Отличный материал по PROFtpd

Взято: http://www.bog.pp.ru/work/ProFTPD.html

ProFTPD разрабатывался группой энтузиастов, недовольных уровнем безопасности и сложностью настройки "классического" FTP-сервера wu-ftpd . Бесплатен (GPL). Описываемая версия - 1.2.8rc1 (28 декабря 2002, заплатка для записи в корневую директорию). Настраивается с помощью одного файла конфигурации, директивы которого напоминают директивы настройки Apache . Реализует RFC-959 (FILE TRANSFER PROTOCOL) и RFC-1123 (кроме команд ACCT, MODE, STRU), частично реализует "IETF Draft: Extensions to FTP" (REST, SIZE, MDTM) и RFC-2228 (FTP Security Extensions), RFC-2389 (Feature negotiation mechanism).

Установка 1.2.10 в CentOS 3.4

Простенький анонимный сервер для централизованной раздачи заплаток (но с возможностью расширения в будущем).

1. получить и распаковать архив
2. make distclean (если не первая сборка)
3. ./configure --with-modules=mod_rewrite:mod_tls --with-includes=/usr/kerberos/include --with-libraries=/usr/kerberos/lib --enable-ctrls (./configure --help даёт список всех ключей; kerberos для tls)
4. можно проверить config.h и настроить include/options.h
5. make
6. make install

- /usr/local/sbin: proftpd (AKA in.proftpd), ftpshut
- /usr/local/bin: ftpcount, ftptop, ftpwho, ftpdctl

- /usr/local/etc/proftpd.conf
- /usr/local/man/man1: ftpwho.1, ftpcount.1, ftptop.1
- /usr/local/man/man5: xferlog.5
- /usr/local/man/man8: proftpd.8, ftpshut.8, ftpdctl.8
- /usr/local/var/proftpd/
- proftpd-inetd
- proftpd.scoreboard

- создать /etc/pam.d/ftp как описано в README.PAM
- добавить в /etc/ftpusers имена пользователей из /etc/passwd, которые имеют пароли, но которым не надо давать доступ к FTP
- настроить ProFTPD (/usr/local/etc/proftpd.conf), в т.ч.
- ServerType standalone
- DefaultServer on
- IdentLookups off # все-равно им никто не пользуется
- PassivePorts *min max*
- Port 21
- TimeoutSession 86400
- UseReverseDNS off # либо требовать двойной проверки (нереализована)
- AllowFilter ^[-A-Za-z0-9_.(),/]*$ # на всякий случай ;)
- AllowForeignAddress off # запретить пересылку сервер-сервер
- AllowOverride off # запретить использование .ftpaccess
- AllowOverwrite on
- DefaultRoot ~
- User nobody # uid/gid по умолчанию с ничтожными правами
- Group nobody
- # сначала запретить доступ снаружи
- Order allow,deny
- Allow from 195.161.72.0/23
- Deny from all

-
-
- IgnoreHidden on

-
- # ножик в руки только своим
- #Order deny,allow
- #AllowUser ftpadmin
- #AllowUser webadmin
- DenyAll

-
- PathDenyFilter "(^.ftpaccess$)" # чтобы не порождать иллюзий
- RequireValidShell no # не всем, имеющим доступ к ftp, нужен shell
- Umask 022
- ServerAdmin spamtrap@deol.ru
- ServerIdent on "FTP server"
- ServerName "имя сервера"
- AllowLogSymlinks off
- DebugLevel 3
- ExtendedLog syslog:debug ALL default
- LogFormat default "%h %l %u %t "%r" %s %b"
- SyslogFacility FTP
- SyslogLevel debug
- TransferLog /var/log/xferlog
- WtmpLog on
-

Установка 1.2.8rc1 в Linux Red Hat 7.2

Задачи, стоящие перед сервером:

- доступ к обихоженной части mirror для своих anonymous
- доступ к софту из нашей библиотеки для доступа к интернет для своих anonymous с возможностью изменений (специальный пользователь ftpadmin, группа ftpadmin)
- доступ к рекламным материалам для всех остальных anonymous с возможностью изменений (пользователь ftpadmin, группа ftpadmin)
- ящик для входящих факсов (специальный пользователь fax, группа fax и имя хоста fax-holder)
- ftp сервер для изменения вебмастером наших сайтов (специальный пользователь webadmin, группа webadmin)
- ftp сервер для клиентских сайтов (группа webusers)

1. получить и распаковать архив
2. make distclean (если не первая сборка)
3. ./configure --with-modules=mod_linuxprivs:mod_rewrite:mod_tls (mod_linuxprivs переименован в mod_cap и встроен; ./configure --help даёт список всех ключей)
4. можно проверить config.h и настроить include/options.h
5. make
6. make install

- /usr/local/sbin: proftpd (AKA in.proftpd), ftpshut
- /usr/local/bin: ftpcount, ftptop, ftpwho
- /usr/local/etc/proftpd.conf
- /usr/local/man/man1: ftpwho.1, ftpcount.1
- /usr/local/man/man5: xferlog.5
- /usr/local/man/man8: proftpd.8, ftpshut.8
- /usr/local/var/proftpd/
- proftpd-inetd
- proftpd.scoreboard

- создать /etc/pam.d/ftp как описано в README.PAM
- добавить в /etc/ftpusers имена пользователей из /etc/passwd, которые имеют пароли, но которым не надо давать доступ к FTP
- настроить ProFTPD (/usr/local/etc/proftpd.conf), в т.ч.
- ServerType inetd # т.к. нагрузка невелика
- DefaultServer on
- IdentLookups off # все-равно им никто не пользуется
- PassivePorts *min max*
- Port 21 # реальное значение задается в /etc/xinetd.d/proftpd
- TimeoutSession 86400
- UseReverseDNS off # либо требовать двойной проверки (нереализована)
- AllowFilter ^[-A-Za-z0-9_.(),/]*$ # на всякий случай ;)
- AllowForeignAddress off # запретить пересылку сервер-сервер
- AllowOverride off # запретить использование .ftpaccess
- AllowOverwrite on
- DefaultRoot ~
- User nobody # uid/gid по умолчанию с ничтожными правами
- Group nobody
- # сначала запретить доступ снаружи
- Order allow,deny
- Allow from 195.161.72.0/23
- Deny from all

-

-
- IgnoreHidden on

-
- # ножик в руки только своим
- Order deny,allow
- AllowUser ftpadmin
- AllowUser webadmin

-
- PathDenyFilter "(^.ftpaccess$)" # чтобы не порождать иллюзий
- RequireValidShell no # не всем, имеющим доступ к ftp, нужен shell
- Umask 022
- ServerAdmin spamtrap@deol.ru
- ServerIdent on "FTP server"
- ServerName "имя сервера"
- AllowLogSymlinks off
- DebugLevel 3
- ExtendedLog syslog:debug ALL default
- LogFormat default "%h %l %u %t "%r" %s %b"
- SyslogFacility FTP
- SyslogLevel debug
- TransferLog /var/log/xferlog
- WtmpLog on
-
- User ftp
- Group ftp
- RequireValidShell no
- UserAlias anonymous ftp
- WtmpLog off
-
- DenyAll # анонимкам - нет!

-
-

-

- пример скрипта для /etc/rc.d/init.d для запуска/остановки самостоятельного (standalone) ProFTPD приведен здесь (или переделать, например, sshd)
- открыть дырки в сетевых экранах (порты 20, 21 и для пассивных соединений):

- ipchains
- IOS ACL (для клиентов и снаружи)

Настройка

Каждому виртуальному хосту требуется отдельный порт или IP адрес.

ProFTPD может работать в режимах (директива ServerType): standalone или inetd.

Возможно запускать ProFTPD без привилегий суперпользователя. Однако при при этом необходимо установить Port выше 1023, отключить AuthPAM и WtmpLog, обязательно использовать AuthUserFile и AuthGroupFile, установить User и Group на себя. Нельзя использовать DefaultRoot и Anonymous.

Для использования DefaultRoot (chroot) требуется запускать сервер с правами root. Некоторые ОС требуют наличия определенных файлов в корневой директории (например, Solaris требует /dev/tcp и /dev/zero). Символьные ссылки не могут указывать наружу (хотя можно использовать жесткие ссылки или **mount -bind**).

ProFTPD позволяет создавать "виртуальных" пользователей с помощью директив AuthUserFile и AuthGroupFile (или с использованием SQL, LDAP и DB с помощью дополнительных модулей). AuthUserFile определяет замену для /etc/passwd в том же формате, AuthGroupFile - для /etc/group. Зашифрованные пароли хранятся здесь же (аналога для /etc/shadow нет), поэтому права на чтение соответствующих файлов должен иметь только пользователь, указанный в директиве User виртуального сервера (предположительно отдельный пользователь для ftpd). См. также DirFakeUser и DirFakeGroup.

Разнесение ip адресов или шаблонов доменных имен на классы с помощью директив

"Class имя ip адрес/маска" и "Class имя regex шаблон" позволяет ограничить число одновременных соединений для каждого класса с помощью директив "Class имя limit число" (требуется включение механизма классификации директивой "Classes on" и работа в режиме standalone).

Области действия директив конфигурации (секции определяются как в файле настройки Apache с помощью HTML-подобных открывающих и закрывающих тегов):

- основной сервер - все что вне других областей действия
- - здесь задаются параметры, одинаковые для всех виртуальных серверов
- - задание директив для виртуального сервера; использование внутри директивы Port позволяет использовать один адрес для многих виртуальных серверов (только standalone)
- - по умолчанию выполняется chroot() и не проверяется пароль, в отличие от wu-ftpd не требуется наличия других файлов и библиотек в "резервации"; является частью основного сервера или виртуального хоста
- - задаются параметры, специфичные для директории; не могут быть вложенными; последним простым именем может быть "*"; путь должен быть абсолютным, за исключением блока Anonymous; нельзя указывать символьные ссылки; можно использовать символ '~' для указания домашней директории
- - определяет ограничения на использование объектов в директории (дополняет, но не заменяет права доступа файловой системы); в дополнение к командам протокола FTP можно использовать групповые имена: READ (RETR, SITE, SIZE, STAT), WRITE (APPE, DELE, MKD, RMD, RNTO, STOR, XMKD, XRMD), DIRS (CDUP, CWD, LIST, MDTM, NLST, PWD, RNFR, XCUP, XCWD, XPWD), ALL (READ, WRITE, DIRS), LOGIN (только в областях действия - основной сервер, VirtualHost, Anonymous) и имена типа SITE_CHMOD; блоки с групповыми именами имеют меньший приоритет; блок для внутренней области действия имеет больший приоритет, чем для внешней; при определении блока можно указывать несколько имен команд через пробел
- файл .ftpaccess позволяет владельцу директории переопределить ее параметры "на лету"; можно блокировать создание файлов с таким именем или запретить переопределение с помощью директивы "AllowOverride off" (начиная с версии 1.2.8)

Параметры TCP/IP:

- **Bind *IP-адрес*** (область действия - основной сервер, VirtualHost)
- **DefaultAddress *IP-адрес*** (область действия - основной сервер)
- **DefaultServer off** | **on** (использовать ли данную конфигурацию при соединении

на адреса, не упомянутые в VirtualHost; область действия - основной сервер, VirtualHost)

- **IdentLookup on** | **off** (использование протокола ident (RFC 1413) для идентификации подслединившегося клиента; рекомендуется отключить, все равно этот протокол никто больше не использует; область действия - основной сервер, Global, VirtualHost)
- **PassivePorts** ***min max*** (интервал портов, который можно использовать для соединений в пассивном режиме)
- **Port** ***номер-порта*** (только режим standalone)
- **SocketBindTight off** | **on** (только режим standalone; при выключении привязывает сокеты для требуемых портов сразу для всех интерфейсов, иначе - действует аккуратнее, но требует больше открытых файлов)

- **TimeoutIdle** ***секунд*** (600 секунд; никаких действий после входа)
- **TimeoutLogin** ***секунд*** (300 секунд; отводится на авторизацию)
- **TimeoutNoTransfer** ***секунд*** (300 секунд; вошел, но не начал передачу)
- **TimeoutSession** ***секунд*** [**user** ***список-имен-через-запятую*** | **group** ***список-групп-через-запятую***
|
class
имя-класса
] (возможно отрицание, задаваемое восклицательным знаком перед именем; определяет максимальную длительность сессии; по умолчанию - 0 (бесконечность); область действия - основной сервер, VirtualHost, Global, Anonymous)

- **TimeoutStalled** ***секунд*** (3600 секунд; замирание во время пересылки файла; область действия - основной сервер, VirtualHost, Global)
- **UseReverseDNS on** | **off** (определять имя хоста клиента по IP адресу)
- **tcpBackLog** ***размер-очереди*** (5, только для standalone)
- **tcpNoDelay on** | **off** (TCP_NODELAY; область действия - основной сервер, VirtualHost, Global)
- **tcpReceiveWindow** ***байт*** (8192)
- **tcpSendWindow** ***байт*** (8192)

Управление доступом в области действия Limit:

- **Allow from all** | **none** | ***хост*** | ***сеть***
разрешение на действие, определенное в директиве Limit, в зависимости от шаблона IP адреса (**192.168.**) или доменного имени (**.company.ru**); область действия - Limit; по умолчанию - from all;

- **AllowAll** (явное разрешение доступа к области действия Limit, Anonymous или Directory)

- **AllowGroup** ***список-групп-через-запятую***

для доступа к командам, описанным в данной области действия Limit, пользователь должен входить во все упомянутые группы (AND, возможно отрицание, задаваемое восклицательным знаком перед именем группы)

- **AllowUser** ***список-имен-через-запятую***

для доступа к командам, описанным в данной области действия Limit, пользователь должен иметь указанные имена (AND, возможно отрицание, задаваемое восклицательным знаком перед именем)

- **Deny from all** | **none** | ***хост*** | ***сеть***

запрет на действие, определенное в директиве Limit, в зависимости от шаблона IP адреса (**192.168.**) или доменного имени (**.company.ru**); область действия - Limit; по умолчанию - from none;

- **DenyAll** (синоним для команд: "order deny,allow;deny from all")
- **DenyGroup** ***список-групп-через-запятую***

запрещен доступ к командам, описанным в данной области действия Limit, пользователям входящим во все упомянутые группы (AND, возможно отрицание, задаваемое восклицательным знаком перед именем группы)

- **DenyUser** ***список-имен-через-запятую***

запрещен доступ к командам, описанным в данной области действия Limit, для пользователей с указанным именем (AND, возможно отрицание, задаваемое восклицательным знаком перед именем)

- **Order allow,deny** | **deny,allow** (определяет последовательность проверки директив Allow и Deny, а также действия по умолчанию; allow,deny: проверяются директивы Allow, если совпадение найдено, то доступ предоставляется, иначе проверяются директивы Deny и если совпадение найдено, то доступ запрещается, иначе доступ предоставляется; deny,allow: проверяются директивы Deny и если совпадение найдено, то доступ запрещается, иначе проверяются директивы Allow и если совпадение найдено, то доступ предоставляется, иначе доступ запрещается; заметьте, что в apache по умолчанию производятся противоположные действия!)

Управление анонимным доступом:

- **AnonRequirePassword off** | **on**
- **Anonymous** ***корневая-директория*** (задает область действия для анонимного доступа, директория используется для chroot; используется в области действия - основной сервер, Global, VirtualHost)
- **AnonymousGroup** ***список-групп-через-запятую*** (трактовать пользователей из данной группы как анонимных - пароль не требуется, делается chroot в домашнюю директорию; пользователь должен входить во все упомянутые группы (AND, возможно отрицание, задаваемое восклицательным знаком перед именем группы); область действия - основной сервер, Global, VirtualHost)

- **AuthUsingAlias off** | **on** (область действия - Anonymous)

Управление безопасностью:

- **AllowFilter "*регулярное-выражение*"** (ограничение текста параметров команд FTP протокола указанным шаблоном в области действия основной сервер, Global, VirtualHost, Anonymous; рекомендуется задать шаблон, позволяющий использовать буквы, цифры, подчеркивание, точку, запятую и слеш)

- **AllowForeignAddress on** | **off** (разрешить клиентам задавать посторонний IP адрес в команде PORT , что позволяет пересылать данные с одного сервера на другой в области действия основной сервер, Global, VirtualHost, Anonymous)
- **AllowOverride** (?, для apache подобная директива определяет какие опции конфигурации могут быть изменены с помощью .htaccess; off - запрещает использование .ftpaccess?)
- **AllowOverwrite on** | **off** (разрешить перезаписывать существующие файлы, область действия - server config, VirtualHost, Anonymous, Directory, Global, .ftpaccess)

- **AuthAliasOnly off** | **on** (давать доступ только пользователеям, упомянутым в директиве UserAlias, область действия - server config, VirtualHost, Anonymous, Global)

- **AuthGroupFile *имя-файла*** (вместо /etc/group; открывается до chroot; область действия - server config, VirtualHost, Global)
- **AuthOrder** - ?
- **AuthPAM on** | **off** (область действия - основной сервер, Global, VirtualHost)
- **AuthPAMAuthoritative off** | **on** (если PAM отвергает авторизацию, то другие модули даже не вызываются; область действия - основной сервер, Global, VirtualHost)
- **AuthPAMConfig *сервис*** (имя сервиса PAM; по умолчанию - ftp; область действия - основной сервер, Global, VirtualHost)
- **AuthUserfile *имя-файла*** (вместо /etc/passwd; открывается до chroot; если разные пользователи имеют одинаковый uid, то их файлы необходимо разделять с помощью **DefaultRoot ~** ; в этом случае рекомендуется использовать директивы **DirFakeUser on ~** и **DirFakeGroup on ~** ; шифрованный пароль хранится в этом же файле (нет аналога /etc/shadow); MD5 ?; права доступа к этому файлу должны быть достаточны для чтения uid/gid, заданных директивами User/Group, но закрыты ото всех остальных (рекомендуется

создать специального пользователя вместо nobody/nogroup); область действия - server config, VirtualHost, Global)

- **CommandBufferSize *число-символов*** (ограничение максимальной длины команды)
- **DefaultRoot *имя-директории* [*список-групп-через-запятую*]** (куда делать chroot; можно использовать "~" для указания домашней директории; пользователь должен входить во все упомянутые группы (AND, возможно отрицание, задаваемое восклицательным знаком перед именем группы); область действия - server config, VirtualHost, Global)
- **DenyFilter "*регулярное-выражение*"** (запрет текста параметров команд FTP протокола указанным шаблоном в области действия основной сервер, Global, VirtualHost, Anonymous)
- **Group *gid*** (gid, под которым будет работать сервер; область действия - server config, VirtualHost, Global, Anonymous)
- **GroupPassword *gid шифрованный-crypt-пароль*** (использовать не рекомендуется)
- **HideGroup *gid*** (скрывать файлы, принадлежащие данному gid, при выдаче листинга (LIST, NLST), если gid не является первичной группой аутентифицированного пользователя; область действия - Anonymous, Directory)

- **HideNoAccess on** | **off** (скрывать файлы, к которым нет доступа, при выдаче листинга (LIST, NLST); область действия - Anonymous, Directory)

- **HideUser *uid*** (скрывать файлы, принадлежащие данному uid, при выдаче листинга (LIST, NLST), если uid не совпадает с uid аутентифицированного пользователя; область действия - Anonymous, Directory)
- **IgnoreHidden off** | **on** (не только скрывать файлы, на которые распространяется действие директив HideGroup, HideNoAccess и HideUser при выдаче листинга, но имитировать их полное отсутствие; не работает для cd?; область действия - Limit)

- **MasqueradeAddress *ip-адрес*** (в сообщениях клиенту демонстрировать данный адрес или имя в предположении, что по данному адресу работает NAT)

- **MaxClients *число*[*сообщение*]**
- **MaxClientsPerHost *число*[*сообщение*]**
- **MaxClientsPerUser *число*[*сообщение*]**
- **MaxConnectionRate *соединений/секунду***
- **MaxHostsPerUser *число*[*сообщение*]**
- **MaxInstances *число*** (максимальное число одновременно запускаемых процессов в режиме standalone)
- **MaxLoginAttempts *число*** (допускаемое число попыток ввести пароль)
- MaxRetrieveFileSize
- MaxStoreFileSize
- **PathAllowFilter "*регулярное-выражение*"** (ограничение имен создаваемых

файлов указанным шаблоном в области действия основной сервер, Global, VirtualHost, Anonymous; рекомендуется задать шаблон, позволяющий использовать буквы, цифры, подчеркивание, точку, запятую и слеш)

- **PathDenyFilter "*регулярное-выражение*"** (запрет имен создаваемых файлов указанным шаблоном в области действия основной сервер, Global, VirtualHost, Anonymous: PathDenyFilter "(.ftpaccess)|(.htaccess)$"

- **PersistentPasswd on** | **off** (держать ли открытыми файлы /etc/passwd и /etc/group во время работы proftpd, включая chroot)
- **RLimitCPU *soft-limit*|"max"** [***hard-limit***|**"max"**] (максимальное число секунд CPU, отводимых на выполнение процесса)
- **RLimitMemory *soft-limit*|"max"** [***hard-limit***|**"max"**] (максимальное количество байт на процесс)
- **RLimitOpenFiles *soft-limit*|"max"** [***hard-limit***|**"max"**]
- **RequireValidShell on** | **off** (авторизовывать клиента только если он имеет основной shell из списка /et/shells; область действия - основной сервер, Global, VirtualHost, Anonymous)
- **RootLogin off** | **on** (разрешать авторизацию root; область действия - основной сервер, Global, VirtualHost, Anonymous)
- **TCPAccessFiles *имя-allow-файла имя-deny-файла*** (имена файлов содержащих IP адреса, сетки или шаблоны имен в формате tcpwrapper hosts.allow и hosts.deny; имена должны быть абсолютными или начинаться с "~/" или "~имя-пользователя/"; область действия - основной сервер, Global, VirtualHost, Anonymous)
- **TCPGroupAccessFiles *шаблон-группы имя-allow-файла имя-deny-файла*** (задание отдельных hosts.allow и hosts.deny для определенных групп; возможно отрицание, задаваемое восклицательным знаком перед именем группы; область действия - основной сервер, Global, VirtualHost)

- **TCPServiceName *имя-сервиса*** (используется вместо стандартного proftpd при анализе файлов hosts.allow и hosts.deny; область действия - основной сервер, Global, VirtualHost, Anonymous)
- **TCPUserAccessFiles *шаблон-имени-пользователя имя-allow-файла имя-deny-файла***
(задание отдельных hosts.allow и hosts.deny для определенных пользователей; возможно отрицание, задаваемое восклицательным знаком перед именем пользователя; область действия - основной сервер, Global, VirtualHost)

- **UseFtpUsers on** | **off** (пользователи, найденные в файле /etc/ftpusers не допускаются; область действия - основной сервер, Global, VirtualHost, Anonymous)

- **User *uid*** (uid, под которым будет работать сервер; область действия - server config, VirtualHost, Global, Anonymous)
- **UserAlias *входное-имя uid*** (введенное клиентом имя отображается на системный uid; область действия - основной сервер, Global, VirtualHost, Anonymous)

UserAlias anonymous ftp

- **UserDirRoot off** | **on** (chroot на поддиректорию анонимного сервера основываясь на входном имени клиента; область действия - Anonymous) UserAlias foo ftp
  UserDirRoot on
  # аутентификация под именем foo приводит к chroot ~ftp/foo

- **UserPassword *uid шифрованный-crypt-пароль*** (заменяет пароль из /etc/shadow или его аналога; область действия - основной сервер, Global, VirtualHost, Anonymous)

Управление файлами:

- **AllowStoreRestart off** | **on** (разрешить возобновлять запись на сервер, область действия - server config, VirtualHost, Anonymous, Directory, Global, .ftpaccess)

- **DefaultChdir *имя-директории*** [***список-групп-через-запятую***] (можно относительно домашней директории; по умолчанию - в нее; пользователь должен входить во все упомянутые группы (AND, возможно отрицание, задаваемое восклицательным знаком перед именем группы); область действия - server config, VirtualHost, Anonymous, Global)

- **DefaultTransferMode ascii** | **binary**
- **DeleteAbortedStores off** | **on**
- **GroupOwner *имя-группы*** (к какой группе приписывать вновь создаваемые файлы и директории; соблюдаются ограничения прав доступа для текущего пользователя; область действия - Anonymous, Directory, .ftpaccess)

- **HiddenStor on** | **off** (AKA HiddenStores, при загрузке файла на сервер, он записывается под временным именем, а потом переименовывается, что позволяет избежать использования частично переданных файлов; директива несовместима с AllowStoreRestart; область действия - Directory, VirtualHost, Global)

- **StoreUniquePrefix *префикс*** (префикс добавляется к уникальным 6-символьным именам файлов, создаваемых командой STOU)
- **Umask *маска-создаваемых-файлов маска-создаваемых-директорий***(задается восьмеричным числом (см. umask(2)); не позволяет оставить биты eXecute для обычных файлов, но есть команда
SITE CHMOD
права
имя-файла
; область действия - server config, VirtualHost, Anonymous, Global, Directory, .ftpaccess)

- **UserOwner *имя-пользователя*** (к какому uid приписывать вновь создаваемые файлы и директории; соблюдаются ограничения прав доступа для текущего пользователя; не может быть равным 0; область действия - Anonymous, Directory, .ftpaccess)

Управление сообщениями, выдаваемыми клиентам:

- **AccessDenyMsg *сообщение***
- **AccessGrantMsg *сообщение***
- **DeferWelcome off** | **on** (придержать приветствие до аутентификации; часть приветствия все равно выдается)
- **DisplayConnect *имя-файла*** (имя файла абсолютное или относительно домашней директории)
- **DisplayFirstChdir *имя-файла*** (имя файла абсолютное или относительно самой директории; можно использовать макросы:
- %T - текущее время
- %F - свободное место в файловой системе
- %C - имя текущей диретории
- %R - имя удаленного хоста
- %L - имя локального хоста
- %u - имя пользователя, полученное по протоколу ident
- %U - имя пользователя
- %M - максимальное число одновременных соединений
- %N - текущее число соединений
- %E - почтовый адрес администратора
- %x - имя класса пользователя
- %y - число текущих соединений в данном классе
- %z - максимальное число одновременных соединений для данного класса
- %i - число загруженных файлов
- %o - число взятых файлов
- %t - число переданных в обоих направлениях файлов

- **DisplayGoAway *имя-файла*** (имя файла абсолютное или относительно домашней директории; можно использовать макросы)

- **DisplayLogin *имя-файла*** (имя файла абсолютное или относительно домашней директории; можно использовать макросы)
- **DisplayQuit *имя-файла*** (имя файла абсолютное или относительно текущей директории; можно использовать макросы)
- **LoginPasswordPrompt on** | **off** (выдавать ли запрос на ввод пароля, если аутентификация будет безуспешна в любом случае (например, из-за))

- **MultilineRFC2228 off** | **on** (выдавать многострочные сообщения в стандарте RFC 959 или RFC 2228)
- **ServerAdmin *email-администратора*** (%E)
- **ServerIdent off**|**on** [***текст-сообщения***] (текст приветствия, выдаваемого клиенту после соединения; "ProFTPD [version] Server (server name) [hostname]")

- **ServerName *имя-сервера***

Управление журналами (по умолчанию, используется syslog , daemon:debug/authpriv):

- **AllowLogSymlinks on** | **off** (разрешить записывать журнал в файлы, задаваемые символьными ссылками, область действия - основной сервер, Global, VirtualHost)

- **DebugLevel** (уровень отладочной печати, см. ключ --debug)
- **ExtendedLog *имя-файла*** [***список-классов-команд***] ***имя-формата*** (определяет имя файла для записи журнала, имя определенного командой LogFormat формата и список через запятую классов команд: NONE, AUTH, INFO, DIRS, READ, WRITE, MISC, ALL; нельзя давать доступ на запись к директории и файлу никому, кроме root; в качестве имени файла можно использовать строку "syslog:уровень")

- **LogFormat *имя-формата* "*строка-форматирования*"** (привязывает строку форматирования к имени формата; возможные метасимволы (%A, %d, %D, %F, %l, %m, %r, %U передаются от клиента без обработки и могут содержать все, что угодно, включая управляющие символы):

- %% - символ %
- %a - IP адрес клиента
- %A - строка пароля для анонимных клиентов или UNKNOWN
- %b - отправленных байтов
- %{имя переменной окружения}
- %d - простое имя директории для команд работы с директориями
- %D - полное имя директории для команд работы с директориями
- %f - абсолютное имя файла
- %F - имя файла с точки зрения клиента
- %h - DNS имя клиента
- %l - имя клиента, определенное по протоколу ident или UNKNOWN
- %L - IP адрес сервера
- %m - имя команды, полученной от клиента
- %p - номер порта на сервере
- %P - pid сервера
- %r - текст командной строки
- %s - числовой код ответа сервера
- %t - локальное время

- %{формат}t - локальное время в формате strftime(3)
- %T - число секунд, потраченных на передачу
- %u - uid, под которым работал сервер
- %U - параметр команды USER
- %v - имя сервера из ServerName
- %V - DNS имя сервера

LogFormat xfer_fmt "%t %u %f"
ExtendedLog /var/log/upload write xfer_fmt
ExtendedLog /var/log/dnload read xfer_fmt

- **ServerLog** (?)
- **SyslogFacility** источник-сообщения (по умолчанию, сообщения об аутентификации идут как AUTHPRIV, остальные - DAEMON)

- **SyslogLevel** уровень-серьезности (начиная с которого, сообщения будут передаваться на syslog; область действия - сервер, VirtualHost, Global)

- **SystemLog** ***имя-файла*** | **NONE** (перенаправлять сообщения в файл вместо syslog)
- **TCPAccessSyslogLevels** [***уровень-для-allow уровень-для-deny***] (уровень серьезности при записи в syslog соответствующих сообщений tcpwrapper; по умолчанию - info и warn)

- **TransferLog** ***имя-файла*** | **NONE**(имя файла для журнала передачи файлов в формате wu-ftpd; /var/log/xferlog; область действия - сервер, VirtualHost, Anonymous, Global
- **WtmpLog on** | **off** | **NONE** (область действия - сервер, VirtualHost, Anonymous, Global)

Условные операторы: Define (можно также определять параметры в командной строке при запуске proftpd), IfDefine, IfModule. Могут быть вложены. Имеется также директива **Include**.

Формат выдачи оглавления директории (NLST, LIST, STAT)

- DirFakeGroup
- DirFakeMode
- DirFakeUser
- LsDefaultOptions "строка" (область действия - сервер, VirtualHost, Anonymous, Global)

- ListOptions
- **ShowDotFiles off** | **on** (эквивалентно LsDefaultOptions "-A"; область действия - сервер, VirtualHost, Anonymous, Global)
- **ShowSymlinks on** | **off** (показывать символьные ссылки или результатирующие файлы; область действия - сервер, VirtualHost, Anonymous, Global)

- **TimesGMTon** | **off** (показывать GMT или локальные времена; область действия - сервер, VirtualHost, Anonymous, Global)
- **UseGlobbing on** | **off** (позволяет использовать шаблоны вместо имен файлов; область действия - сервер, VirtualHost, Anonymous, Global)

Расположение локальных файлов:

- **PidFile *имя-файла*** (только режим standalone)
- **ScoreboardFile *имя-файла*** (/var/run/proftpd.scoreboard; файл, в котором хранится информация о текущих сессиях)

Ограничение трафика.

- **RateReadBPS *байт-в-секунду*** (область действия - сервер, VirtualHost, Global, Anonymous, Directory)
- **RateReadFreeBytes *байт*** (первые байты бесплатно; область действия - сервер, VirtualHost, Global, Anonymous, Directory)
- **RateReadHardBPS off** | **on** (ждать ли после исчерпания первых бесплатных байт пока средняя скорость не опустится до RateReadBPS)
- **RateWriteBPS *байт-в-секунду*** (область действия - сервер, VirtualHost, Global, Anonymous, Directory)
- **RateWriteFreeBytes *байт*** (первые байты бесплатно; область действия - сервер, VirtualHost, Global, Anonymous, Directory)
- **RateWriteHardBPS off** | **on** (ждать ли после исчерпания первых бесплатных байт пока средняя скорость не опустится до RateWriteBPS)
- **TransferRate** (заменяет старые директивы Rate*)

Модули mod_ratio, mod_ldap, mod_radius, mod_sql имеют свои наборы директив:

- mod_ratio: AnonRatio, ByteRatioErrMsg, CwdRatioMsg, FileRatioErrMsg, GroupRatio, HostRatio, LeechRatioMsg, RatioFile, RatioTempFile, Ratios, SaveRatios, UserRatio

- mod_ldap: LDAPAuthBinds, LDAPDNInfo, LDAPDefaultAuthScheme, LDAPDefaultGID, LDAPDefaultUID, LDAPDoAuth, LDAPDoGIDLookups, LDAPDoUIDLookups, LDAPForceDefaultGID, LDAPForceDefaultUID, LDAPHomedirOnDemand, LDAPHomedirOnDemandPrefix, LDAPHomedirOnDemandPrefixNoUsername, LDAPHomedirOnDemandSuffix, LDAPNegativeCache, LDAPQueryTimeout, LDAPSearchScope, LDAPServer, LDAPUseTLS
- mod_radius: RadiusAcctServer, RadiusAuthServer, RadiusEngine, RadiusLog, RadiusRealm, RadiusUserInfo
- mod_sql: SQLAuthTypes, SQLAuthenticate, SQLAuthoritative, SQLConnectInfo, SQLDefaultGID, SQLDefaultHomedir, SQLDefaultUID, SQLDoAuth, SQLDoGroupAuth, SQLGidField, SQLGroupGIDField, SQLGroupInfo, SQLGroupMembersField, SQLGroupTable, SQLGroupWhereClause, SQLGroupnameField, SQLHomedir, SQLHomedirField, SQLHomedirOnDemand, SQLLog, SQLLogDirs, SQLLogHits, SQLLogHosts, SQLLogStats, SQLLoginCountField, SQLMinID, SQLMinUserGID, SQLMinUserUID, SQLNamedQuery, SQLNegativeCache, SQLPasswordField, SQLProcessGrEnt, SQLProcessPwEnt, SQLRatioStats, SQLRatios, SQLSSLHashedPasswords, SQLScrambledPasswords, SQLShellField, SQLShowInfo, SQLUidField, SQLUserInfo, SQLUserTable, SQLUserWhereClause, SQLUsernameField, SQLWhereClause

mod_unixprivs.

mod_tls.

mod_rewrite.

mod_quota и mod_quotatab (учитываются только данные, переданные по FTP протоколу для данного пользователя).

proftpd и другие программы

proftpd - основная программа пакета, реализующая FTP сервер. Запускается автономно или с помощью xinetd (inetd). Ключи запуска:

- **--help**
- **--version**
- **--list** (выдать список встроенных модулей)
- **--debug *уровень*** (от 0 до 9, 1 - бессмысленный минимум, 4 - вполне достаточный уровень, 5 - слишком подробно; выдается на syslog с уровнем DEBUG, источник задается в конфигурационном файле)

- **--config *имя-файла***
- **--configtest** (только проверить синтаксис)
- **--nodaemon** (не отсоединяться от терминала, вывод на stderr вместо syslog)
- **--define *параметр*** (используется в)

В автономном режиме при получении **SIGHUP** перечитывает файл с описанием конфигурации.

ftpcount - показывает число соединений в настоящий момент (с разбивкой по виртуальным хостам).

ftpwho - показывает информацию о каждом текущем соединении (--verbose показывает также текущую рабочую директорию).

ftptop - аналог программы top для процессов ProFTPD.

Журналы

Logwatch имеет скрипты для обработки журналов ProFTPD.

Формат журнала xferlog (имя файла задается директивой TransferLog):

1. сокращенное английское название дня недели (Sat)
2. сокращенное английское название месяца (Dec)
3. день месяца
4. часы:минуты:секунды (время местное)
5. год (4 цифры)
6. продолжительность передачи в секундах
7. имя или адрес удаленного хоста
8. размер файла в байтах
9. полное имя файла (безотносительно chroot)
10. тип передачи

- a - ascii
- b - binary

- действие над файлом в процессе передачи (для ProFTPD всегда отсутствует)
- C - сжат
- U - разжат
- T - tar-ед
- _- не было произведено никаких действий

- направление передачи
- o - с сервера
- i - на сервер
- d - удаление

- тип пользователя
- a - анонимный
- g - guest
- r - real (из /etc/passwd)

- имя реального пользователя или идентификационная строка (вводимая вместо пароля) для анонимного или гостя (м.б. пробел)
- имя сервиса (ftp)
- способ аутентификации
- 0 - никакой
- 1 - ident (rfc931)

- аутентифицированный идентификатор пользователя. Если аутентификация не использовалась, то звездочка
- завершенность передачи
- c - передача была закончена
- i - не закончена