

15.5. Opciones de configuración `vsftpd`

Aún cuando `vsftpd` quizás no ofrezca el nivel de personalización que otros servidores FTP disponible globalmente tienen, `vsftpd` ofrece suficientes opciones para satisfacer la mayoría de las necesidades de un administrador. El hecho de que no está sobrecargado de funcionalidades limita los errores de configuración y de programación.

Toda la configuración de `vsftpd` es manejada por su archivo de configuración, `/etc/vsftpd/vsftpd.conf`. Cada directriz está en su propia línea dentro del archivo y sigue el formato siguiente:

```
<directive>=<value>
```

Para cada directriz, reemplace `<directive>` con una directriz válida y `<value>` con un valor válido.



Importante

No deben existir espacios entre la `<directive>`, el símbolo de igualdad y el `<value>` en una directriz.

Se debe colocar el símbolo de almohadilla (`#`) antes de una línea en comentarios. El demonio ignorará cualquier línea en comentarios.

Para una lista completa de las directrices disponibles, consulte las páginas man para `vsftpd.conf`.



Importante

Para una descripción general de las formas de asegurar `vsftpd`, consulte el capítulo llamado ***Seguridad del servidor*** en el ***Manual de seguridad de Red Hat Enterprise Linux***.

A continuación se presenta una lista de las directrices más importantes dentro de `/etc/vsftpd/vsftpd.conf`. Todas las directrices que no se encuentren explícitamente dentro del archivo de configuración de `vsftpd` se colocan a sus valores por defecto.

15.5.1. Opciones de demonios

La lista siguiente presenta las directrices que controlan el comportamiento general del demonio `vsftpd`.

- `listen` — Cuando está activada, `vsftpd` se ejecuta en modo independiente. Red Hat Enterprise Linux configura este valor a `YES`. Esta directriz no se puede utilizar en conjunto con la directriz `listen_ipv6`.

El valor predeterminado es `NO`.

- `listen_ipv6` — Cuando esta directriz está activada `vsftpd` se ejecuta en modo independiente, pero solamente escucha a los sockets IPv6. Esta directriz no se puede utilizar junto con la directriz `listen`.

El valor predeterminado es `NO`.

- `session_support` — Si está activada, `vsftpd` intentará mantener sesiones de conexión para cada usuario a través de Pluggable Authentication Modules (PAM). Para más información, consulte el [Capítulo 16](#). Si no es necesario hacer sesiones de conexión, el desactivar esta opción hace que `vsftpd` se ejecute con menos procesos y privilegios más bajos.

El valor por defecto es `YES`.

15.5.2. Opciones de conexión y control de acceso

La siguiente es una lista de las directrices que controlan el comportamiento de los inicios de sesión y los mecanismos de control de acceso.

- `anonymous_enable` — Al estar activada, se permite que los usuarios anónimos se conecten. Se aceptan los nombres de usuario `anonymous` y `ftp`.

El valor por defecto es `YES`.

Consulte la [Sección 15.5.3](#) para una lista de las directrices que afectan a los usuarios anónimos.

- `banned_email_file` — Si la directriz `deny_email_enable` tiene el valor de `YES`, entonces esta directriz especifica el archivo que contiene una lista de contraseñas de correo anónimas que no tienen permitido acceder al servidor.

El valor predeterminado es `/etc/vsftpd.banned_emails`.

- `banner_file` — Especifica un archivo que contiene el texto que se mostrará cuando se establece una conexión con el servidor. Esta opción supersede cualquier texto especificado en la directriz `ftpd_banner`.

Esta directriz no tiene un valor predeterminado.

- `cmds_allowed` — Especifica una lista delimitada por comas de los comandos FTP que permite el servidor. Se rechaza el resto de los comandos.

Esta directriz no tiene un valor predeterminado.

- `deny_email_enable` — Si está activada, se le niega el acceso al servidor a cualquier usuario anónimo que utilice contraseñas de correo especificadas en `/etc/vsftpd.banned_emails`. Se puede especificar el nombre del archivo al que esta directriz hace referencia usando la directriz `banned_email_file`.

El valor predeterminado es `NO`.

- `ftpd_banner` — Si está activada, se muestra la cadena de caracteres especificada en esta directriz cuando se establece una conexión con el servidor. `banner_file` puede sobrescribir esta opción.

Por defecto, `vsftpd` muestra su pancarta estándar.

- `local_enable` — Al estar activada, los usuarios locales pueden conectarse al sistema.

El valor por defecto es `YES`.

Consulte la [Sección 15.5.4](#) para una lista de las directrices que afectan a los usuarios locales.

- `pam_service_name` — Especifica el nombre de servicio PAM para `vsftpd`.

El valor predeterminado es `ftp`, sin embargo, bajo Red Hat Enterprise Linux, el valor es `vsftpd`.

- `tcp_wrappers` — Al estar activada, se utilizan TCP wrappers para otorgar acceso al servidor. También, si el servidor FTP está configurado en múltiples direcciones IP, la opción `VSFTPD_LOAD_CONF` se puede utilizar para cargar diferentes archivos de configuración en la dirección IP solicitada por el cliente. Para más información sobre los TCP Wrappers, consulte el [Capítulo 17](#).

El valor predeterminado es `NO`, sin embargo, bajo Red Hat Enterprise Linux el valor está configurado a `YES`.

- `userlist_deny` — Cuando se utiliza en combinación con la directriz `userlist_enable` y con el valor de `NO`, se les niega el acceso a todos los usuarios locales a menos que sus nombres esten listados en el archivo especificado por la directriz `userlist_file`. Puesto que se niega el acceso antes de que se le pida la contraseña al cliente, al configurar esta directriz a `NO` previene a los usuarios locales a proporcionar contraseñas sin encriptar sobre la red.

El valor por defecto es `YES`.

- `userlist_enable` — Cuando está activada, se les niega el acceso a los usuarios listados en el archivo especificado por la directriz `userlist_file`. Puesto que se niega el acceso al cliente antes de solicitar la contraseña, se previene que los usuarios suministren contraseñas sin encriptar sobre la red.

El valor predeterminado es `NO`, sin embargo, bajo Red Hat Enterprise Linux el valor está configurado a `YES`.

- `userlist_file` — Especifica el archivo al que `vsftpd` hace referencia cuando la directriz `userlist_enable` está activada.

El valor predeterminado es `/etc/vsftpd.user_list` y es creado durante la instalación.

- `cmds_allowed` — Especifica una lista separada por comas de los comandos FTP que permite el servidor. Cualquier otro comando es rechazado.

Esta directriz no tiene un valor predeterminado.

15.5.3. Opciones de usuario anónimo

A continuación, se presenta una lista de las directrices que controlan el acceso de usuarios anónimos al servidor. Para utilizar estas opciones, la directriz `anonymous_enable` debe tener el valor de `YES`.

- `anon_mkdir_write_enable` — Cuando se activa en combinación con la directriz `write_enable`, los usuarios anónimos pueden crear nuevos directorios dentro de un directorio que tiene permisos de escritura.

El valor predeterminado es `NO`.

- `anon_root` — Especifica el directorio al cual `vsftpd` cambia luego que el usuario anónimo se conecta.

Esta directriz no tiene un valor predeterminado.

- `anon_upload_enable` — Cuando se usa con la directriz `write_enable`, los usuarios anónimos pueden cargar archivos al directorio padre que tiene permisos de escritura.

El valor predeterminado es `NO`.

- `anon_world_readable_only` — Si está activada, los usuarios anónimos solamente pueden descargar archivos legibles por todo el mundo.

El valor por defecto es `YES`.

- `ftp_username` — Especifica la cuenta del usuario local (listada en `/etc/passwd`) utilizada por el usuario FTP anónimo. El directorio principal especificado en `/etc/passwd` para el usuario es el directorio raíz del usuario FTP anónimo.

El valor por defecto es `ftp`.

- `no_anon_password` — Cuando está activada, no se le pide una contraseña al usuario anónimo.

El valor predeterminado es `NO`.

- `secure_email_list_enable` — Cuando está activada, solamente se aceptan una lista de contraseñas especificadas para las conexiones anónimas. Esto es una forma conveniente de ofrecer seguridad limitada al contenido público sin la necesidad de usuarios virtuales.

Se previenen las conexiones anónimas a menos que la contraseña suministrada esté listada en `/etc/vsftpd.email_passwords`. El formato del archivo es una contraseña por línea, sin espacios al comienzo.

El valor predeterminado es `NO`.

15.5.4. Opciones del usuario local

La siguiente es una lista de las directrices que caracterizan la forma en que los usuarios locales acceden al servidor. Para utilizar estas opciones, la directriz `local_enable` debe estar a `YES`.

- `chmod_enable` — Cuando está activada, se permite el comando FTP `SITE CHMOD` para los usuarios locales. Este comando permite que los usuarios cambien los permisos en los archivos.

El valor por defecto es `YES`.

- `chroot_list_enable` — Cuando está activada, se coloca en una prisión de `chroot` a los usuarios locales listados en el archivo especificado en la directriz `chroot_list_file`.

Si se utiliza en combinación con la directriz `chroot_local_user`, los usuarios locales listados en el archivo especificado en la directriz `chroot_list_file`, *no* se colocan en una prisión `chroot` luego de conectarse.

El valor predeterminado es NO.

- `chroot_list_file` — Especifica el archivo que contiene una lista de los usuarios locales a los que se hace referencia cuando la directriz `chroot_list_enable` está en YES.

El valor por defecto es `/etc/vsftpd.chroot_list`.

- `chroot_local_user` — Si está activada, a los usuarios locales se les cambia el directorio raíz (se hace un `chroot`) a su directorio principal luego de la conexión.

El valor predeterminado es NO.



Aviso

Al activar `chroot_local_user` se abren varios problemas de seguridad, especialmente para los usuarios con privilegios para hacer cargas. Por este motivo, *no* se recomienda su uso.

- `guest_enable` — Al estar activada, todos los usuarios anónimos se conectan como `guest`, el cual es el usuario local especificado en la directriz `guest_username`.

El valor predeterminado es NO.

- `guest_username` — Especifica el nombre de usuario al cual `guest` está asignado.

El valor por defecto es `ftp`.

- `local_root` — Especifica el directorio al cual `vsftpd` se cambia después de que el usuario se conecta.

Esta directriz no tiene un valor predeterminado.

- `local_umask` — Especifica el valor de `umask` para la creación de archivos. Observe que el valor por defecto está en forma octal (un sistema numérico con base ocho), que incluye un prefijo de "0". De lo contrario el valor es tratado como un valor entero de base 10.

El valor por defecto `022`.

- `passwd_chroot_enable` — Cuando se activa junto con la directriz `chroot_local_user`, `vsftpd` cambia la raíz de los usuarios locales basado en la ocurrencia de `./` en el campo del directorio principal dentro de `/etc/passwd`.

El valor predeterminado es NO.

- `user_config_dir` — Especifica la ruta a un directorio que contiene los archivos de configuración con los nombres de los usuarios locales. Contiene información específica sobre ese usuario. Cualquier directriz en el archivo de configuración del usuario ignora aquellas encontradas en `/etc/vsftpd/vsftpd.conf`.

Esta directriz no tiene un valor predeterminado.

15.5.5. Opciones de directorio

La siguiente es una lista de directrices que afectan a los directorios.

- `dirlist_enable` — Al estar activada, los usuarios pueden ver los listados de directorios.

El valor por defecto es `YES`.

- `dirmessage_enable` — Al estar activada, cada vez que un usuario entra en un directorio con un archivo de mensaje. Este mensaje se encuentra dentro del directorio al que se entra. El nombre de este archivo se especifica en la directriz `message_file` y por defecto es `.message`.

El valor predeterminado es `NO`, sin embargo, bajo Red Hat Enterprise Linux el valor está configurado a `YES`.

- `force_dot_files` — Al estar activada, se listan en los listados de directorios los mensajes que comienzan con un punto (`.`), a excepción de los archivos `.` y `...`

El valor predeterminado es `NO`.

- `hide_ids` — Cuando está activada, todos los listados de directorios muestran `ftp` como el usuario y grupo para cada archivo.

El valor predeterminado es `NO`.

- `message_file` — Especifica el nombre del archivo de mensaje cuando se utiliza la directriz `dirmessage_enable`.

El valor predeterminado es `.message`.

- `text_userdb_names` — Cuando está activado, se utilizan los nombres de usuarios y grupos en lugar de sus entradas UID o GID. Al activar esta opción puede que reduzca el rendimiento del servidor.

El valor predeterminado es `NO`.

- `use_localtime` — Al estar activada, los listados de directorios revelan la hora local para el computador en vez de GMT.

El valor predeterminado es `NO`.

15.5.6. Opciones de transferencia de archivos

La siguiente es una lista de directrices que afectan a los directorios.

- `download_enable` — Cuando está activada, se permiten las descargas de archivos.

El valor por defecto es `YES`.

- `chown_uploads` — Si está activada, todos los archivos cargados por los usuarios anónimos pertenecen al usuario especificado en la directriz `chown_username`.

El valor predeterminado es `NO`.

- `chown_username` — Especifica la propiedad de los archivos cargados anónimamente si está activada la directriz `chown_uploads`.

El valor predeterminado es `root`.

- `write_enable` — Cuando está activada, se permiten los comandos FTP que pueden modificar el sistema de archivos, tales como `DELE`, `RNFR` y `STOR`.

El valor por defecto es YES.

15.5.7. Opciones de conexión

A continuación se presenta una lista con las directrices que afectan el comportamiento de conexión de `vsftpd`.

- `dual_log_enable` — Cuando se activa en conjunto con `xferlog_enable`, `vsftpd` escribe simultáneamente dos archivos: un registro compatible con `wu-ftp` al archivo especificado en la directriz `xferlog_file` (por defecto `/var/log/xferlog`) y un archivo de registro estándar `vsftpd` especificado en la directriz `vsftpd_log_file` (por defecto `/var/log/vsftpd.log`).

El valor predeterminado es NO.

- `log_ftp_protocol` — Cuando está activado en conjunto con `xferlog_enable` y con `xferlog_std_format` configurada a NO, se registran todos los comandos y respuestas. Esta directriz es muy útil para propósitos de depuración.

El valor predeterminado es NO.

- `syslog_enable` — Cuando se activa en conjunto con `xferlog_enable`, todos los registros que normalmente se escriben al archivo estándar `vsftpd` especificado en la directriz `vsftpd_log_file`, se envían al registro del sistema bajo la facilidad FTPD.

El valor predeterminado es NO.

- `vsftpd_log_file` — Especifica el archivo de registro de `vsftpd`. Para que se utilice este archivo, `xferlog_enable` debe estar activado y `xferlog_std_format` debe ser bien sea NO o, si está en YES, entonces `dual_log_enable` debe estar activado. Es importante resaltar que si `syslog_enable` está en YES, se utiliza el registro del sistema en lugar del archivo especificado en esta directriz.

El valor por defecto es `/var/log/vsftpd.log`.

- `xferlog_enable` — Cuando se activa, `vsftpd` registra las conexiones (solamente formato `vsftpd`) y la información de transferencia, al archivo de registro especificado en la directriz `vsftpd_log_file` (por defecto es `/var/log/vsftpd.log`). Si `xferlog_std_format` está configurada a YES, se registra la información de transferencia de archivo pero no las conexiones y en su lugar se utiliza el archivo de registro especificado en `xferlog_file` (por defecto `/var/log/xferlog`). Es importante observar que se utilizan ambos archivos y formatos de registro si `dual_log_enable` tiene el valor de YES.

El valor predeterminado es NO, sin embargo, bajo Red Hat Enterprise Linux el valor está configurado a YES.

- `xferlog_file` — Especifica el archivo de registro compatible con `wu-ftp`. Para que se utilice este archivo, `xferlog_enable` debe estar activado y `xferlog_std_format` debe tener el valor de YES. También se utiliza si `dual_log_enable` tiene el valor de YES.

El valor por defecto es `/var/log/xferlog`.

- `xferlog_std_format` — Cuando se activa en combinación con `xferlog_enable`, sólo se escribe un archivo de registro compatible con `wu-ftpd` al archivo especificado en la directriz `xferlog_file` (por defecto `/var/log/xferlog`). Es importante resaltar que este archivo solamente registra transferencias de archivos y no las conexiones al servidor.

El valor predeterminado es `NO`, sin embargo, bajo Red Hat Enterprise Linux el valor está configurado a `YES`.



Importante

Para mantener la compatibilidad con los archivos de registro escritos por el servidor FTP más antiguo `wu-ftpd`, se configura la directriz `xferlog_std_format` a `YES` bajo Red Hat Enterprise Linux. Sin embargo, esta configuración implica que las conexiones al servidor no son registradas.

Para registrar ambas conexiones en formato `vsftpd` y mantener un archivo de registro de transferencia compatible con `wu-ftpd`, configure `dual_log_enable` a `YES`.

Si no es de importancia mantener un archivo de registro de transferencias compatible con `wu-ftpd`, entonces configure `xferlog_std_format` a `NO`, comente la línea con un carácter de almohadilla (`#`) o borre completamente la línea.

15.5.8. Opciones de red

Lo siguiente lista las directrices que afectan cómo `vsftpd` interactúa con la red.

- `accept_timeout` — Especifica la cantidad de tiempo para un cliente usando el modo pasivo para establecer una conexión.

El valor por defecto `60`.

- `anon_max_rate` — Especifica la cantidad máxima de datos transmitidos por usuarios anónimos en bytes por segundo.

El valor por defecto es `0`, lo que no limita el ratio de transferencia.

- `connect_from_port_20` — Cuando está activada, `vsftpd` se ejecuta con privilegios suficientes para abrir el puerto 20 en el servidor durante las transferencias de datos en modo activo. Al desactivar esta opción, se permite que `vsftpd` se ejecute con menos privilegios, pero puede ser incompatible con algunos clientes FTP.

El valor predeterminado es `NO`, sin embargo, bajo Red Hat Enterprise Linux el valor está configurado a `YES`.

- `connect_timeout` — Especifica la cantidad máxima de tiempo que un cliente usando el modo activo tiene para responder a una conexión de datos, en segundos.

El valor por defecto `60`.

- `data_connection_timeout` — Especifica la cantidad máxima de tiempo que las conexiones se pueden aplazar en segundos. Una vez lanzado, se cierra la conexión con el cliente remoto.

El valor predeterminado es 300.

- `ftp_data_port` — Especifica el puerto utilizado por las conexiones de datos activas cuando `connect_from_port_20` está configurado a YES.

El valor predeterminado es 20.

- `idle_session_timeout` — Especifica la cantidad máxima de tiempo entre comandos desde un cliente remoto. Una vez disparado, se cierra la conexión al cliente remoto.

El valor predeterminado es 300.

- `listen_address` — Especifica la dirección IP en la cual `vsftpd` escucha por las conexiones de red.

Esta directriz no tiene un valor predeterminado.



Sugerencia

Si se están ejecutando varias copias de `vsftpd` sirviendo diferentes direcciones IP, el archivo de configuración para cada copia del demonio `vsftpd` debe tener un valor diferente para esta directriz. Consulte la [Sección 15.4.1](#) para más información sobre servidores FTP multihome.

- `listen_address6` — Especifica la dirección IPv6 en la cual `vsftpd` escucha por conexiones de red cuando `listen_ipv6` está configurada a YES.

Esta directriz no tiene un valor predeterminado.



Sugerencia

Si se están ejecutando varias copias de `vsftpd` sirviendo diferentes direcciones IP, el archivo de configuración para cada copia del demonio `vsftpd` debe tener un valor diferente para esta directriz. Consulte la [Sección 15.4.1](#) para más información sobre servidores FTP multihome.

- `listen_port` — Especifica el puerto en el cual `vsftpd` escucha por conexiones de red.

El valor predeterminado es 21.

- `local_max_rate` — Especifica el máximo ratio de transferencia de datos para los usuarios locales conectados en el servidor en bytes de segundo.

El valor por defecto es 0, lo que no limita el ratio de transferencia.

- `max_clients` — Especifica el número máximo de clientes simultáneos que tienen permitido conectarse al servidor cuando se ejecuta en modo independiente. Cualquier conexión adicional resultará en un mensaje de error.

El valor predeterminado es 0, lo que no limita las conexiones.

- `max_per_ip` — Especifica el máximo número de clientes que tienen permitido conectarse desde la misma dirección IP fuente.

El valor predeterminado es 0, lo que no limita las conexiones.

- `pasv_address` — Especifica la dirección IP para la IP del lado público del servidor para los servidores detrás de cortafuegos Network Address Translation (NAT). Esto permite que `vsftpd` entregue la dirección correcta de retorno para las conexiones pasivas.

Esta directriz no tiene un valor predeterminado.

- `pasv_enable` — Cuando está activa, se permiten conexiones en modo pasivo.

El valor por defecto es `YES`.

- `pasv_max_port` — Especifica el puerto más alto posible enviado a los clientes FTP para las conexiones en modo pasivo. Esta configuración es utilizada para limitar el intervalo de puertos para que las reglas del cortafuegos sean más fáciles de crear.

El valor predeterminado es `0`, lo que no limita el rango de puertos pasivos más alto. El valor no puede exceder de `65535`.

- `pasv_min_port` — Especifica el puerto más bajo posible para los clientes FTP para las conexiones en modo pasivo. Esta configuración es utilizada para limitar el intervalo de puertos para que las reglas del cortafuego sean más fáciles de implementar.

El valor predeterminado es `0`, lo que no limita el intervalo de puertos pasivos más bajo. El valor no debe ser menor que `1024`.

- `pasv_promiscuous` — Cuando está activada, las conexiones de datos no son verificadas para asegurarse de que se originan desde la misma dirección IP. Este valor solamente es útil para ciertos tipos de tunneling.



Atención

No active esta opción a menos que sea absolutamente necesario ya que desactiva una funcionalidad de seguridad muy importante la cual verifica que las conexiones en modo pasivo partan desde la misma dirección IP que la conexión de control que inicia la transferencia de datos.

El valor predeterminado es `NO`.

- `port_enable` — Cuando está activada, se permiten las conexiones en modo activo.

El valor por defecto es `YES`.

[Anterior](#)

Iniciar y detener `vsftpd`

[Inicio](#)

[Subir](#)

[Siguiendo](#)

Recursos adicionales