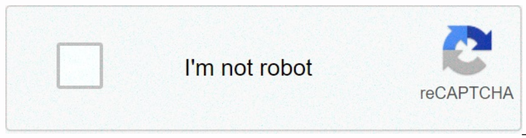

Continue

Vsftpd. conf default file

Courtesy: vsftpd_3.0.3-9build1_amd64 NAME vsftpd.conf - a configuration file for vsftpd DESCRIPTION vsftpd.conf can be used to control various aspects of vsftpd behavior. By default, vsftpd searches for this file at /etc/vsftpd.conf. However, you can override this by specifying the vsftpd command line argument. A command line argument is the name of the configuration file path for vsftpd. This behavior is useful because you can use an advanced inet such as xinetd to run vsftpd with different configuration files based on the virtual host. FORMAT Format vsftpd.conf is very simple. Each line is a comment or directive. Comment lines start with # and are ignored. The directive line has a format: option = value It is important to note that this is an error to put any space between the option= and the value. Each option has a default compilation that can be changed in the configuration file. Boolean OPTIONS Below is a list of logical parameters. The boolean value can be set to Yes or No. allow_anon_ssl applies only if the ssl_enable is active. If set to YES, anonymous users will be allowed to use secure SSL connections. Default: If anon_mkdir_write_enable set to YES, anonymous users will be allowed to create new directories under certain conditions. In order for this to work, the write_enable need to be activated, and an anonymous FTP user must have write permission to the parent directory. Default: If anon_other_write_enable set to YES, anonymous users will be allowed to perform write operations other than downloading and creating a directory, such as deleting and renaming. This is generally not recommended, but included for completeness. Default: If anon_upload_enable set to YES, anonymous users will be allowed to download files under certain conditions. In order for this to work, you write_enable to activate, and an anonymous FTP user must have write permission at the desired download locations. This option is also required to download virtual users; by default, virtual users are processed with anonymous (i.e. maximum limited) privilege. Default: anon_world_readable_only if this option is checked If this option is checked, anonymous users will only be allowed to download files that can be read in the world. This recognizes that the FTP user can own files, especially if downloads are available. Default: This anonymous_enable whether anonymous sign-in is allowed or not. If this option is checked, both FTP usernames and anonymous ones are recognized as anonymous logins. Default: ascii_download_enable if this option is checked If this option is checked, ascii mode data will not be transmitted at boot time. Default: ascii_upload_enable if this option is checked, data in ASCII mode will be executed during upload. Default: If async_abor_enable enabled, a special FTP command known as async ABOR will be enabled. Only poorly advised FTP customers will use this feature. Additionally, this feature is uncomfortable to handle, so it is disabled by default. Unfortunately, some FTP clients will cancellation of the transfer if this feature is not available, so you can enable it. Default: no background When enabled, and vsftpd on startup in listening mode, vsftpd will be the background of the listening process. ie control will be immediately returned to the shell that launched vsftpd. Default: No check_shell Note! This option only has an effect for non-PAM builds vsftpd. If this option is disabled, vsftpd will not check /etc/shells for a valid user shell for local logins. Default: This chmod_enable, if enabled, allows you to use the CHMOD command on the site. Note! This applies only to on-premises users. Anonymous users never get to use the CHMOD site. Default: This is chown_uploads If checked, all anonymously downloaded files will have ownership changed to the user specified in the chown_username. This is useful from an administrative, and possibly security, point of view. Default: chroot_list_enable If activated, you can provide a list of local users who are in chroot() jail in their home directory after logging in. The value is slightly different if chroot_local_user is set to YES. In this scenario, the list becomes a list of users who should not be placed in chroot() jail. By default, the file containing this list is /etc/vsftpd.chroot_list, but you can override it with chroot_list_file option. Default: NO chroot_local_user If set to YES, local users will be (by default) placed in chroot() jail in their home directory after logging in. Warning: This option has security implications, especially if users have permission to download or access the shell. Turn on only if you know what you're doing. Note that these security implications are not vsftpd specific. They apply to all FTP terms that offer to place local users in chroot() jail. Default: connect_from_port_20 this option determines whether a PORT 20 (ftp data) port (ftp) data connection is used on the server computer. For security reasons, some customers may insist that this is the case. Conversely, disabling this option allows vsftpd to work with slightly less privileges. Default: NO (but the sample configuration file enables it) debug_ssl If so, the OpenSSL connection diagnostics are reset to the vsftpd log file. (Added to v2.0.6). Default value: delete_failed_uploads if so, any files cannot be uploaded are deleted. (Added to v2.0.7). Default: Deny_email_enable if activated, you can provide a list of anonymous password email replies that cause the login to be denied. By default, the file containing this list is /etc/vsftpd.banned_emails, but you can override it with banned_email_file option. Default: If dirlist_enable set to NO, all commands in the list will be refused permission. Default: This is dirmessage_enable If enabled, FTP server users can display messages when they first log on to the new directory. By default, the directory is scanned for a .message file, but this can be overridden with the configuration message_file. Default: NO (but the sample configuration file enables it) download_enable If set to NO, all requests will give a waiver of the permit. Default: YES dual_log_enable If enabled, two log files are created in parallel, moving the default to /var/log/xferlog and /var/log/vsftpd.log. The first is wu-ftpd style transfer log, which can be promoted with standard tools. The latter is its own vsftpd style magazine. Default: No force_dot_files If enabled, files and directories starting with . will be displayed in directory lists, even if the a mark has not been used by the client. This override excludes . And.. Entries. Default: The force_anon_data_ssl is only applied if ssl_enable activated. If enabled, all anonymous logins are forced to use a secure SSL connection to send and retrieve data about data connections. Default: The force_anon_logins_ssl is only applied if the ssl_enable is activated. If enabled, all anonymous logins are forced to use a secure SSL connection in order to send a password. Default: The force_local_data_ssl is only applied if ssl_enable activated. If enabled, all non-anonymized logins are forced to use a secure SSL connection to send and retrieve data connection data. Default: The force_local_logins_ssl is only applied if ssl_enable activated. If enabled, all non-anonymized logins are forced to use a secure SSL connection in order to send a password. Default: YES, guest_enable is enabled, all non-anonymous login is classified as a guest login. The guest login will be re-specified to the user specified in guest_username configuration. Default: hide_ids if checked, all user and group data in directory lists will be displayed as 'ftp'. Default: implicit_ssl if enabled, ssl handshakes are the first thing expected on all connections (FTPS). To support explicit SSL and/or plain text, too, you need to start a separate vsftpd listening process. Default: Do not listen If this option is checked, vsftpd will work offline. This means that vsftpd should not be launched from an inet of some kind. Instead, the vsftpd executable file runs once directly. vsftpd itself will then take care of listening and processing incoming connections. Default: Listen_ipv6 as an audition option, except vsftpd will listen on the IPv6 connector instead of IPv4. Note that socket listening on IPv6 is any address (::) will accept both IPv6 and IPv4 connections by default. This option and the listening option are mutually exclusive. Default: The local_enable determines whether local inputs are allowed or not. If this option is checked, regular user accounts in the /etc/passwd file (or wherever your PAM configuration links are) can be used to log in. This must be enabled for any non-anonymous sign-in to work, including Users. Default value: lock_upload_files if this option is checked, all uploads will not be checked, all uploads will be marked as locking the entry in the upload file. All downloads go to the shared read lock in the download file. Warning! Before you turn this on, keep in mind that malicious readers can starve a writer who wants to add a file, for example. Default: Yes log_ftp_protocol if enabled, all FTP requests and are logged, ensuring the xferlog_std_format option is not enabled. Useful for debugging. Default value: ls_recurse_enable checked, this option will allow the use of ls-R. This is a minor security risk because ls -R at the top level of a large site can consume a lot of resources. Default value: mdtm_write will not be checked if this option is checked, this option will allow MDTM to set the file change time (subject to normal access checks). Default: Yes, no_anon_password is enabled, it prevents vsftpd from asking for an anonymous password – an anonymous user will log in directly. Default value: no_log_lock if this option is checked If this option is checked, you will not let vsftpd get file lock when writing to log files. This option should not be referred to normally. It exists to solve operating system errors, such as a combination of the Solaris/Veritas file system, which has been observed to occasionally detect hangs trying to lock log files. Default: One_process_model if you have a Linux 2.4 kernel, you can use a different security model that uses only one connection process. It's a less clean security model, but gets performance. You really don't want to include this unless you know what you're doing and your site supports a huge number of simultaneously connected users. Default value: passwd_chroot_enable If enabled, with chroot_local_user , the chroot() prison location can be specified based on each user. Each user's prison comes from their home directory line in /etc/passwd. The appearance of /./ in the home directory line indicates that the prison is in this particular location on the way. Default: pasv_addr_resolve is set as if you want to use a host name (as opposed to an IP address) and pasv_address option. Default: pasv_enable set to NO if you want to take pasv to retrieve the data connection. Default: The pasv_promiscuous is set to yes if you want to disable PASV security checks, which ensures that the data connection originates from the same IP address as the connection control. Only turn on if you know what you're doing! The only legitimate use for this is some form of secure tunnelling scheme, or perhaps to facilitate FXP support. Default value: port_enable set to NO if you want to set the port method to retrieve the data connection. Default: The port_promiscuous is set to yes if you want to disable port security checks, which ensures that the source data connections can only be connected to the client. Only turn on if you know what you're doing! Default: Require_cert if set to Yes, all SSL client connections are required to present a client certificate. The degree of verification applied to this certificate is validate_cert (added to v2.0.6). Default: require_ssl_reuse If set to Yes, all SSL data connections are required to reuse the SSL session (which proves that they know the same basic secret as the control channel). Although it is safe by default, it can disrupt many FTP clients so you can disable it. Fora Fora consequences, see <a0><a1></a1> (Added to v2.1.0). Default: This run_as_launching_user set to YES if you want vsftpd to run as the user who started vsftpd. This is useful if root access is not available. MASS WARNING! Do not enable this option if you do not know exactly what you are doing, as naïve use of this option can create massive security issues. Specifically, vsftpd does not / can not use chroot technology to restrict access to files when this option is installed (even if it is run by the root). A bad substitute might be to use deny_file such as {/*,*.. *}, but the reliability of this cannot be compared to a meal, and should not be relied upon. If you use this option, there are many restrictions on other options. For example, you do not expect parameters such as non-anonymized logins, change of ownership of downloads, connections from port 20, and listening to ports less than 1024. Other options may be affected. Default value: secure_email_list_enable set as if you want to accept only the specified list of email passwords for anonymous logins. This is useful as a low way to restrict access to low-security content without the need for virtual users. If this option is checked, anonymous inputs will not be warned unless the specified password is specified in the file email_password_file option. A file format is one password per line, with no additional space. The default filename is /etc/vsftpd.email_passwords. Default: Session_support this option determines whether vsftpd is trying to support logon sessions. If vsftpd supports sessions, it will try to update utmp and wtmp. It will also open pam_session using PAM for authentication, and only close this when you log off. You can disable this if you don't need session logging and you want to give vsftpd more options to run with smaller processes and/or fewer privileges. Note - utmp and WTMP support is provided only with PAM included builds. Default: If setproctitle_enable checked, vsftpd will try to display session status information in the list of system processes. In other words, the reported process name will change to reflect what the vsftpd session does (idly, download, etc.). You probably want to leave this for security purposes. Default: ssl_enable if enabled and vsftpd has been compiled against OpenSSL, vsftpd will support secure SSL connections. This includes connecting a control (including a login) and data connections. You will also need an SSL-enabled client. Note!! Beware of including this option. Turn it on only if you need it. vsftpd can not make any guarantees about the security of OpenSSL libraries. By en on this option, you declare that you trust the security of the installed Openssl. Default: ssl_request_cert If checked, vsftpd will ask (but not necessarily required; see require_cert)acertificateoncomingSSLconnections.Normally this should not cause any generally, but IBM zOS seems to have a problem. (New in v2.0.7). Default: The ssl_sslv2 is only applied if ssl_enable activated. If this option is checked, this option will allow SSL v2 connection. TLS v1 connections are the best. Default: The ssl_sslv3 is only applied if the ssl_enable is activated. If this option is checked, this option allows ssl v3 connection. TLS v1 connections are the best. Default: The ssl_tlsv1 is only applied if ssl_enable activated. If this option is checked, this option will allow TLS v1 to connect. TLS v1 connections are the best. Default: Yes, strict_ssl_read_eof is enabled, SSL download data is required to stop over SSL instead of EOF on the socket. This option should make sure that the attacker does not stop downloading prematurely tampered with TCP FIN. (New in v2.0.7). Default: If strict_ssl_write_shutdown enabled, SSL data downloads must be stopped over SSL, not EOF on the socket. This is disabled by default because I could not find one FTP client doing this. He's insignificant. All this affects our ability to tell whether the client has confirmed the full receipt of the file. Even without this option, the client is able to verify the integrity of the download. (New in v2.0.7). Default: syslog_enable if enabled, any log output that would go to /var/log/vsftpd.log goes to the system log instead. Logging is performed under the FTPD object. Default: If tcp_wrappers enabled and vsftpd has been compiled with tcp_wrappers, incoming connections will be tcp_wrappers access control. Additionally, there is a mechanism for IP-based configuration. If tcp_wrappers the environment VSFTPD_LOAD_CONF, the vsftpd session will try to load the vsftpd configuration file specified in this variable. Default: By default text_userdb_names numeric identifiers are displayed in user fields and directory list groups. You can get text names by enacting this option. This is disabled by default for performance reasons. Default: tilde_user_enable If this option is checked, vsftpd will try to solve path names such as ~chris/pics, i.e. the tilde followed by the username. Note that vsftpd will always solve the path names ~ and ~ / something (in this case ~ connects to the original login directory). Note that ~ user paths will only be solved if the /etc/passwd file can be found in prison _current_chroot(). Default: If use_localtime checked, vsftpd will show directory lists over time in your local time zone. The default is to display GMT. This option is also affected by the time returned by the MDTM FTP command. Default: USE_SENDFILE Internal setting used to test relative benefits sendfile() system call on your platform. Default: This option userlist_deny is considered if the userlist_enable is enabled. If you set this option to NO, then users will be denied the login if they are explicitly in the file specified userlist_file. When the login is denied, a waiver is issued before the user is prompted for a password. Default: YES userlist_enable, vsftpd will load a list of usernames from the filename specified userlist_file. If a user tries to sign in with a name in that file, they will be denied before they are prompted for a password. This can be useful for preventing passwords from being transferred with clear text. See also userlist_deny. Default: validate_cert if set to yes, all received SSL client certificates should check OK. Self-determination certificates are not OK. (New in v2.0.6). Default: virtual_use_local_privs 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 tend to be more restrictive (especially in terms of write access). Default: write_enable this option determines whether any FTP commands that change the file system are allowed. These commands are STOR, DELE, RNFR, RNTO, MKD, RMD, APPE, and SITE. Default value: xferlog_enable if checked, the log file will store detailed uploads and downloads. By default, this file will be placed at /var/log/vsftpd.log but this location can be overridden using the configuration vsftpd_log_file. Default: NO (but the sample configuration file enables it) xferlog_std_format If checked, the transfer log file will be written in the standard xferlog format used by wu-ftpd. This is useful because you can reuse existing transmission statistics generators. However, the default format is more readable. The default location for this log file style is /var/log/xferlog, but can be changed by using xferlog_file. Default: No numeric parameters Below is a list of numeric parameters. The numeric parameter must be set as a non-negative integer. Octagonal numbers are supported for ease of mask settings. To specify an eight-digit number, use 0 as the first digit of the number. accept_timeout time-out in seconds for the remote client to establish a pasv-style data connection. Default: 60 anon_max_rate Maximum data speed allowed, in bytes per second, for anonymous clients. Default: 0 (unlimited) anon_umask value that umask to create a file is set to anonymous users. Note! If you want to specify eight values, remember the prefix 0, otherwise the value will be treated as the base integer 10! Default: 077 chown_upload_mode in file mode to force chown()ed anonymous downloads. (Added to v2.0.6). Default: 0600 connect_timeout timeout in seconds for the remote client to respond to port data connection style. Default: 60 data_connection_timeout timeout, in seconds, which is about the maximum time we allow data to be transferred to a stall without progress. If the time-out starts, the remote client starts. Default: 300 delay_failed_login number of seconds to pause before reporting unsuccessful sign-in. Default: 1 1 The number of seconds to pause before allowing successful logon. Default: 0 file_open_mode with permissions to create downloaded files. Umasks are applied on top of this value. You can change to 0777 if you want the downloaded files to be executed. Default: 0666 ftp_data_port port from which port connection style is deeded (as long as bad connect_from_port_20 enabled). Default is 20 idle_session_timeout timeout, in seconds, which is the maximum time a remote client can spend between FTP commands. If the time-out starts, the remote client starts. Default: 300 listen_port If vsftpd is offline, it is the port it will listen to for incoming FTP connections. Default: 21 local_max_rate Maximum allowed byte transfer rate per second for on-premises authenticated users. Default: 0 (unlimited) local_umask value that umask to create a file is set to local users. Note! If you want to specify eight values, remember the prefix 0, otherwise the value will be treated as the base integer 10! Default: 077 max_clients if vsftpd is offline, this is the maximum number of clients that can be connected. Any additional customers who connect will receive the error message. Default: 0 (unlimited) and max_login_fails many login errors, the session will be killed. Default: 3 max_per_ip if vsftpd is offline, this is the maximum number of clients that can be connected from a single source Internet address. Customer will receive an error message if they pass this restriction. The default value is 0 (unlimited) pasv_max_port the maximum port for highlighting PASV-style data connections. You can use to determine a narrow range of ports to assist the firewall. Default value: 0 (use any port) pasv_min_port minimum port to allocate PASV-style data connections. You can use to determine a narrow range of ports to assist the firewall. Default: 0 (use any port) trans_chunk_size You probably don't want to change that, but try setting it to something like 8192 for a much smoother bandwidth limiter. Default: 0 (let vsftpd choose a smart configuration) LINE OPTIONS Below is a list of string options. anon_root This option represents a directory that vsftpd will try to change after anonymous logon. Failure is silently ignored. Default: (none) banned_email_file this option is a filename containing a list of anonymous email passwords that are not allowed. This file will be consulted if you deny_email_enable option. Default: /etc/vsftpd.banned_emails banner_file This option is the filename, contains text to display when someone connects to the server. If this option is checked, it overrides the banner line ftpd_banner option. Default: (none) ca_certs_file This option is the file name for downloading certification certificates in order to validate client certificates. Downloaded certificates are also advertised to the client to satisfy TLSv1.0 clients, such as the z/OS FTP client. Ftp. the default SSL CA certificate paths are not used because of the use of vsftpd limited file system spaces (chroot). (Added to v2.0.6). Default: (none) chown_username this is the name of the user who is granted ownership of anonymously downloaded files. This option is only up-to-date if you chown_uploads the file that is set. Default: chroot_list_file the filename containing a list of local users to be placed in chroot() jail in its home directory. This option is only up-to-date if the chroot_list_enable option is enabled. If the chroot_local_user, the list file becomes a list of users who do not put it in chroot() jail. Default: /etc/vsftpd.chroot_list cmds_allowed This option allows you to specify a list of allowed FTP commands separated by commas (after logging on. USER, PASS and QUIT, and others are always allowed to log on). Other commands were rejected. This is a powerful method to really block the FTP server. Example: cmds_allowed =PASV,RETR,QUIT Default: (none) cmds_denied These options allow a comma-separated list of rejected FTP commands (after logging on. USER, PASS, QUIT, and others are always allowed to log on). If the command appears on both this and the cmds_allowed then the waiver takes precedence. (Added to v2.1.0). Default: (none) deny_file This option can be used to set a template for filenames (and directory names, etc.) that should not be available in any way. Problematic items are not hidden, but any attempt to do anything with them (download, change to directory, affect something in the directory, etc.) will be denied. This option is very simple and should not be used for serious access control – file system permissions should be used in benefits. However, this option may be useful for some virtual users to install. In particular, it is known that if the file name is available by different names (possibly through symbolic links or hard links), you must take care of denying access to all names. Access will be denied to items if their name contains a string provided hide_file or if it matches the regular expression specified by hide_file. Note that the regular matching code of vsftpd expressions is a simple implementation, which is a subset of the full functionality of regular expressions. Because of this, you will need to thoroughly and exhaustively test any application of this option. And it is recommended that you use file system permissions for any important security policies because of their greater reliability. The supported syntax of a regular file is any number of *, ? and unnecessary operators {,}. Matching formal viewfips is only supported on the last component of the path, such as a/b/? supported, but a/?/c is not an example: deny_file={*.mp3,*.mov,.private} Default: (none) download_file the option can be configured to restrict the download of files with names that match the specified template. If the file name also matches the deny_file template, the failure takes precedence. For information about usage and template, see deny_file. Default: (none) dsa_cert_file is this specifies the location of the DSA certificate for encrypted SSL connections. Default: (no - RSA certificate is sufficient) dsa_private_key_file this option specifies the DSA private key location for encrypted SSL connections. If this option is not set, it is expected that the private key will be in the same file as the certificate. Default: (none) and email_password_file can be used to provide an alternate file to use secure_email_list_enable option. Default: /etc/vsftpd.email_passwords ftp_username This is the username we use to handle anonymous FTP. This user's home directory is the root of the anonymous FTP area. Default: ftp ftpd_banner This line allows you to override the welcome banner displayed by vsftpd on the first connection. Default: (none - the default vsftpd banner is displayed) guest_username see the guest_enable to describe what constitutes the guest's entrance. This option is the real name of the user with whom guest users are matched. Default: ftp hide_file This option can be used to set a template for filenames (and directory names, etc.) that should be hidden from directory lists. Despite the stealth, files/directories etc are fully accessible to customers who know which names to actually use. Items will be hidden if their names contain a string specified hide_file, or if they match the regular expression specified by hide_file. Note that the regular matching code of vsftpd expressions is a simple implementation, which is a subset of the full functionality of regular expressions. For more information about which regular file syntax is supported, see deny_file details. Example: hide_file={*.mp3,.hidden,hide*,h?} Default: (none) listen_address If vsftpd is offline, the default listening address (from all local interfaces) can be overridden with this option. Enter a numeric IP address. Default: (none) listen_address6 Like listen_address, but specifies the default listening address for the IPv6 listening (which is used when set to listen_ipv6 setting). The format is the default IPv6 address format. Default value: (none) local_root this option represents the directory that vsftpd will try to change after local (i.e. not anonymous) login. Failure is silently ignored. Default: (none) message_file this option is the name of the file we are looking for when a new directory is entered. The content is displayed to a remote user. This option is only up-to-date if the dirmessage_enable option is enabled. Default: .message nopriv_user is the user name that is used by vsftpd when it wants to be completely unprivilidated. Note that this should be highlighted by the user, not by a single one. No one is usually used to many important things on most machines. Default: No pam_service_name this line is the name of the PAM vsftpd service to be used. Default: vsftpd pasv_address use this option to override the IP address that vsftpd will advertise in response to the PASV command. Provide numeric IP address for IP address if you pasv_addr_resolve, in this case, you can enter the host name that will be resolved by DNS at startup. Default: (none - Address taken from incoming connected socket) rsa_cert_file This option specifies the location of the RSA certificate to use for encrypted SSL 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 encrypted SSL connections. If this option is not set, it is expected that the private key will be in the same file as the certificate. Default: (none) secure_chroot_dir this option must be the name of an empty directory. Additionally, the directory must not be recorded by the FTP user. This directory is used as a secure prison chroot() sometimes vsftpd does not require access to the file system. Default: /var/run/vsftpd/empty ssl_ciphers This option can be used to select which SSL vsftpd encryptions will allow encrypted SSL connections. See the man encrypts page for more information. Note that limiting the encrypts can be a useful security precaution because it prevents malicious remote parties forcing the encrypt with which they have detected problems. Default: DES-CBC3-SHA upload_file This option can be configured to restrict the download of files with names that match the specified template. If the file name also matches the deny_file template, the failure takes precedence. For information about usage and template, see deny_file. Default value: (none) user_config_dir this powerful option allows you to override any configuration parameter specified on the guide page based on each user. The use is simple, and best illustrated by example. If you set user_config_dir /etc/vsftpd_user_conf and then log on as a chris user, vsftpd will apply the settings in the /etc/vsftpd_user_conf/chris file throughout the session. The format of this file is also described in detail on this page of the manual! Note that not all parameters are effective based on each user. For example, many parameters are only before the session of the user who started. Examples of settings that won't affect any behviour based on each user include listen_address, banner_file, max_per_ip, max_clients, xferlog_file, etc. Default: (none) user_sub_token this option is useful, it is a combination with virtual users. It is used to automatically create a home directory for each virtual user based on the template. For example, if the real user's home directory specified with guest_username is /home/virtual/$USER, and user_sub_token is set to $USER, then when a virtual user fred logs in, it will end up (usually chroot()'ed) in the /home/virtual/fred directory. This option is also affected if local_root contains user_sub_token. Typical (none) userlist_file this option is the file name loaded userlist_enable the error parameter option is active. Default: /etc/vsftpd.user_list vsftpd_log_file This option is the filename to which we write the vsftpd style log file. This log is only written if the option installed, and xferlog_std_format not set. Also, it's written if you've installed dual_log_enable. Another complication is that if you have installed syslog_enable, then this file is not written and the output is sent to the system log. Default: /var/log/vsftpd.log xferlog_file This option is the name of the file to which we write wu-ftpd style transfer log. The upload log will only be recorded if a xferlog_enable is set, next to xferlog_std_format. Also, it's written if you've installed dual_log_enable. Default: /var/log/xferlog AUTHOR scarybeasts@gmail.com VSFTPD. CONF(5) SSFTPD. (5)