistema e instala vsftpd junto con herramientas para gestionar usuarios virtuales (`db-util`).

```
sudo apt update && sudo apt upgrade -y
sudo apt install vsftpd db-util -y
sudo systemctl enable vsftpd
sudo systemctl start vsftpd
sudo systemctl status vsftpd
```

Explicación: Se asegura que el sistema está actualizado y se instala el servidor FTP seguro, además de habilitarlo para iniciar automáticamente.

---

2. Configuración básica

Archivo `/etc/vsftpd.conf`:

```
listen=YES
listen_ipv6=NO
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
allow_writeable_chroot=YES
xferlog_enable=YES
xferlog_file=/var/log/vsftpd.log
ftpd_banner=Bienvenido al servidor FTP
```

Explicación: Se activa la escucha en IPv4, se deshabilita el acceso anónimo, se permiten usuarios locales y escritura, se restringe a los usuarios a su directorio (chroot) y se configuran los logs y mensaje de bienvenida.

Reiniciar:

```
sudo systemctl restart vsftpd
```

---

3. Tabla de directivas importantes de vsftpd

Directiva	Valor típico	Descripción
listen	YES / NO	Activa el modo escucha en IPv4.
listen_ipv6	YES / NO	Escucha en IPv6. Normalmente NO si no se usa IPv6.
anonymous_enable	YES / NO	Permite o deniega acceso anónimo.
local_enable	YES / NO	Permite usuarios locales.
write_enable	YES / NO	Permite subir, renombrar y borrar archivos.
chroot_local_user	YES / NO	Restringe a los usuarios a su home.
allow_writeable_chroot	YES / NO	Permite escritura dentro del chroot.
xferlog_enable	YES / NO	Habilita logs de transferencia.
ftpd_banner	Texto	Mensaje mostrado al conectar.
pasv_enable	YES / NO	Habilita modo pasivo para clientes detrás de NAT/firewall.
pasv_min_port / pasv_max_port	30000-30100	Rango de puertos pasivos.

Directiva	Valor típico	Descripción
guest_enable	YES / NO	Permite que usuarios virtuales se mapeen a un usuario del sistema.
guest_username	Nombre	Usuario del sistema propietario de virtuales.
virtual_use_local_privs	YES / NO	Usuarios virtuales usan permisos locales.
user_sub_token	$USER	Token para carpetas virtuales de cada usuario.
local_root	Ruta	Carpeta raíz para un usuario o virtual.
ssl_enable	YES / NO	Habilita FTPS.
rsa_cert_file / rsa_private_key_file	Ruta	Certificados para FTPS.
force_local_data_ssl / force_local_logins_ssl	YES / NO	Obliga cifrado de datos y login.

Explicación: Esta tabla permite consultar rápidamente las directivas más importantes y cómo afectan al funcionamiento del servidor.

---

4. Usuarios locales y grupos

4.1 Crear grupo y usuarios

```
sudo groupadd ftpgroup
sudo adduser ftpuser1 --ingroup ftpgroup
sudo adduser ftpuser2 --ingroup ftpgroup
```

Explicación: Se crea un grupo para manejar permisos compartidos y se añaden usuarios locales al grupo.

4.2 Crear carpeta compartida

```
sudo mkdir -p /srv/ftp/shared
sudo chown root:ftpgroup /srv/ftp/shared
sudo chmod 770 /srv/ftp/shared
```

Explicación: Carpeta donde los miembros del grupo pueden leer/escribir, pero otros usuarios no tienen acceso.

4.3 Carpetas personales

```
sudo mkdir -p /home/ftpuser1/files
sudo mkdir -p /home/ftpuser2/files
sudo chown ftpuser1:ftpgroup /home/ftpuser1/files
sudo chown ftpuser2:ftpgroup /home/ftpuser2/files
sudo chmod 750 /home/ftpuser1/files /home/ftpuser2/files
```

Explicación: Carpetas privadas para cada usuario, donde sólo el propietario y grupo tienen acceso según los permisos configurados.

---

5. Carpetas virtuales y usuarios virtuales

5.1 ¿Qué son las carpetas virtuales?

Las carpetas virtuales son directorios que no corresponden al home de un usuario del sistema, sino que se asignan a **usuarios virtuales**. Los usuarios virtuales no existen en Linux, pero vsftpd los mapea a un **usuario del sistema** (`guest_username`) para manejar permisos.

- Cada usuario virtual puede tener su propio directorio dentro de `/srv/ftp` .
- Se usan tokens (`$USER`) para aislar carpetas de cada usuario virtual.

5.2 Crear usuarios virtuales y base de datos

Archivo `/etc/vsftpd/virtual_users.txt` :

```
vuser1
vuser1pass
vuser2
vuser2pass
```

Convertirlo en base de datos PAM:

```
sudo db_load -T -t hash -f /etc/vsftpd/virtual_users.txt /etc/vsftpd/virtual_users.db
sudo chmod 600 /etc/vsftpd/virtual_users.db
```

Configurar PAM en `/etc/pam.d/vsftpd.virtual` :

```
auth required pam_userdb.so db=/etc/vsftpd/virtual_users
account required pam_userdb.so db=/etc/vsftpd/virtual_users
```

5.3 Crear usuario del sistema para carpetas virtuales

```
sudo adduser ftpguest --home /srv/ftp
sudo groupadd ftpvirtual
sudo usermod -aG ftpvirtual ftpguest
```

5.4 Crear carpetas virtuales por usuario

```
sudo mkdir -p /srv/ftp/vuser1 /srv/ftp/vuser2
sudo chown ftpguest:ftpvirtual /srv/ftp/vuser1 /srv/ftp/vuser2
sudo chmod 770 /srv/ftp/vuser1 /srv/ftp/vuser2
```

Explicación: Cada usuario virtual accede a su propia carpeta. `ftpguest` es propietario y el grupo `ftpvirtual` controla acceso a nivel de grupo.

5.5 Configuración en vsftpd.conf

```
guest_enable=YES
guest_username=ftpguest
virtual_use_local_privs=YES
user_sub_token=$USER
local_root=/srv/ftp/$USER
```

Explicación: Permite que cada usuario virtual se conecte solo a su carpeta virtual, aislado de otros usuarios.

5.6 Carpetas compartidas por grupo

Se puede crear una carpeta que solo miembros de un grupo accedan:

```
sudo groupadd ftpgroup1
sudo groupadd ftpgroup2
sudo adduser ftpuser1 --ingroup ftpgroup1
sudo adduser ftpuser2 --ingroup ftpgroup2
sudo mkdir -p /srv/ftp/shared1 /srv/ftp/shared2
sudo chown root:ftpgroup1 /srv/ftp/shared1
sudo chown root:ftpgroup2 /srv/ftp/shared2
sudo chmod 770 /srv/ftp/shared1 /srv/ftp/shared2
```

Explicación: Solo los miembros del grupo correspondiente pueden leer y escribir en la carpeta compartida.

---

6. Configuración modo pasivo

```
pasv_enable=YES
pasv_min_port=30000
pasv_max_port=30100
```

Explicación: Habilita modo pasivo y define el rango de puertos que los clientes usarán para transferencias detrás de firewalls/NAT.

---

7. Firewall con iptables

```
sudo iptables -F
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 20 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
sudo iptables -A INPUT -p tcp --match multiport --dports 30000:30100 -j ACCEPT
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

Explicación: Permite FTP estándar, pasivo y SSH, bloqueando todo lo demás.

8. FTPS básico

```
sudo mkdir -p /etc/ssl/private /etc/ssl/certs
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
    -keyout /etc/ssl/private/vsftpd.key \
    -out /etc/ssl/certs/vsftpd.crt \
    -subj "/C=ES/ST=Madrid/L=Madrid/O=MiEmpresa/OU=IT/CN=ftp.example.com"
```

En `/etc/vsftpd.conf`:

```
ssl_enable=YES
rsa_cert_file=/etc/ssl/certs/vsftpd.crt
rsa_private_key_file=/etc/ssl/private/vsftpd.key
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

Explicación: Genera certificados auto-firmados y fuerza cifrado para logins y datos.

Reiniciar:

```
sudo systemctl restart vsftpd
```

---

9. Ejemplo de conexión

9.1 Usuario de grupo (ftpuser1)

```
ftp 192.168.1.100
# Usuario: ftpuser1
cd /srv/ftp/shared
put archivo.txt
ls
```

9.2 Usuario virtual (vuser1)

```
lftp ftp://vuser1:vuser1pass@192.168.1.100
# cd /    # Inicio en /srv/ftp/vuser1
put ejemplo.txt
ls
```

Explicación: Los usuarios pueden subir y listar archivos en sus carpetas según permisos y tipo de usuario.

---

10. Permisos sobre carpetas y archivos

```
sudo chown ftpuser1:ftpgroup /home/ftpuser1/files
sudo chmod 750 /home/ftpuser1/files
sudo chown root:ftpgroup /srv/ftp/shared
sudo chmod 770 /srv/ftp/shared
sudo chown ftpguest:ftpvirtual /srv/ftp/vuser1
sudo chmod 770 /srv/ftp/vuser1
```

Explicación: Se asegura separación de permisos y control de acceso a nivel de usuario y grupo.

---

11. Solución de problemas

- Login fallido: `/var/log/auth.log` y `/var/log/vsftpd.log`
- Permisos denegados: revisar propietario, grupo y `allow_writeable_chroot=YES`
- Problemas pasivo detrás de NAT: puertos 30000-30100 abiertos en iptables
- FTPS falla: verificar certificados y rutas en vsftpd.conf

---

12. Conclusión

Servidor vsftpd listo con:

- Usuarios locales y grupos.
- Usuarios virtuales con carpetas virtuales independientes.
- Carpetas compartidas y permisos claros.
- Modo activo/pasivo funcional.
- FTPS básico habilitado.
- Firewall iptables configurado.

Referencias

- Documentación oficial de vsftpd
- Guía Debian vsftpd
- LDAP / bases de datos relacionales para autenticación centralizada.