Logiciel

Page de man de Vsftpd.conf

vsftpd.conf contrôle le comportement de vsftpd. Par défaut, **vsftpd** recherche ce fichier à l'emplacement **/etc/vsftpd.conf**.

Vous pouvez cchanger cela en spécifiant le chemin d'accès du fichier de configuration de vsftpd en argument de la ligne de commande pour vsftpd.

Format

Chaque ligne est un commentaire ou une directive. Les lignes de commentaires commencent par un # et sont ignorées. Une ligne de directive a le format:

```
option=value
```

Ne pas mettre d'espace entre l'option, = et la valeur.

Chaque paramètre a une valeur par défaut qui peut être modifiée dans le fichier de configuration.

Les paramètres booléens prennent la valeur YES ou NO

Paramètres booléens

mode autonome (standalone)

Paramètre	valeur par défaut	Explication
listen	**YES**	mode autonome (exécution directe de l'exécutable de vsftpd qui écoute les connexions entrantes).
listen_ipv6	**NO**	id. que listen, mais en IPv6 au lieu d'IPv4.
listen_port	**21**	If vsftpd is in standalone mode, this is the port it will listen on for incoming FTP connections.
listen_address	**(none)**	If vsftpd is in standalone mode, the default listen address (of all local interfaces) may be overridden by this setting. Provide a numeric IP address.
listen_address6	**(none)**	Like listen_address, but specifies a default listen address for the IPv6 listener (which is used if listen_ipv6 is set). Format is standard IPv6 address format.

listen et listen_ipv6 sont mutuellement exclusifs

Connexion et contrôle d'accès

Paramètre	**valeur par défaut**	**Explication**
ftpd_banner	**none (default vsftpd banner is displayed)**	This string option allows you to override the greeting banner displayed by vsftpd when a connection first comes in.
banner_file	**(none)**	This option is the name of a file containing text to display when someone connects to the server. If set, it overrides the banner string provided by the ftpd_banner option.
anonymous_enable	**YES**	Autorise les connexions anonymes : les utilisateurs ftp et les anonymes sont tous reconnus comme des connexions anonymes.
no_anon_password	**NO**	When enabled, this prevents vsftpd from asking for an anonymous password - the anonymous user will log straight in.
local_enable	**NO**	Autorise les connexions locales : les comptes d'utilisateurs normaux listés dans /etc/passwd (ou dans la configuration de PAM) peuvent être utilisés pour se connecter.
deny_email_enable	**NO**	YES → liste de mots de passe e-mail anonymes à rejeter dans le fichier du paramètre **banned_email_file**. Utile pour lutter contre certaines attaques par déni de service.
		NO → pas de liste de mots de passe e-mail anonymes à rejeter
banned_email_file	**/etc/vsftpd.banned_emails**	This option is the name of a file containing a list of anonymous e-mail passwords which are not permitted. This file is consulted if the option deny_email_enable is enabled.
secure_email_list_enable	**NO**	Set to YES if you want only a specified list of e-mail passwords for anonymous logins to be accepted. This is useful as a low-hassle way of restricting access to low-security content without needing virtual users. When enabled, anonymous logins are prevented unless the password provided is listed in the file specified by the email_password_file setting. The file format is one password per line, no extra whitespace. The default filename is /etc/vsftpd.email_passwords.

Paramètre	valeur par défaut	Explication
email_password_file	**/etc/vsftpd.email_passwords**	This option can be used to provide an alternate file for usage by the secure_email_list_enable setting.
one_process_model	**NO**	If you have a Linux 2.4 kernel, it is possible to use a different security model which only uses one process per connection. It is a less pure security model, but gains you performance. You really don't want to enable this unless you know what you are doing, and your site supports huge numbers of simultaneously connected users.
pasv_addr_resolve	**NO**	Set to YES if you want to use a hostname (as opposed to IP address) in the pasv_address option.
pasv_address	**(none - the address is taken from the incoming connected socket)**	Use this option to override the IP address that vsftpd will advertise in response to the PASV command. Provide a numeric IP address, unless pasv_addr_resolve is enabled, in which case you can provide a hostname which will be DNS resolved for you at startup.
pasv_enable	**YES**	NO if you want to disallow the PASV method of obtaining a data connection.
pasv_promiscuous	**NO**	Set to YES if you want to disable the PASV security check that ensures the data connection originates from the same IP address as the control connection. Only enable if you know what you are doing! The only legitimate use for this is in some form of secure tunnelling scheme, or perhaps to facilitate FXP support.
pasv_max_port	**0 (use any port)**	The maximum port to allocate for PASV style data connections. Can be used to specify a narrow port range to assist firewalling.
pasv_min_port	**0 (use any port)**	The minimum port to allocate for PASV style data connections. Can be used to specify a narrow port range to assist firewalling.
port_enable	**YES**	Set to NO if you want to disallow the PORT method of obtaining a data connection.
port_promiscuous	**NO**	Set to YES if you want to disable the PORT security check that ensures that outgoing data connections can only connect to the client. Only enable if you know what you are doing!

Paramètre	**valeur par défaut**	**Explication**
run_as_launching_user	**NO**	Set to YES if you want vsftpd to run as the user which launched vsftpd. This is useful where root access is not available. MASSIVE WARNING! Do NOT enable this option unless you totally know what you are doing, as naive use of this option can create massive security problems. Specifically, vsftpd does not / cannot use chroot technology to restrict file access when this option is set (even if launched by root). A poor substitute could be to use a deny_file setting such as {/*,*..*}, but the reliability of this cannot compare to chroot, and should not be relied on. If using this option, many restrictions on other options apply. For example, options requiring privilege such as non-anonymous logins, upload ownership changing, connecting from port 20 and listen ports less than 1024 are not expected to work. Other options may be impacted.
userlist_deny	**YES**	This option is examined if userlist_enable is activated. If you set this setting to NO, then users will be denied login unless they are explicitly listed in the file specified by userlist_file. When login is denied, the denial is issued before the user is asked for a password.
userlist_enable	**NO**	If enabled, vsftpd will load a list of usernames, from the filename given by userlist_file. If a user tries to log in using a name in this file, they will be denied before they are asked for a password. This may be useful in preventing cleartext passwords being transmitted. See also userlist_deny.
userlist_file	**/etc/vsftpd.user_list**	This option is the name of the file loaded when the userlist_enable option is active.
accept_timeout	**60**	The timeout, in seconds, for a remote client to establish connection with a PASV style data connection.
connect_timeout	**60**	The timeout, in seconds, for a remote client to respond to our PORT style data connection.

Paramètre	valeur par défaut	Explication
data_connection_timeout	**300**	The timeout, in seconds, which is roughly the maximum time we permit data transfers to stall for with no progress. If the timeout triggers, the remote client is kicked off.
delay_failed_login	**1**	The number of seconds to pause prior to reporting a failed login.
delay_successful_login	**0**	The number of seconds to pause prior to allowing a successful login.
idle_session_timeout	**300**	délai maximal d'attente, en secondes, entre les commandes FTP d'un client distant. Si le délai d'attente est dépassé, le client distant est déconnecté.
max_login_fails	**3**	After this many login failures, the session is killed.
ftp_username	**ftp**	This is the name of the user we use for handling anonymous FTP. The home directory of this user is the root of the anonymous FTP area.
nopriv_user	**nobody**	This is the name of the user that is used by vsftpd when it wants to be totally unprivileged. Note that this should be a dedicated user, rather than nobody. The user nobody tends to be used for rather a lot of important things on most machines.

Droits d'écriture et de lecture

Par défaut, les utilisateurs virtuels ont des privilèges “anonyme”

Paramètre	valeur par défaut	Explication
write_enable	**NO**	autorise l'écriture (commandes STOR, DELE, RNFR, RNTO, MKD, RMD, APPE et SITE).

Si write_enable=YES,

Paramètre	valeur par défaut	Explication
anon_upload_enable	**NO**	autorise les utilisateurs anonymes (donc aussi les utilisateurs virtuels) à téléverser des fichiers. Nécessite que l'utilisateur FTP anonyme ait la permission d'écriture sur les répertoires concernés.
anon_mkdir_write_enable	**NO**	autorise la création de nouveaux répertoires pour les utilisateurs anonymes (donc aussi les utilisateurs virtuels). Nécessite que l'utilisateur FTP anonyme ait la permission d'écriture sur le répertoire parent.

Paramètre	**valeur par défaut**	**Explication**
anon_world_readable_only	**YES**	n'autorise les utilisateurs anonymes qu'à télécharger des fichiers lisibles par tous. Cela suppose que l'utilisateur FTP peut posséder les fichiers, surtout en cas d'upload.
anon_other_write_enable	**NO**	autorise la suppression et le renommage pour les utilisateurs anonymes (donc aussi les utilisateurs virtuels). Généralement pas recommandé.
anon_umask	**077**	The value that the umask for file creation is set to for anonymous users. NOTE! If you want to specify octal values, remember the “0” prefix otherwise the value will be treated as a base 10 integer!
local_umask	**077**	The value that the umask for file creation is set to for local users. NOTE! If you want to specify octal values, remember the “0” prefix otherwise the value will be treated as a base 10 integer!
dirlist_enable	**YES**	S'il est réglé sur NO, toutes les commandes de listage de répertoire donneront permission refusée.
ls_recurse_enable	**NO**	When enabled, this setting will allow the use of “ls -R”. This is a minor security risk, because a ls -R at the top level of a large site may consume a lot of resources.
download_enable	**YES**	Si la valeur NO, toutes les demandes de téléchargement donneront permission refusée.
mdtm_write	**YES**	When enabled, this setting will allow MDTM to set file modification times (subject to the usual access checks).
chown_upload_mode	**0600**	The file mode to force for chown()ed anonymous uploads.
file_open_mode	**0666**	The permissions with which uploaded files are created. Umasks are applied on top of this value. You may wish to change to 0777 if you want uploaded files to be executable.
cmds_allowed	**(none)**	This options specifies a comma separated list of allowed FTP commands (post login. USER, PASS and QUIT and others are always allowed pre-login). Other commands are rejected. This is a powerful method of really locking down an FTP server. Example: cmds_allowed=PASV,RETR,QUIT
cmds_denied	**(none)**	This options specifies a comma separated list of denied FTP commands (post login. USER, PASS, QUIT and others are always allowed pre-login). If a command appears on both this and cmds_allowed then the denial takes precedence. (Added in v2.1.0).

Paramètre	valeur par défaut	Explication
deny_file	**(none)**	This option can be used to set a pattern for filenames (and directory names etc.) which should not be accessible in any way. The affected items are not hidden, but any attempt to do anything to them (download, change into directory, affect something within directory etc.) will be denied. This option is very simple, and should not be used for serious access control - the filesystem's permissions should be used in preference. However, this option may be useful in certain virtual user setups. In particular aware that if a filename is accessible by a variety of names (perhaps due to symbolic links or hard links), then care must be taken to deny access to all the names. Access will be denied to items if their name contains the string given by hide_file, or if they match the regular expression specified by hide_file. Note that vsftpd's regular expression matching code is a simple implementation which is a subset of full regular expression functionality. Because of this, you will need to carefully and exhaustively test any application of this option. And you are recommended to use filesystem permissions for any important security policies due to their greater reliability. Supported regex syntax is any number of *, ? and unnested {,} operators. Regex matching is only supported on the last component of a path, e.g. a/b/? is supported but a/?/c is not. Example: deny_file={*.mp3,*.mov,.private}

utilisateurs virtuels

Paramètre	valeur par défaut	Explication
guest_enable	**NO**	Si YES, toutes les connexions non anonymes sont faites sous le compte de l'utilisateur spécifié par **guest_username**.
guest_username	**ftp**	utilisateur sous le compte duquel les utilisateurs sont connectés, ainsi qu'à son home.
chmod_enable	**YES**	autorise les utilisateurs locaux à utiliser chmod. (les anonymes n'y sont jamais autorisés)
virtual_use_local_privs	**NO**	If enabled, virtual users will use the same privileges as local users. By default, virtual users will use the same privileges as anonymous users, which tends to be more restrictive (especially in terms of write access).
user_sub_token	**(none)**	This option is useful is conjunction with virtual users. It is used to automatically generate a home directory for each virtual user, based on a template. For example, if the home directory of the real user specified via guest_username is /home/virtual/$USER, and user_sub_token is set to $USER, then when virtual user fred logs in, he will end up (usually chroot()'ed) in the directory /home/virtual/fred. This option also takes affect if local_root contains user_sub_token.

chrootage

Paramètre	valeur par défaut	Explication
chroot_local_user	**NO**	YES → chrootage des utilisateurs locaux dans leur répertoire personnel.
		NO → pas de chrootage des utilisateurs locaux dans leur répertoire personnel
chroot_list_enable	**NO**	YES → - Si chroot_local_user=YES, le fichier **chroot_list_file** liste les utilisateurs locaux qui ne sont pas chrootés dans leur répertoire personnel. - Si chroot_local_user=NO, le fichier **chroot_list_file** liste les utilisateurs locaux qui sont chrootés dans leur répertoire personnel.
		NO → ne liste pas les utilisateurs locaux qui sont chrootés ou non dans leur répertoire personnel
chroot_list_file	**/etc/vsftpd.chroot_list**	fichier contenant la liste des utilisateurs locaux qui seront chrootés ou non.
passwd_chroot_enable	**NO**	YES → combiné avec **chroot_local_user**, un emplacement de prison chroot() peut être spécifié sur une base per-user. La prison de chaque utilisateur est dérivée de son répertoire de base dans **/etc/passwd**. L'apparition de /./ dans la chaîne de répertoire d'accueil indique que la prison est à cet endroit particulier dans le chemin.
		NO → pas de prison chroot

Réseau

max_clients	**0 (unlimited)**	If vsftpd is in standalone mode, this is the maximum number of clients which may be connected. Any additional clients connecting will get an error message.
max_per_ip	**0 (unlimited)**	If vsftpd is in standalone mode, this is the maximum number of clients which may be connected from the same source internet address. A client will get an error message if they go over this limit.
ftp_data_port	**20**	The port from which PORT style connections originate (as long as the poorly named connect_from_port_20 is enabled).
connect_from_port_20	**NO (mais le fichier de configuration le met à YES)**	Contrôle si les connexions de données de style PORT utilisent le port 20 (ftp-data) sur la machine serveur. Pour des raisons de sécurité, certains clients peuvent insister pour que ce soit le cas. A l'inverse, la désactivation de cette option permet à vsftpd de tourner avec un peu moins privilèges.

Répertoires

Paramètre	valeur par défaut	Explication
dirmessage_enable	**NO (mais le fichier de configuration le met à YES).**	Si YES, les utilisateurs du serveur FTP peuvent recevoir des messages à leur arrivée dans un nouveau répertoire. Par défaut, un répertoire est scanné pour le fichier .message, mais cela peut être modifié avec le paramètre de configuration message_file.
message_file	**.message**	This option is the name of the file we look for when a new directory is entered. The contents are displayed to the remote user. This option is only relevant if the option dirmessage_enable is enabled.
force_dot_files	**NO**	Si activé, les fichiers et répertoires commençant par un point (.) seront affichés dans les listes de répertoires, ainsi que “.” et “..”, même si le flag “a” n'a pas été utilisé par le client.
hide_ids	**NO**	Si activé, tous les utilisateurs et information de groupe dans les listes de répertoires comme “ftp”.
use_localtime	**NO**	If enabled, vsftpd will display directory listings with the time in your local time zone. The default is to display GMT. The times returned by the MDTM FTP command are also affected by this option.
anon_root	**(none)**	This option represents a directory which vsftpd will try to change into after an anonymous login. Failure is silently ignored.
local_root	**(none)**	This option represents a directory which vsftpd will try to change into after a local (i.e. non-anonymous) login. Failure is silently ignored.
hide_file	**(none)**	This option can be used to set a pattern for filenames (and directory names etc.) which should be hidden from directory listings. Despite being hidden, the files / directories etc. are fully accessible to clients who know what names to actually use. Items will be hidden if their names contain the string given by hide_file, or if they match the regular expression specified by hide_file. Note that vsftpd's regular expression matching code is a simple implementation which is a subset of full regular expression functionality. See deny_file for details of exactly what regex syntax is supported. Example: hide_file={*.mp3,.hidden,hide*,h?}

éviter l'erreur "refusing to run with writable root inside chroot()"

Paramètre	valeur par défaut	Explication
allow_writeable_chroot=YES		

Configurations par utilisateur

Paramètre	valeur par défaut	Explication
user_config_dir	**(none)**	This powerful option allows the override of any config option specified in the manual page, on a per-user basis. Usage is simple, and is best illustrated with an example. If you set user_config_dir to be /etc/vsftpd_user_conf and then log on as the user “chris”, then vsftpd will apply the settings in the file /etc/vsftpd_user_conf/chris for the duration of the session. The format of this file is as detailed in this manual page! PLEASE NOTE that not all settings are effective on a per-user basis. For example, many settings only prior to the user's session being started. Examples of settings which will not affect any behviour on a per-user basis include listen_address, banner_file, max_per_ip, max_clients, xferlog_file, etc.

Journalisation

Paramètre	valeur par défaut	Explication
xferlog_enable	**NO (mais le fichier de configuration le met à YES)**	YES → un fichier journal des transferts sera maintenu.
		NO → pas de fichier journal des transferts
vsftpd_log_file	**/var/log/vsftpd.log**	nom du fichier journal des transferts. Ce journal n'est écrit que si l'option xferlog_enable = YES, et xferlog_std_format = NO. Alternativement, il est écrit si l'option dual_log_enable est activée. Une complication supplémentaire : si syslog_enable est activé, ce fichier n'est pas écrit et la sortie est envoyée au journal du système à la place.
xferlog_std_format	**NO**	YES → fichier journal de transfert au format xferlog standard, tel qu'utilisé par wu-ftpd.
		NO → fichier journal de transfert pas au format par défaut (plus lisible que le faormat xferlog standard)
xferlog_file	**/var/log/xferlog**	nom du fichier dans lequel est écrit le journal de transfert de style wu-ftpd.
dual_log_enable	**NO**	YES → deux fichiers journaux sont générés en parallèle, par défaut /var/log/xferlog et /var/log/vsftpd.log. Le premier est de style wu-ftpd. L'autre est de style propre à vsftpd.
		NO → un seul fichier journal
log_ftp_protocol	**NO**	Lorsque activé, toutes les demandes et réponses FTP sont enregistrées.
no_log_lock	**NO**	YES → empêche vsftpd de verrouiller le fichier lors de l'écriture des fichiers journaux. Cette option ne doit généralement pas être activée. Sert à contourner certaine bogues du système.
syslog_enable	**NO**	YES → une sortie de journal qui serait allée à /var/log/vsftpd.log va à la place dans le journal du système. L'enregistrement se fait sous le service FTPD.

Transferts

Paramètre	valeur par défaut	Explication
ascii_download_enable	**NO**	Si activé, les téléchargements de données se feront en mode ASCII.
ascii_upload_enable	**NO**	Si activé, les téléversements de données se feront en mode ASCII.
chown_uploads	**NO**	Si activé, tous les fichiers téléversés anonymement seront propriété de l'utilisateur spécifié dans le paramètre **chown_username**.
chown_username	**root**	This is the name of the user who is given ownership of anonymously uploaded files. This option is only relevant if another option, chown_uploads, is set.
delete_failed_uploads	**NO**	Si YES, tous les fichiers de téléversements échoués sont supprimés.
lock_upload_files	**YES**	Si activé, tous les uploads verrouillent en écriture le fichier téléchargé. ATTENTION! Avant d'activer cela, il faut savoir que les lecteurs malveillants pourraient empêcher un utilisateur, par exemple, d'ajouter un fichier.
anon_max_rate	**0 (unlimited)**	The maximum data transfer rate permitted, in bytes per second, for anonymous clients.
local_max_rate	**0 (unlimited)**	The maximum data transfer rate permitted, in bytes per second, for local authenticated users.
trans_chunk_size	**0 (let vsftpd pick a sensible setting)**	You probably don't want to change this, but try setting it to something like 8192 for a much smoother bandwidth limiter.

Fonctionnement

async_abor_enable	**NO**	Si activé, une commande FTP spéciale **async ABOR** sera activée. Fonction est difficile à manipuler, désactivée par défaut.
background	**NO**	Si activé et que vsftpd est démarré en mode **listen**, vsftpd sera lancé en tâche de fond, c'est à dire que le contrôle sera immédiatement rendu au processus qui a lancé vsftpd.
check_shell	**YES**	Cette option n'a d'effet que pour vsftpd sans PAM. Si désactivé, vsftpd ne vérifie pas dans /etc/shells la validité d'un shell utilisateur pour les connexions locales.
session_support	**NO**	This controls whether vsftpd attempts to maintain sessions for logins. If vsftpd is maintaining sessions, it will try and update utmp and wtmp. It will also open a pam_session if using PAM to authenticate, and only close this upon logout. You may wish to disable this if you do not need session logging, and you wish to give vsftpd more opportunity to run with less processes and / or less privilege. NOTE - utmp and wtmp support is only provided with PAM enabled builds.
setproctitle_enable	**NO**	If enabled, vsftpd will try and show session status information in the system process listing. In other words, the reported name of the process will change to reflect what a vsftpd session is doing (idle, downloading etc). You probably want to leave this off for security purposes.

SSL

Paramètre	valeur par défaut	Explication
ssl_enable	**NO**	YES → vsftpd supportera les connexions sécurisées via SSL. Cela s'applique au contrôle de connexion (y compris login) et aux les connexions de données. Vous aurez besoin d'un client avec le support SSL. N'activez cette option que si vous en avez besoin.

Si **ssl_enable=YES** :

Paramètre	valeur par défaut	Explication
allow_anon_ssl	**NO**	YES → les utilisateurs anonymes sont autorisés à utiliser des connexions SSL sécurisées.
force_anon_data_ssl	**NO**	YES → toutes les connexions anonymes doivent utiliser une connexion SSL sécurisée pour envoyer et recevoir des données.
force_anon_logins_ssl	**NO**	YES → toutes les connexions anonymes doivent utiliser une connexion SSL sécurisée pour envoyer le mot de passe.
force_local_data_ssl	**YES**	YES → toutes les connexions non anonymes doivent utiliser une connexion SSL sécurisée pour envoyer et recevoir des données.
force_local_logins_ssl	**YES**	YES → toutes les connexions non anonymes doivent utiliser une connexion SSL sécurisée pour envoyer le mot de passe.
ssl_sslv2	**NO**	Only applies if ssl_enable is activated. If enabled, this option will permit SSL v2 protocol connections. TLS v1 connections are preferred.
ssl_sslv3	**NO**	Only applies if ssl_enable is activated. If enabled, this option will permit SSL v3 protocol connections. TLS v1 connections are preferred.
ssl_tlsv1	**YES**	Only applies if ssl_enable is activated. If enabled, this option will permit TLS v1 protocol connections. TLS v1 connections are preferred.

Paramètre	valeur par défaut	Explication
debug_ssl	**NO**	YES → les diagnostic de liaison OpenSSL sont ajoutés au fichier journal de vsftpd.
implicit_ssl	**NO**	YES → toutes les connexions se font en SSL (protocole FTPS).
require_cert	**NO**	YES → toutes les connexions SSL doivent présenter un certificat. Le degré de validation appliqué à ce certificat est contrôlé par validate_cert.
require_ssl_reuse	**YES**	YES → toutes les connexions de données SSL sont tenus de présenter la réutilisation de la session SSL (qui prouve qu'ils ont la même clé). Bien que ce soit un défaut de sécurité, il peut gêner beaucoup de clients FTP, de sorte que vous voudrez peut-être désactiver.
ssl_request_cert	**YES**	YES → vsftpd will request (but not necessarily require).

Paramètre	valeur par défaut	Explication
strict_ssl_read_eof	**NO**	If enabled, SSL data uploads are required to terminate via SSL, not an EOF on the socket. This option is required to be sure that an attacker did not terminate an upload prematurely with a faked TCP FIN. Unfortunately, it is not enabled by default because so few clients get it right. (New in v2.0.7).
strict_ssl_write_shutdown	**NO**	If enabled, SSL data downloads are required to terminate via SSL, not an EOF on the socket. This is off by default as I was unable to find a single FTP client that does this. It is minor. All it affects is our ability to tell whether the client confirmed full receipt of the file. Even without this option, the client is able to check the integrity of the download. (New in v2.0.7).
validate_cert	**NO**	If set to yes, all SSL client certificates received must validate OK. Self-signed certs do not constitute OK validation. (New in v2.0.6).

Politique Debian

Paramètre	valeur par défaut	Explication
secure_chroot_dir	**/usr/share/empty**	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.
pam_service_name	**ftp**	This string is the name of the PAM service vsftpd will use.
rsa_cert_file	**/usr/share/ssl/certs/vsftpd.pem**	This option specifies the location of the RSA certificate to use for SSL encrypted connections.
rsa_private_key_file	**(none)**	This option specifies the location of the RSA private key to use for SSL encrypted connections. If this option is not set, the private key is expected to be in the same file as the certificate.
ssl_ciphers	**DES-CBC3-SHA**	This option can be used to select which SSL ciphers vsftpd will allow for encrypted SSL connections. See the ciphers man page for further details. Note that restricting ciphers can be a useful security precaution as it prevents malicious remote parties forcing a cipher which they have found problems with.
ca_certs_file	**(none)**	This option is the name of a file to load Certificate Authority certs from, for the purpose of validating client certs. Regrettably, the default SSL CA cert paths are not used, because of vsftpd's use of restricted filesystem spaces (chroot). (Added in v2.0.6).

Paramètre	valeur par défaut	Explication
dsa_cert_file	**(none - an RSA certificate suffices)**	This option specifies the location of the DSA certificate to use for SSL encrypted connections.
dsa_private_key_file	**(none)**	This option specifies the location of the DSA private key to use for SSL encrypted connections. If this option is not set, the private key is expected to be in the same file as the certificate.

Autres

Paramètre	valeur par défaut	Explication
tcp_wrappers	**NO**	If enabled, and vsftpd was compiled with tcp_wrappers support, incoming connections will be fed through tcp_wrappers access control. Furthermore, there is a mechanism for per-IP based configuration. If tcp_wrappers sets the VSFTPD_LOAD_CONF environment variable, then the vsftpd session will try and load the vsftpd configuration file specified in this variable.
text_userdb_names	**NO**	By default, numeric IDs are shown in the user and group fields of directory listings. You can get textual names by enabling this parameter. It is off by default for performance reasons.
tilde_user_enable	**NO**	If enabled, vsftpd will try and resolve pathnames such as ~chris/pics, i.e. a tilde followed by a username. Note that vsftpd will always resolve the pathnames ~ and ~/something (in this case the ~ resolves to the initial login directory). Note that ~user paths will only resolve if the file /etc/passwd may be found within the _current_ chroot() jail.
use_sendfile	**YES**	An internal setting used for testing the relative benefit of using the sendfile() system call on your platform.

Options numériques

Voici une liste d'options numériques. Une option numérique est obligatoirement un nombre entier non négatif.. Les nombres en octal sont pris en charge, pour des raisons de commodité des options de l'umask. Pour définir un nombre octal, utilisez 0 comme premier chiffre du nombre.

accept_timeout

The timeout, in seconds, for a remote client to establish connection with a PASV style data connection.

Default: **60**

anon_max_rate

The maximum data transfer rate permitted, in bytes per second, for anonymous clients.

Default: **0 (unlimited)**

anon_umask

The value that the umask for file creation is set to for anonymous users. NOTE! If you want to specify octal values, remember the “0” prefix otherwise the value will be treated

as a base 10 integer!

Default: **077**

chown_upload_mode

The file mode to force for chown()ed anonymous uploads. (Added in v2.0.6).

Default: **0600**

connect_timeout

The timeout, in seconds, for a remote client to respond to our PORT style data connection.

Default: **60**

data_connection_timeout

The timeout, in seconds, which is roughly the maximum time we permit data transfers to stall for with no progress. If the timeout triggers, the remote client is kicked off.

Default: **300**

delay_failed_login

The number of seconds to pause prior to reporting a failed login.

Default: **1**

delay_successful_login

The number of seconds to pause prior to allowing a successful login.

Default: **0**

file_open_mode

The permissions with which uploaded files are created. Umasks are applied on top of this value. You may wish to change to 0777 if you want uploaded files to be executable.

Default: **0666**

ftp_data_port

The port from which PORT style connections originate (as long as the poorly named connect_from_port_20 is enabled).

Default: **20**

idle_session_timeout

The timeout, in seconds, which is the maximum time a remote client may spend between FTP commands. If the timeout triggers, the remote client is kicked off.

Default: 300

listen_port

If vsftpd is in standalone mode, this is the port it will listen on for incoming FTP connections.

Default: 21

local_max_rate

The maximum data transfer rate permitted, in bytes per second, for local authenticated users.

Default: 0 (unlimited)

local_umask

The value that the umask for file creation is set to for local users. NOTE! If you want to specify octal values, remember the “0” prefix otherwise the value will be treated as a base 10 integer!

Default: 077

max_clients

If vsftpd is in standalone mode, this is the maximum number of clients which may be connected. Any additional clients connecting will get an error message.

Default: 0 (unlimited)

max_login_fails

After this many login failures, the session is killed.

Default: 3

max_per_ip

If vsftpd is in standalone mode, this is the maximum number of clients which may be connected from the same source internet address. A client will get an error message if they go over this limit.

Default: 0 (unlimited)

pasv_max_port

The maximum port to allocate for PASV style data connections. Can be used to specify a narrow port range to assist firewalling.

Default: 0 (use any port)

pasv_min_port

The minimum port to allocate for PASV style data connections. Can be used to specify a narrow port range to assist firewalling.

Default: 0 (use any port)

trans_chunk_size

You probably don't want to change this, but try setting it to something like 8192 for a much smoother bandwidth limiter.

Default: 0 (let vsftpd pick a sensible setting)

Options de chaîne

Below is a list of string options.

anon_root

This option represents a directory which vsftpd will try to change into after an anonymous login. Failure is silently ignored.

Default: (none)

banned_email_file

This option is the name of a file containing a list of anonymous e-mail passwords which are not permitted. This file is consulted if the option deny_email_enable is enabled.

Default: /etc/vsftpd.banned_emails

banner_file

This option is the name of a file containing text to display when someone connects to the server. If set, it overrides the banner string provided by the ftpd_banner option.

Default: (none)

ca_certs_file

This option is the name of a file to load Certificate Authority certs from, for the purpose of validating client certs. Regrettably, the default SSL CA cert paths are not used, because of vsftpd's use of restricted filesystem spaces (chroot). (Added in v2.0.6).

Default: (none)

chown_username

This is the name of the user who is given ownership of anonymously uploaded files. This option is only relevant if another option, chown_uploads, is set.

Default: root

chroot_list_file

The option is the name of a file containing a list of local users which will be placed in a chroot() jail in their home directory. This option is only relevant if the option chroot_list_enable is enabled. If the option chroot_local_user is enabled, then the list file becomes a list of users to NOT place in a chroot() jail.

Default: /etc/vsftpd.chroot_list

cmds_allowed

This options specifies a comma separated list of allowed FTP commands (post login. USER, PASS and QUIT and others are always allowed pre-login). Other commands are rejected. This is a powerful method of really locking down an FTP server. Example: cmds_allowed=PASV,RETR,QUIT

Default: (none)

cmds_denied

This options specifies a comma separated list of denied FTP commands (post login. USER, PASS, QUIT and others are always allowed pre-login). If a command appears on both this and cmds_allowed then the denial takes precedence. (Added in v2.1.0).

Default: (none)

deny_file

This option can be used to set a pattern for filenames (and directory names etc.) which should not be accessible in any way. The affected items are not hidden, but any attempt to do anything to them (download, change into directory, affect something within directory etc.) will be denied. This option is very simple, and should not be used for serious access control - the filesystem's permissions should be used in preference. However, this option may be useful in certain virtual user setups. In particular aware that if a filename is accessible by a variety of names (perhaps due to symbolic links or hard links), then care must be taken to deny access to all the names. Access will be denied to items if their name contains the string given by hide_file, or if they match the regular expression specified by hide_file. Note that vsftpd's regular expression matching code is a simple implementation which is a subset of full regular expression functionality. Because of this, you will need to carefully and exhaustively test any application of this option. And you are recommended to use filesystem permissions for any important security policies due to their greater reliability. Supported regex syntax is any number of *, ? and unnested {,} operators. Regex matching is only supported on the last component of a path, e.g. a/b/? is supported but a/?/c is not. Example: deny_file={*.mp3,*.mov,.private}

Default: (none)

dsa_cert_file

This option specifies the location of the DSA certificate to use for SSL encrypted connections.

Default: (none - an RSA certificate suffices)

dsa_private_key_file

This option specifies the location of the DSA private key to use for SSL encrypted connections. If this option is not set, the private key is expected to be in the same file as

the certificate.

Default: (none)

email_password_file

This option can be used to provide an alternate file for usage by the secure_email_list_enable setting.

Default: /etc/vsftpd.email_passwords

ftp_username

This is the name of the user we use for handling anonymous FTP. The home directory of this user is the root of the anonymous FTP area.

Default: ftp

ftpd_banner

This string option allows you to override the greeting banner displayed by vsftpd when a connection first comes in.

Default: (none - default vsftpd banner is displayed)

guest_username

See the boolean setting guest_enable for a description of what constitutes a guest login. This setting is the real username which guest users are mapped to.

Default: ftp

hide_file

This option can be used to set a pattern for filenames (and directory names etc.) which should be hidden from directory listings. Despite being hidden, the files / directories etc. are fully accessible to clients who know what names to actually use. Items will be hidden if their names contain the string given by hide_file, or if they match the regular expression specified by hide_file. Note that vsftpd's regular expression matching code is a simple implementation which is a subset of full regular expression functionality. See deny_file for details of exactly what regex syntax is supported. Example: hide_file={*.mp3,.hidden,hide*,h?}

Default: (none)

listen_address

If vsftpd is in standalone mode, the default listen address (of all local interfaces) may be overridden by this setting. Provide a numeric IP address.

Default: (none)

listen_address6

Like listen_address, but specifies a default listen address for the IPv6 listener (which is used if listen_ipv6 is set). Format is standard IPv6 address format.

Default: (none)

local_root

This option represents a directory which vsftpd will try to change into after a local (i.e. non-anonymous) login. Failure is silently ignored.

Default: (none)

message_file

This option is the name of the file we look for when a new directory is entered. The contents are displayed to the remote user. This option is only relevant if the option dirmessage_enable is enabled.

Default: .message

nopriv_user

This is the name of the user that is used by vsftpd when it wants to be totally unprivileged. Note that this should be a dedicated user, rather than nobody. The user nobody tends to be used for rather a lot of important things on most machines.

Default: nobody

pam_service_name

This string is the name of the PAM service vsftpd will use.

Default: ftp

pasv_address

Use this option to override the IP address that vsftpd will advertise in response to the PASV command. Provide a numeric IP address, unless pasv_addr_resolve is enabled, in which case you can provide a hostname which will be DNS resolved for you at startup.

Default: (none - the address is taken from the incoming connected socket)

rsa_cert_file

This option specifies the location of the RSA certificate to use for SSL encrypted connections.

Default: /usr/share/ssl/certs/vsftpd.pem

rsa_private_key_file

This option specifies the location of the RSA private key to use for SSL encrypted connections. If this option is not set, the private key is expected to be in the same file as the certificate.

Default: (none)

secure_chroot_dir

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.

Default: /usr/share/empty

ssl_ciphers

This option can be used to select which SSL ciphers vsftpd will allow for encrypted SSL connections. See the ciphers man page for further details. Note that restricting ciphers can be a useful security precaution as it prevents malicious remote parties forcing a cipher which they have found problems with.

Default: DES-CBC3-SHA

user_config_dir

This powerful option allows the override of any config option specified in the manual page, on a per-user basis. Usage is simple, and is best illustrated with an example. If you set user_config_dir to be /etc/vsftpd_user_conf and then log on as the user “chris”, then vsftpd will apply the settings in the file /etc/vsftpd_user_conf/chris for the duration of the session. The format of this file is as detailed in this manual page! PLEASE NOTE that not all settings are effective on a per-user basis. For example, many settings only prior to the user's session being started. Examples of settings which will not affect any behviour on a per-user basis include listen_address, banner_file, max_per_ip, max_clients, xferlog_file, etc.

Default: (none)

user_sub_token

This option is useful is conjunction with virtual users. It is used to automatically generate a home directory for each virtual user, based on a template. For example, if the home

directory of the real user specified via guest_username is /home/virtual/$USER, and user_sub_token is set to $USER, then when virtual user fred logs in, he will end up (usually chroot()'ed) in the directory /home/virtual/fred. This option also takes affect if local_root contains user_sub_token.

Default: (none)

userlist_file

This option is the name of the file loaded when the userlist_enable option is active.

Default: /etc/vsftpd.user_list

vsftpd_log_file

This option is the name of the file to which we write the vsftpd style log file. This log is only written if the option xferlog_enable is set, and xferlog_std_format is NOT set. Alternatively, it is written if you have set the option dual_log_enable. One further complication - if you have set syslog_enable, then this file is not written and output is sent to the system log instead.

Default: /var/log/vsftpd.log

xferlog_file

This option is the name of the file to which we write the wu-ftpd style transfer log. The transfer log is only written if the option xferlog_enable is set, along with xferlog_std_format. Alternatively, it is written if you have set the option dual_log_enable.

Default: /var/log/xferlog

Voir aussi

- **(en)** Page de man

Basé sur Page de manuel.

From:
https://doc.wikis.frapp.fr/ - **doc**

Permanent link:
https://doc.wikis.frapp.fr/doku.php?id=logiciel:reseau:ftp:serveur:vsftpd:man:start

Last update: **2024/09/21 13:41**