

FTP SERVER LINUX

 [Descargar PDF](#)

▼ FTP SERVER LINUX

- SERVIDORES FTP EN LINUX

▼ EL SERVIDOR VSFTPD

▼ INSTALACIÓN DEL SERVIDOR

- INSTALACIÓN
- ESTRUCTURA DE DIRECTORIOS Y ARCHIVOS

▼ CONFIGURACIÓN

- PARÁMETROS PRINCIPALES

▼ GESTIÓN DE USUARIOS

- USUARIOS DEL SISTEMA
- Gestión de usuarios del sistema
- Usuarios virtuales
- Seguridad en VSFTPD

- EL SERVIDOR PURE-FTPD

SERVIDORES FTP EN LINUX

En entornos GNU/Linux existen varias implementaciones del protocolo FTP, cada una con un enfoque distinto en cuanto a seguridad, flexibilidad, rendimiento y facilidad de administración. Las soluciones más consolidadas y mantenidas son:

- **vsftpd** (*Very Secure FTP Daemon*)

Diseñado con un enfoque prioritario en la **seguridad y la simplicidad**. Es el servidor FTP predeterminado en distribuciones como RHEL, CentOS y Ubuntu para entornos que requieren estabilidad y una superficie de ataque mínima. Opera exclusivamente con usuarios del sistema y delega en el sistema operativo funciones avanzadas como cuotas de disco o control de acceso por red. Resulta especialmente adecuado para escenarios con pocos usuarios técnicos o accesos internos controlados.

- **Pure-FTPd**

Combina **facilidad de uso con funcionalidades avanzadas**, manteniendo un alto nivel de seguridad. Ofrece soporte nativo para **usuarios virtuales, cuotas de disco por usuario, límites de ancho de banda individuales** y una configuración modular basada en archivos independientes. Es ideal para entornos multiusuario —como hosting o servicios compartidos— donde no se desea crear cuentas reales en el sistema.

- **ProFTPD**

Inspirado en la arquitectura de Apache, proporciona una **gran flexibilidad mediante módulos** que permiten integración con SQL, LDAP, cuotas, logs personalizados, y reglas complejas de acceso (por IP, horario, clase de usuario, etc.). Aunque potente y altamente configurable, su curva de aprendizaje es más pronunciada. Se considera una opción sólida para entornos empresariales con requisitos específicos, aunque queda fuera del alcance de este documento.

Este documento se centra en **vsftpd** y **Pure-FTPd** por representar dos enfoques contrastados pero ampliamente utilizados: uno minimalista y orientado a la seguridad del sistema, y otro orientado a la gestión práctica de múltiples usuarios sin comprometer la robustez del servicio.

EL SERVIDOR VSFTPD

El servidor `vsftpd` es una de las opciones más populares y seguras para implementar un servicio FTP en sistemas GNU/Linux. Su diseño se centra en minimizar la superficie de ataque, lo que lo convierte en una opción ideal para entornos donde la seguridad es una prioridad. La gestión de usuarios se puede llevar a cabo de dos maneras:

- **Mediante las cuentas del sistema**, donde cada usuario FTP corresponde a una cuenta de usuario del sistema operativo. Esto simplifica la administración de permisos y la integración con otras herramientas del sistema, pero requiere una cuidadosa gestión de usuarios para evitar riesgos de seguridad.
- **Mediante usuarios virtuales**, utilizando PAM para mapear sesiones FTP a un único usuario del sistema. Esta opción es más compleja de configurar pero permite una mayor flexibilidad y aislamiento entre usuarios.

INSTALACIÓN DEL SERVIDOR

INSTALACIÓN

El servidor `vsftpd` está disponible en los repositorios oficiales de la mayoría de las distribuciones GNU/Linux, lo que facilita su instalación. Nosotros nos centraremos en las **distribuciones basadas en Debian**, aunque el

Este proceso es similar en otras distribuciones. Para instalar `vsftpd` utilizaremos el gestor de paquetes `apt` que es el más común en sistemas basados en Debian.

```
apt install vsftpd
```

Este comando instala `vsftpd` como servidor autónomo, sin necesidad de instalar paquetes adicionales. El proceso de instalación también configura el servicio para que se inicie automáticamente al arrancar el sistema. Podemos verificar que el servicio se ha instalado correctamente y está activo utilizando el siguiente comando:

```
systemctl status vsftpd
```

ESTRUCTURA DE DIRECTORIOS Y ARCHIVOS

Una vez instalado, `vsftpd` crea la siguiente estructura de directorios y archivos:

- `/etc/vsftpd.conf` — Archivo de configuración principal del servicio
- `/etc/vsftpd/` — Directorio que contiene archivos de configuración adicionales (listas de usuarios, configuraciones específicas, etc.)
- `/var/log/vsftpd.log` — Archivo de registro de actividades del servidor
- `/srv/ftp/` — Directorio raíz por defecto para usuarios anónimos (puede variar según configuración)
- `/etc/pam.d/vsftpd` — Configuración de PAM para autenticación de usuarios

Además, dependiendo de la configuración, pueden existir otros archivos y directorios relacionados con la gestión de usuarios virtuales, certificados SSL para FTPS, o scripts personalizados para eventos específicos.

CONFIGURACIÓN

La configuración de `vsftpd` se centraliza en un único archivo principal: `/etc/vsftpd.conf`. Este archivo es un archivo de texto plano que contiene **directivas clave-valor**. Cada línea define una opción específica del servidor, y el formato es simple e intuitivo. Los comentarios comienzan con el carácter `#` y se ignoran. Las líneas en blanco también se ignoran. He aquí un ejemplo de estructura básica:

Configuración básica

```
# Habilitar acceso anónimo
anonymous_enable=YES

# Habilitar usuarios locales
local_enable=YES

# Permitir comandos de escritura
write_enable=YES

# Directorio raíz para usuarios locales
local_root=/home/ftp
```

PARÁMETROS PRINCIPALES

Los parámetros en `vsftpd.conf` controlan diversos aspectos del comportamiento del servidor, desde la autenticación y el control de acceso hasta la configuración de puertos y la seguridad. A continuación se describen

algunos de los parámetros más importantes agrupados por categorías. Para una descripción completa de cada parámetro, se recomienda consultar la documentación oficial de `vsftpd` o el manual (`man vsftpd.conf`).

Control de acceso anónimo

Parámetro	Descripción
<code>anonymous_enable</code>	Habilita o deshabilita el acceso anónimo.
<code>anon_root</code>	Especifica el directorio raíz para usuarios anónimos.
<code>anon_upload_enable</code>	Permite o deniega la capacidad de los usuarios anónimos para subir archivos.
<code>anon_mkdir_write_enable</code>	Permite o deniega la capacidad de los usuarios anónimos para crear directorios.

Control de usuarios locales

Parámetro	Descripción
<code>local_enable</code>	Habilita o deshabilita el acceso para usuarios locales.
<code>local_root</code>	Especifica el directorio raíz para usuarios locales.
<code>chroot_local_user</code>	Enjaula a los usuarios locales en su directorio raíz.
<code>allow_writeable_chroot</code>	Permite que los usuarios locales tengan permisos de escritura incluso cuando están enjaulados.
<code>write_enable</code>	Permite o deniega la capacidad de los usuarios locales para subir archivos.

Puertos y modos de conexión

Parámetro	Descripción
<code>listen_port</code>	Especifica el puerto en el que el servidor escucha las conexiones FTP.
<code>pasv_enable</code>	Habilita o deshabilita el modo pasivo para transferencias de datos.
<code>pasv_min_port</code>	Especifica el puerto mínimo para conexiones pasivas.
<code>pasv_max_port</code>	Especifica el puerto máximo para conexiones pasivas.
<code>port_enable</code>	Habilita o deshabilita el modo activo para transferencias de datos.

Transferencia de datos

Parámetro	Descripción
<code>ascii_upload_enable</code>	Permite o deniega la capacidad de subir archivos en modo ASCII.
<code>ascii_download_enable</code>	Permite o deniega la capacidad de descargar archivos en modo ASCII.

Registro y auditoría

Parámetro	Descripción
xferlog_enable	Habilita o deshabilita el registro de transferencias de archivos.
xferlog_file	Especifica la ubicación del archivo de registro de transferencias.
log_ftp_protocol	Habilita o deshabilita el registro detallado de comandos FTP.
syslog_enable	Habilita o deshabilita el registro de eventos en el sistema syslog.

Seguridad

Parámetro	Descripción
ssl_enable	Habilita o deshabilita el soporte para conexiones seguras mediante SSL/TLS.

Esta tabla proporciona una visión general de los parámetros más comunes, pero `vsftpd` ofrece una amplia gama de opciones adicionales para personalizar el comportamiento del servidor según las necesidades específicas de cada entorno.

GESTIÓN DE USUARIOS

Como anteriormente hemos comentado, tenemos dos opciones para gestionar los usuarios en `vsftpd`: mediante las **cuentas del sistema** o mediante **usuarios virtuales**. A continuación se describen ambas opciones y sus implicaciones en términos de seguridad y administración.

USUARIOS DEL SISTEMA

En este enfoque, cada usuario FTP corresponde a una cuenta de usuario del sistema operativo. Esto significa que para cada usuario que necesite acceso FTP, se debe crear una cuenta de usuario en el sistema utilizando comandos como `useradd` o `adduser`. Es importante configurar estas cuentas de manera segura, asignándoles un shell de inicio que no permita acceso interactivo (como `/usr/sbin/nologin`) y un directorio raíz adecuado, y asegurándose de que los permisos de los directorios sean adecuados para evitar accesos no autorizados.

Usuario del sistema para FTP

```
useradd -m -d /home/ftp/usuario1 -s /usr/sbin/nologin usuario1
passwd usuario1
```

En este ejemplo, se crea un usuario llamado `usuario1` con un directorio raíz en `/home/ftp/usuario1` y se le asigna un shell que no permite acceso interactivo. Luego se establece una contraseña para el usuario.

Gestión de usuarios del sistema

Usuarios virtuales

Seguridad en VSFTPD

EL SERVIDOR PURE-FTPD