

vsftpd перевод конфигурационного файла

```
# Разрешать анонимный доступ
anonymous_enable=NO/YES
#Разрешать анонимным пользователям пользоваться SSL
allow_anon_ssl=NO/YES
# Разрешить создавать директории анонимным пользователям в incoming
anon_mkdir_write_enable=NO/YES
# Разрешить запись в другие директории анонимному пользователю
anon_other_write_enable=NO/YES
# Разрешить заливать файлы анонимным пользователям в incoming
anon_upload_enable=NO/YES
При включение этой опции, анонимным пользователям будет разрешено скачивать только видимые ими
из мира файлы. Предполагается полезным, если пользователи могут загружать
на сервер и хранить на нем собственные файлы.
anon_world_readable_only=NO/YES
Default: YES
Если включить, ASCII режим передачи данных будет разрешен при download.
ascii_download_enable=NO/YES
Default: NO
Если включить, ASCII режим передачи будет разрешен при uploads.
ascii_upload_enable=NO/YES
Default: NO
При включении, специальные FTP команды известные как «asynс ABOR» будут разрешены. Только плохо
продуманные FTP клиенты используют эту функцию.
В добавок эта функция неудобна в управлении, поэтому отключена по умолчанию. К сожалению,
некоторые FTP клиенты могут зависать в момент отмены передачи,
если эта функция выключена. Если это происходит можно попробовать включить эту функцию.
asynс_abor_enable=NO/YES
Default: NO
При включении, vsftpd стартуя в режиме listen, работает в фоновом режиме. Т.е. контроль передается той
оболочке в которой был запущен vsftpd.
background=NO/YES
Default: NO
(проверять /etc/shells при попытке входа локальных пользователей)
check_shell=NO/YES
Default: YES
Эта опции разрешает использование SITE CHMOD команд устанавливающих права доступа для файла.
Анонимные пользаки не могу это использовать.
chmod_enable=NO/YES
Default: YES
Меняться у всех анонимно закачанных файлов на сервер будут изменены владельцы на пользователя в
указанного в chown_username.
chown_uploads=NO/YES
Default: NO
/etc/vsftpd.chroot_list задаётся список пользователей, при аутентификации которых делается chroot в их
домашний каталог
chroot_list_enable=NO/YES
```

Default: NO

Привязать локального пользователя к замкнутой среде. Если выбрано локальные пользователи будут (по умолчанию) перенесены в chroot () «заточение»

в их домашнем каталоге после входа. Внимание: эта опция имеет смысл быть включенной из соображений безопасности, особенно если пользователи имеют права позволяющие загрузку файлов на сервер, или shell доступ.

chroot_local_user=NO/YES

Default: NO

При включении исходящие с сервера соединения исходят с порта 20, при выключении сервер может работать с несколько меньшими привилегиями.

connect_from_port_20=NO/YES

Default: NO

Значение YES приводит к протоколированию работы подключений по SSL. (Добавлено в 2.0.6)

debug_ssl=NO/YES

Default: NO

Начиная с версии 2.0.7 vsftpd умеет удалять неудавшиеся загрузки, если определить следующий параметр.

delete_failed_uploads=NO/YES

Default: NO

позволяет использовать список анонимных паролей типа e-mail, при использовании которых попытки подключения будут отвергнуты. По умолчанию, файл содержащий этот список располагается в /etc/vsftpd.banned_emails, но имеется возможность изменить путь, указав альтернативный путь в banned_email_file.

deny_email_enable=NO/YES

Default: NO

Значение NO запрещает доступ на выполнение команд просмотра содержимого каталогов.

dirlist_enable=NO/YES

Default: YES

При входе в каталог пользователям показывается сообщение из файла .message. По умолчанию, директория сканируется на наличие

сообщения в файле .message, что можно изменить задав имя другого файла.параметром message_file

dirmessage_enable=NO/YES

Default: NO (but the sample config file enables it)

Значение NO запрещает выполнять скачивание файлов.

download_enable=NO/YES

Default: YES

Значение YES включает параллельную генерацию двух журналов /var/log/xferlog и /var/log/vsftpd.log.

Первый формируется в стиле wu-ftp, второй в собственном формате vsftpd.

dual_log_enable=NO/YES

Default: NO

Файлы и каталоги имена которых начинаются с «.» будут показаны при листинге каталогов, даже если флаг «a» не был использован клиентом.

force_dot_files=NO/YES

Default: NO

Работает только если включен параметр ssl_enable. Значение YES принудительно переключает соединения всех анонимных пользователей в режим SSL при скачивании и закивании файлов.

force_anon_data_ssl=NO/YES

Default: NO

Разрешено только при включенном ssl_enable. При включении, все анонимные подключения будут использовать безопасные SSL соединения при посылке паролей.

force_anon_logins_ssl=NO/YES

Default: NO

Разрешено только если ssl_enable активно. При включении, все не анонимные подключения используют безопасные SSL соединения для приема и передачи данных.

force_local_data_ssl=NO/YES

Default: YES

Работает только если включен параметр ssl_enable. Значение YES принудительно переключает соединения всех НЕ-анонимных пользователей в режим SSL при отправке пароля.

force_local_logins_ssl=NO/YES

Default: YES

Все неанонимные входы рассматриваются от имени гостевого пользователя; это позволяет производить аутентификацию с помощью PAM (pam_userdb) относительно файла имён виртуальных пользователей.

guest_enable=NO/YES

Default: NO

Скрывать имена владельцев файлов и группы.

hide_ids=NO/YES

Default: NO

Установка SSL соединения происходит в первую очередь.

implicit_ssl=NO/YES

Default: NO

Если опция включена сервер стартует в независимом от inetd/xinetd режиме «standalone mode». В этом случае он сам заботится о прослушивании и определении входящих соединений.

listen=NO/YES

Default: NO

Тоже что и для параметра listen, только vsftpd будет обслуживать IPv6, а не только IPv4. Этот параметр и параметр listen являются взаимоисключающими.

listen_ipv6=NO/YES

Default: NO

Разрешает или запрещает вход для локальных пользователей. Если включено обычные пользовательские аккаунты в /etc/passwd могут быть использованы для входа.

Должно быть включено для разрешения любых не анонимных входов, включая вход виртуальных пользователей.

local_enable=NO/YES

Default: NO

При включении опции, все загрузки на сервер происходят с блокировкой записи загружаемого файла. Все загрузки с сервера совершаются с общей блокировкой чтения скачиваемых файлов.

lock_upload_files=NO/YES

Default: NO

Значение YES приводит к протоколированию всех запросов и ответов протокола FTP, а также в выключению параметра xferlog_std_format.

log_ftp_protocol=NO/YES

Default: NO

Значение YES включает использование «ls -R». Это создаёт значительный риск безопасности, потому что выполнение «ls -R» для каталога верхнего уровня, который содежит множество подкаталогов и файлов, может привести к очень большому потреблению ресурсов.

ls_recurse_enable=NO/YES

Default: NO

Разрешает обновления времени модификации файла через MDTM ftp команды.

mdtm_write=NO/YES

Default: YES

Если YES vsftpd не спрашивает пароль у анонимных пользователей, позволяя им подключаться сразу.

no_anon_password=NO/YES

Default: NO

Значение YES говорит vsftpd не выполнять блокировку при записи в файлы журналов. Обычно данный параметр выключен. В Solaris в связке с файловой системой Veritas иногда появляется ошибка, выражающаяся в зависании при попытке установить блокировку на файлы журналов.

no_log_lock=NO/YES

Default: NO

Для ядер 2.4 поддерживается другая модель безопасности: один процесс на одно соединение. Такая модель менее безопасна, но более производительна. Не включайте, если не понимаете что делаете и если вашему серверу не нужна поддержка огромного количества отдельных соединений.

one_process_model=NO/YES

Default: NO

Работает при включенном параметре chroot_local_user. Пользователи помещаются в свои домашние директории, которые указаны в файле /etc/passwd.

Точное указание пути ./ указывает что пользователь будет перемещен при входе в директорию в этом пути.

passwd_chroot_enable=NO/YES

Default: NO

Установите YES, если вы хотите использовать имя (вместо IP адреса) в pasv_addr.

pasv_addr_resolve=NO/YES

Default: NO

Если хотим запретить PASV метод соединения. То отключаем.

pasv_enable=NO/YES

Default: YES

Включите, если хотите запретить PASV security check, контролирующую подключения с одинаковыми ip адресами. Включайте это, только если вы знаете что делаете! Используется в некоторых туннельных соединениях, возможно в FXP.

pasv_promiscuous=NO/YES

Default: NO

Установите NO, если вы хотите запретить метод PORT в полученном соединении для приёма/передачи данных.

port_enable=NO/YES

Default: YES

Установите YES, если вы хотите запретить проверку безопасности PORT, назначение которой убедиться, что исходящее соединение подключено именно к клиенту. Включайте только если понимаете, что делаете!

port_promiscuous=NO/YES

Default: NO

Значение YES требует от всех SSL клиентов наличия клиентского сертификата. Уменьшение подлинности, применимое к этому сертификату, управляется параметром validate_cert (добавлен в 2.0.6).

require_cert=NO/YES

Default: NO

Требовать многократного использование SSL сессии.

Опции require_ssl_reuse=NO стоит уделить особое внимание, по умолчанию она включена в результате некоторые ftp-клиенты не смогут подключиться к серверу (возникнет ошибка SSL connection failed; session reuse required). Поэтому ее стоит либо переключить в NO, тем самым увеличив угрозу перехвата данных. Либо перейти на "правильный" клиент, это FileZilla, lftp и консольный ftp-ssl.

require_ssl_reuse=NO/YES

Default: YES

Установите YES, если вы хотите запускать vsftpd от пользователя, который собственно и производит запуск. Обычно это нужно в тех случаях, когда доступ от пользователя root недоступен. **СЕРЬЁЗНЕЙШЕЕ ЗАМЕЧАНИЕ!** НЕ включайте этот параметр пока вы полностью не осознаете то, что вы делаете, так как использование этого параметра может создать серьёзную проблему с безопасностью. Особенно важно,

чтобы vsftpd не мог использовать / в качестве корневого каталога, а также используйте chroot для ограничения доступа к файлам, когда включен данный параметр (даже если vsftpd запущен от root). Менее подходящим решением может быть использование deny_file с такими аргументами как {/*, *..*}, но надёжность такого решения не может сравниться с chroot, так что сильно на это не полагайтесь. При использовании этого параметра, вводятся ограничения на другие опции. Например не ждите, что будут работать опции требующие привелегий, такие как неанонимные входы, загрузка файлов с изменением владельца, соединение по 20 порту и подключение по портам меньше, чем 1024, а также и другие подобные.

run_as_launching_user=NO/YES

Default: NO

Если хотим разрешить вход анонимным пользователям только на основе проверки паролей указанных в e-mail листе. Это простой путь ограничения доступа к низко безопасному содержимому без необходимости в виртуальных пользователях. При включении, анонимные входы блокируются если пароль не содержится в файле указанном опцией email_password_file. Формат файла — один пароль на строку. По умолчанию файл располагается в /etc/vsftpd.email_passwords.

secure_email_list_enable=NO/YES

Default: NO

При значении YES, vsftpd будет пытаться вести сессии. При этом он будет пытаться обновлять wtmp и utmp. Если для авторизации используется PAM, то vsftpd также будет пытаться открывать pam_session при входе и закрывать его только при выходе пользователя. Если вам не нужно протоколирование сессий, вы можете запретить это, а также вы можете указать vsftpd запускать меньше процессов и/или с меньшими привилегиями. Модификация wtmp и utmp работает только, если vsftpd собран с поддержкой PAM.

session_support=NO/YES

Default: NO

Если значения выставим в YES то vsftpd будет пытаться показывать информацию о состоянии сессий в списке процессов. Другими словами, показываемое имя процесса будет изменено, чтобы отражать состояние сессии vsftpd (idle, downloading и т.д.) Из соображений безопасности, возможно вам лучше оставить этот параметр выключенным.

setproctitle_enable=NO/YES

Default: NO

Vsftpd будет обслуживать безопасные соединения через SSL. Это относится как к управляющим соединениям, так и к соединениям передающим данные. Также необходимо, чтобы и клиент поддерживал SSL соединения. Используйте этот параметр с осторожностью, потому что vsftpd целиком полагается на библиотеку openssl в плане безопасности SSL соединений и не может гарантировать, что эта библиотека свободна от ошибок.

ssl_enable=NO/YES

Default: NO

Vsftpd запрашивает (но не делает из этого необходимости) у клиента сертификат. Обычно, это не вызывает проблем, но IBM zOS считает иначе (добавлено в 2.0.7).

ssl_request_cert=NO/YES

Default: YES

Применяется только если включен параметр ssl_enable. В случае YES допускаются соединения по протоколу SSL v2. Предпочтительными являются соединения по протоколу TLS V1.

ssl_sslv2=NO/YES

Default: NO

Применяется только если включен параметр ssl_enable. В случае YES допускаются соединения по протоколу SSL v3. Предпочтительными являются соединения по протоколу TLS V1.

ssl_sslv3=NO/YES

Default: NO

Разрешено только если ssl_enable включено. Если разрешено, эта опция разрешает соединения по

протоколу TLS v1 который является оптимальным.

ssl_tlsv1=NO/YES

Default: YES

Загрузки должны завершаться через SSL, а не через EOF принятый через сокет. Это сделано для того чтобы убедиться что атакующий не завершил закачку подделанным TCP FIN.

strict_ssl_read_eof=NO/YES

Default: NO

Если параметр установлен в «YES», то скачиваемые с vsftpd SSL-данные обязаны заканчиваться через SSL, а не через EOF на сожете. По-умолчанию параметр установлен в «NO», так как не нашлось ни одного FTP-клиента, который бы это поддерживал. Потребность в использовании этого параметра незначительна. Всё, на что влияет этот параметр, является возможностью сервера удостовериться в том, подтвердил ли FTP-клиент окончание скачанного файла. FTP-клиенты в состоянии проверить целостность скачанных файлов даже без этого параметра. (Добавлено в v2.0.7).

strict_ssl_write_shutdown=NO/YES

Default: NO

При включении, все выходы журнала направляемые ранее в /var/log/vsftpd.log будут направляться в системный журнал вместо этого.

syslog_enable=NO/YES

Default: NO

Если включено, и vsftpd был скомпилирован с поддержкой tcp_wrappers, входящие соединения контролируются через tcp_wrappers. Этот механизм предоставляет возможность контролировать соединения по ip адресам, назначая конкретному подключению отдельный конфигурационный файл vsftpd. Параметры tcp_wrappers устанавливаются в конфигурационных файлах /etc/hosts.allow и /etc/hosts.deny, среди них есть переменная окружения VSFTPD_LOAD_CONF, указывающая на месторасположения файла с альтернативными vsftpd.conf параметрами для определенного правила (ip адреса) напротив которого она указана.

tcp_wrappers=NO/YES

Default: NO

По умолчанию в полях листинга каталогов пользователей и групп отображаются цифровые ID. Включив эту опцию можно задать текстовые отображения. Это выключено по умолчанию по причине производительности.

text_userdb_names=NO/YES

Default: NO

При включении, vsftpd распознает имена каталогов с тильдой «~» в начале как папки пользователей, папки будут распознаны только если файл /etc/passwd находится в _current_chroot().

tilde_user_enable=NO/YES

Default: NO

Если параметр установлен в «YES», то vsftpd будет отображать время в вашей локальной временной зоне в списке содержимого в каталоге. По-умолчанию отображается GMT. Этот параметр может затронуть также время, возвращаемое FTP-командой «MDTM».

use_localtime=NO/YES

Default: NO

Внутреннее значение, используемое для проверки относительной выгоды использования системного вызова sendfile() на вашей платформе.

use_sendfile=NO/YES

Default: YES

Эта опция работает если userlist_enable включен. Если выбрано значение NO, значит вход пользователей будет отклонен если они не найдены в файле указанном usrlst_file. Если вход отклоняется, отказ производится перед тем как у пользователя будет запрошен пароль.

userlist_deny=NO/YES

Default: YES

Эта опция работает если `userlist_enable` включен. Если выбрано значение NO, значит вход пользователей будет отклонен если они не найдены в файле указанном `usrlist_file`. Если вход отклоняется, отказ производится перед тем как у пользователя будет запрошен пароль.

`userlist_enable=NO/YES`

Default: NO

Если параметр установлен в «YES», то все полученные SSL-сертификаты от клиентов должны пройти проверку «ОК». Самостоятельно подписанные сертификаты не проходят проверку «ОК». (Добавлено в v2.0.6).

`validate_cert=NO/YES`

Default: NO

Если включено, виртуальные пользователи будут использовать одинаковые с локальными пользователями привилегии. По умолчанию, виртуальные пользователи используют одинаковые с анонимными пользователями привилегии, предполагающие большие ограничения, (особенно условия доступа на запись).

`virtual_use_local_privs=NO/YES`

Default: NO

Разрешает FTP команды изменяющие файловую систему. Такие команды как: STOR, DELE, RNFR, RNT0, MKD, RMD, APPE, SITE.

`write_enable=NO/YES`

Default: NO

Если включено, журнал будет включать детальные отчеты о заках на сервер, и заках с сервера (uploads, downloads). По умолчанию, этот файл будет располагаться в `/var/log/vsftpd.log`, но расположение может быть изменено используя опцию `vsftpd_log_file`.

`xferlog_enable=NO/YES`

Default: NO (but the sample config file enables it)

Если включено, запись в журнал производится в стандартном `wu-ftp` стиле, `xferlog` формата. Полезно при желании использования уже существующих привычных способов генерации статистики. Однако с другой стороны, формат используемый по умолчанию лучше читается. Расположение журнала по умолчанию `/var/log/xferlog`, что может быть изменено при помощи опции `xferlog_file`.

`xferlog_std_format=NO/YES`

Default: NO

Численные значения.

Максимальное время в секундах для выделения подключения с PASV стилем передачи данных.

`accept_timeout`

Default: 60

Максимальная допустимая скорость передачи данных для анонимных пользователей, выражена в байтах в секунду .

`anon_max_rate`

Default: 0 (unlimited)

Значение «`umask`», для создания файлов, применяемое к анонимным пользователям. ПРИМЕЧАНИЕ!

Если вы хотите указать восьмеричные значения, помните о префиксе «0», иначе значение будет принято как десятичное число.

`anon_umask`

Default: 077

Права на файл для операции `chown()` над анонимно загруженными файлами на `vsftpd`. (Добавлено в v2.0.6).

`chown_upload_mode`

Default: 0600

Значение `timeout`, в секундах, которое отводится удалённому ftp-клиенту для ответа на команду «PORT»

`connect_timeout`

Default: 60

Максимальный временной промежуток в секундах, разрешенного замирания процесса передачи данных. Если перерыв превышен, соединение с удаленным клиентом отбрасывается.

`data_connection_timeout`

Default: 300

Число секунд для паузы перед записью в лог после неуспешной авторизации в vsftpd.

`delay_failed_login`

Default: 1

Число секунд для паузы после успешной авторизации в vsftpd.

`delay_successful_login`

Default: 0

Маска файлов назначаемая при загрузке файлов на сервер. При желании возможно изменить на 0777 если есть необходимость сделать исполняемыми загружаемые на сервер файлы.

`file_open_mode`

Default: 0666

Указывается порт для входящих соединений с сервером (пока `connect_from_port_20` включен).

`ftp_data_port`

Default: 20

Значение `timeout`, в секундах, которое отводится удалённому ftp-клиенту для ввода очередной FTP-команды. Если срабатывает событие по `timeout`, то удалённый клиент сбрасывается.

`idle_session_timeout`

Default: 300

Если vsftpd запущен в `standalone` (автономном) режиме, то этот порт будет слушать входящие FTP-соединения.

`listen_port`

Default: 21

Максимальная скорость передачи данных, выраженная в байтах в секунду, для локально аутентифицированных пользователей.

`local_max_rate`

Default: 0 (unlimited)

Значение маски назначения прав доступа к файлам созданным локальными пользователями. Помните! Если вы хотите указать параметр в качестве цифрового значения, указывайте «0» (нулевую) приставку, иначе значение будет определено как целое десятизначное.

`local_umask`

Default: 077

Если vsftpd запущен в `standalone` (автономном) режиме, то этот параметр указывает максимальное количество FTP-клиентов, которое может быть подключено. Любые, дополнительно подключившиеся пользователи, получают сообщение об ошибке.

`max_clients`

Default: 0 (unlimited)

Количество неудачных попыток входа, после которых сессия прекращается.

`max_login_fails`

Default: 3

Если vsftpd находится в `standalone mode`, эта опция указывает максимально возможное количество клиентов с одинаковыми ip адресами. Клиентские подключения пытающиеся превысить этот лимит, получают сообщение об ошибке.

`max_per_ip`

Default: 0 (unlimited)

Максимальное значение порта, для соединения типа «PASV». Может использоваться для указания диапазона портов фаерволу.

`pasv_max_port`

Default: 0 (use any port)

Минимальное значение порта, для соединения типа «PASV». Может использоваться для указания диапазона портов фаерволу.

pasv_min_port

Default: 0 (use any port)

Возможно, и не потребуется менять это значение, но попробуйте установить значение «8192» для более гладкого лимита пропускной способности.

trans_chunk_size

Default: 0 (let vsftpd pick a sensible setting)

СТРОКОВЫЕ ПАРАМЕТРЫ

В этой строке указывается каталог, в который vsftp будет переводить анонимных пользователей после входа. При неудаче просто игнорируется.

anon_root

Default: (none)

Эта опция указывает имя файла, в котором содержится список анонимных e-mail паролей не принимаемых сервером. Сервер сверяется с этим файлом если опция deny_email_enable включена.

banned_email_file

Default: /etc/vsftpd.banned_emails

Параметр содержит имя файла, в котором содержится текст, который отображается когда кто-то подключился к серверу. Если параметр установлен, то он отменяет параметр «ftpd_banner».

banner_file

Default: (none)

Параметр содержит имя файла, из которого загружаются сертификаты «Certificate Authority» (CA) для проверки подлинности сертификатов от FTP-клиентов. К сожалению, по-умолчанию путь до файла с SSL-сертификатами CA не используется, так как vsftpd использует ограничения доступа к файлам в различных местах файловой системы (из-за chroot). (Добавлено в v2.0.6).

ca_certs_file

Default: (none)

Параметр содержит пользователя, которому принадлежат права на анонимно загруженные на vsftpd файлы. Этот параметр работает только если параметр «chown_uploads» установлен в «YES».

chown_username

Default: root

Опция является дополнением к chroot_list_enable указывает альтернативный путь к файлу содержащему список локальных пользователей которые будут перемещены в chroot()

заточение в их домашние каталоги при входе. Эта опция уместна только при разрешенной

chroot_list_enable. Если опция chroot_local_user включена, наоборот указывает

файл списка пользователей не помещаемых в chroot() заточение.

chroot_list_file

Default: /etc/vsftpd.chroot_list

В этой опции указывается список разделенных запятыми команд разрешенных FTP (post login. USER, PASS и QUIT pre-login всегда разрешены). Другие команды запрещены.

Пример: cmds_allowed=PASV,RETR,QUIT

cmds_allowed

Default: (none)

Параметр содержит разделённый запятыми список, в котором указаны запрещённые FTP-команды (post login. «USER», «PASS» и «QUIT» всегда разрешены в pre-login). Если команда указывается в двух списках — в этом параметре и в «cmds_allowed», то тогда, отказ имеет приоритет.

cmds_denied

Default: (none)

Эта опция может быть использована для выбора шаблона имен файлов к которым необходимо ограничить доступ. Обозначенный в шаблоне элемент не скрывается, но любая попытка

сделать с ним что нибудь (скачать, изменить и др.) будет отклонена. Эта опция очень проста и не должна использоваться для серьезного контроля доступа. Может быть использована с настройками виртуальных пользователей. Пример: deny_file={*.mp3,*.mov,.private}

deny_file

Default: (none)

Эта опция указывает местонахождение DSA сертификата для использования в SSL зашифрованных соединениях.

dsa_cert_file

Default: (none — an RSA certificate suffices)

Эта опция задает расположение личного DSA ключа для использования в SSL зашифрованных соединениях. Если эта опция не выбрана, сертификат предусматривается как личный ключ.

dsa_private_key_file

Default: (none)

Параметр может использоваться для указания на альтернативный файл для параметра «secure_email_list_enable».

email_password_file

Default: /etc/vsftpd.email_passwords

Имя пользователя, которое будет использоваться для обработки анонимного FTP. Домашний каталог этого пользователя — это корень пространства анонимного FTP.

ftp_username

Default: ftp

В этой опции можно указать банер-строку выводимую на экран клиента при подключении к серверу.

ftpd_banner

Default: (none — default vsftpd banner is displayed)

Опция содержит имя «гостевого» пользователя, определяющее его домашнюю директорию. Работает при включенной guest_enable.

guest_username

Default: ftp

Параметр может быть использован для установки шаблона имён файлов (и имён каталогов, и т.д.), которые должны быть скрыты из просмотра содержимого в каталоге. И, тем не менее, не смотря на то, что они являются скрытыми, они полностью абсолютно доступны для тех, кто знает какие фактические названия (файлов, каталогов) использовать. Файлы и каталоги будут скрыты, если их имена будут содержать строку, полученную из «hide_file», или, если их имена попадают под шаблон регулярного выражения, указанного в «hide_file». Заметьте, что шаблоны регулярных выражений для совпадений в vsftpd — всего лишь простая реализация, которая является подмножеством полнофункциональных регулярных выражений. Для более подробной информации о шаблонах для совпадения в регулярных выражениях смотрите параметр «deny_file». Например: hide_file={*.mp3,.hidden,hide*,h?}.

hide_file

Default: (none)

Если запущен в standalone mode, обычно слушает все адреса (или все локальные интерфейсы). Что может быть отменено указанием определенных ip адресов в этой строке.

listen_address

Default: (none)

Параметр подобен параметру «listen_address», но указывается адрес по-умолчанию для прослушивания входящих IPv6-соединений (которые используются если параметр «listen_ipv6» установлен в «YES»).

Указывается в виде стандартного формата IPv6-адреса.

listen_address6

Default: (none)

Эта опция указывает каталог в который vsftpd должен перевести пользователя после локального не анонимного входа. В случае неудачи просто игнорируется.

local_root

Default: (none)

Параметр указывает на имя файла, который отображается при переходе в новый каталог. Содержимое файла отображается у удалённого пользователя. Параметр будет работать, только если «dirmessage_enable» установлена в «YES».

message_file

Default: .message

Имя пользователя, которое используется vsftpd, когда vsftpd хочет быть полностью непривилегированным. Заметьте, что параметр должен содержать скорее имя пользователя, чем «nobody». На большинстве машин пользователь «nobody» не должен использоваться для большинства важных вещей.

nopriv_user

Default: nobody

В этой строке можно указать имя PAM сервиса который будет использоваться для vsftpd.

pam_service_name

Default: vsftpd

Этой опцией задается IP адрес для ответа на запрос PASV команды. Адрес указывается в цифровом виде, если не включен pasv_addr_resolve. По умолчанию, берётся адрес сокета входящего соединения.

pasv_address

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

Параметр содержит путь в файловой системе до сертификата RSA для использования в зашифрованных SSL-соединениях.

rsa_cert_file

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

Параметр содержит путь в файловой системе до закрытого ключа RSA для использования в зашифрованных SSL-соединениях. Если этот параметр не установлен, то подразумевается, что закрытый ключ находится в одном и том же файле, с сертификатом.

rsa_private_key_file

Default: (none)

Эта опция указывает на имя пустого каталога. Также, каталог не должен быть записываемый для ftp пользователя. Этот каталог используется как безопасный chroot(), когда vsftpd не нужен доступ к файловой системе.

secure_chroot_dir

Default: /usr/share/empty

Параметр может быть использован для выбора SSL-шифра, который vsftpd будет принимать для защищенных SSL соединений. Для более подробной информации смотрите страницы руководства man ciphers. Ограничение шифром может быть использовано для улучшения безопасности, поскольку это предотвращает удалённые попытки отгадать шифр.

ssl_ciphers

Default: DES-CBC3-SHA

Эта опция позволяет задавать дополнительные параметры относительно к отдельным пользователям. Например если в user_config_dir выбрать /etc/vsftpd_user_conf, тогда вход пользователя «chris», означает что vsftpd будет использовать настройки из конфигурационного файла /etc/vsftpd_user_conf/chris для этой сессии. Обратите внимание, не все настройки применимы к отдельным пользователям, например listen_address, banner_file, max_per_ip, max_clients, xferlog_file, и другие.

user_config_dir

Default: (none)

Параметр полезен для взаимодействия с виртуальными пользователями. Параметр используется для автоматического создания домашнего каталога каждому виртуальному пользователю, основываясь на шаблоне. Например, если домашний каталог для настоящего пользователя, задаётся через

«guest_username» как «/home/virtual/\$USER», а «user_sub_token» установлен в «\$USER», то затем как виртуальный пользователь «fred» авторизуется, он попадёт (обычно через chroot()) в каталог «/home/virtual/fred». Этот параметр будет работать, только если «local_root» будет содержать значение «user_sub_token»

user_sub_token

Default: (none)

Этот параметр указывает путь к файлу списка пользователей, загружаемому если userlist_enable параметр включен.

userlist_file

Default: /etc/vsftpd.user_list

Параметр содержит имя файла, в который будет записываться лог в стиле vsftpd. Лог будет писаться только если параметр «xferlog_enable» будет установлен в «YES», а параметр «xferlog_std_format» будет установлен в «NO». Либо будет писаться, если параметр «dual_log_enable» установлен в «YES». Одна сложность — если у вас параметр «syslog_enable» установлен в «YES», то в этот файл ничего записываться не будет, а лог попадет в системный лог.

vsftpd_log_file

Default: /var/log/vsftpd.log

В параметре этой опции можно указать альтернативный путь к файлу журнала записываемому в стиле wu-ftp. Запись в этот журнал производится только при включенной xferlog_enable опции, включительно с xferlog_std_format. Также журнал ведется если включена опция dual_log_enable.

xferlog_file

Default: /var/log/xferlog