Pure-ftpd - настройка фтп-сервера pure-ftpd с хранением пользователй в БД MySQL

Опубликовано kolodem в Сб, 2010-07-24 08:40

Итак, приступаем к установке сервера с поддержкой виртуальних юзеров в мускуле.

Ищем пакет в портах:

```
# whereis pure-ftpd
 pure-ftpd: /usr/ports/ftp/pure-ftpd
```

Начинаем инсталяццию:

```
# cd /usr/ports/ftp/pure-ftpd && make install clean && rehash
```

Опции интуитивно понятные, но для наглядности приведу список.

```
[ ] LDAP           Support for users in LDAP directories[X] MYSQL          Support f
or users in MySQL database[ ] PAM            Support for PAM authentication[ ] PGSQL
          Support for users in PostgreSQL database[ ] TLS            Support for TLS
 (experimental)[X] PRIVSEP        Enable privilege separation[X] PERUSERLIMITS  Per-
user concurrency limits[X] THROTTLING     Bandwidth throttling[ ] UPLOADSCRIPT   Sup
port uploadscript daemon[X] UTF8           Support for charset conversion[X] SENDFIL
E       Support for the sendfile syscall[X] LARGEFILE      Support downloading files
 larger than 2Gb[X] VIRTUALCHROOT  Follow symlinks outside a chroot jail[X] ANONRESU
ME     Allow anonymous user to resume file upload[ ] ANONRENAME     Allow anonymous
user to rename file[ ] ANONDELETE     Allow anonymous user to delete file
```

Сообщим фре, что сервер нужен при каждой загрузке:

```
# echo '# Pureftpd FTP Server' >> /etc/rc.conf
 # echo 'pureftpd_enable="YES" ' >> /etc/rc.conf
```

Займемся созданием пользователя фтп:

```
# adduser
Username: pureftpd
Full name: FTP User
Uid (Leave empty for default):
Login group [pureftpd]:
Login group is pureftpd.
Invite proftpd into other groups? []:
Login class [default]:
Shell (sh csh tcsh bash nologin) [sh]: nologin
Home directory [/home/ftp]:
Use password-based authentication? [yes]: no
Lock out the account after creation? [no]:
Username : pureftpd
```

```
Password :
Full Name : FTP User
Uid : 1050
Class :
Groups : pureftpd
Home : /home/pureftpd
Shell : /usr/sbin/nologin
Locked : no
OK? (yes/no): yes
adduser: INFO: Successfully added (ftp) to the user database.
Add another user? (yes/no): no
Goodbye!
```

Начинаем консумацию с БД:

```
# mysql –u username –p
 Enter password:
mysql> create database pureftpd;

Query OK, 1 row affected (0.00 sec)
mysql> grant all on pureftpd.* to 'pureftpd@'localhost' identified by 'password';

Query OK, 0 rows affected (0.00 sec)
mysql>quit

# mysql -u pureftpd -p pureftpd < ftp.sql
```

А вот. собственно и текст дампа (импортировать можно с помощью вкладки SQL в PhpMyAdmin):

```
  use pureftpd;
create table `users` (
`User` varchar(16) NOT NULL default '',
`Password` varchar(32) binary NOT NULL default '',
`Uid` int(11) NOT NULL default '14',
`Gid` int(11) NOT NULL default '5',
`Dir` varchar(128) NOT NULL default '',
`QuotaFiles` int(10) NOT NULL default '500',
`QuotaSize` int(10) NOT NULL default '30',
`ULBandwidth` int(10) NOT NULL default '80',
`DLBandwidth` int(10) NOT NULL default '80',
`Ipaddress` varchar(15) NOT NULL default '*',
`Comment` tinytext,
`Status` enum('0','1') NOT NULL default '1',
`ULRatio` smallint(5) NOT NULL default '1',
`DLRatio` smallint(5) NOT NULL default '1',
PRIMARY KEY (`User`),
UNIQUE KEY `User` (`User`)
) type=MyISAM;

insert into pureftpd.users VALUES ('test',MD5('test'),65534, 31, '/usr', 100, 50, 75, 75, '*', 'Ftp user
(for example)', '1', 0, 0);
```

Настраиваем сервер, редактируя /usr/local/etc/pure-ftpd.conf до следующего состояния:

```
ChrootEveryone yes
BrokenClientsCompatibility no
```

```
MaxClientsNumber 50
Daemonize yes
MaxClientsPerIP 8
VerboseLog no
DisplayDotFiles yes
AnonymousOnly no
NoAnonymous no
DontResolve yes
MaxIdleTime 15
MySQLConfigFile /usr/local/etc/pureftpd-mysql.conf
LimitRecursion 2000 8
AnonymousCanCreateDirs no
MaxLoad 4
Umask 133:022
MinUID 100
AllowUserFXP no
AllowAnonymousFXP no
ProhibitDotFilesWrite no
ProhibitDotFilesRead no
AutoRename no
AnonymousCantUpload no
MaxDiskUsage 90
CustomerProof yes
IPV4Only yes
AltLog w3c:/var/log/pureftpd.log
```

Ну и пояснительная записка;):

```
# Для запуска Pure-FTPd с этой конфигурацией, вместо параметров
# командной строки, запустите такую команду:
# /usr/local/sbin/pure-config.pl /usr/local/etc/pure-ftpd.conf #
# Не забудте изучить документацию на сайте, для получения
# полного списка команд - http://www.pureftpd.org/documentation.shtml [1]
# Chroot`ить всех пользователей в их хомяках
ChrootEveryone yes

# Если в предыдущей опции было выбрано "no", то члены следующей
# группы не будут chroot`ится. Всё остальные - будуте. Если Вы не хотите
# chroot`ить всех, то просто раскоментируйте ChrootEveryone и TrustedGID.

# TrustedGID 100

# Включить "фичи" совместимости, для кривых клиентов

BrokenClientsCompatibility no

# Максимальное число одновременных юзеров

MaxClientsNumber 50

# Работать в фоне (демоном)

Daemonize yes

# Максимальное число одновременных соединений с одного IP

MaxClientsPerIP 8

# Если вы хотите логировать все команды клиентов, то в этом
```

```
# пункте должно быть "yes". Если необходимо логгировать также
# ответы сервера, то просто продублируйте этот пункт.

VerboseLog no

# Показывать или нет файлы, начинающиеся с точки, даже когда клиент
# явно не говорит что это надо делать, опцией "-a".

DisplayDotFiles yes

#Не разрешать аутентифицированных юзеров - этот FTP
# только для анонимных клиентов.

AnonymousOnly no

# Запретить анонимоусов - FTP тока для регистрованных юзеров.

NoAnonymous no

# Средства syslog (auth, authpriv, daemon, ftp, security, user, local*)
# Дефолт - "ftp". "none" - отключает логирование. SyslogFacility ftp
# Показывать куки.

# FortunesFile /usr/share/fortune/zippy

# Не резольвить имена хостов в логах. Логи становятся менее информативными,
# но и ресурсов требуется меньше. "yes" - имеет смысл ставить на очень
# загруженных серверах, или при неработающем DNS.

DontResolve yes

# Максимальное время простоя (по окончании рвётся коннект), в минутах
# (default = 15 minutes)

MaxIdleTime 15

# Файл конфигурации LDAP (смотрите README.LDAP)

# LDAPConfigFile /etc/pureftpd-ldap.conf

# Файл конфигурации MySQL (смотрите README.MySQL)

MySQLConfigFile /usr/local/etc/pureftpd-mysql.conf

# Файл конфигурации Postgres (смотрите README.PGSQL)

# PGSQLConfigFile /etc/pureftpd-pgsql.conf

# база данных юзеров PureDB (смотрите README.Virtual-Users)

# PureDB /etc/pureftpd.pdb

# путь к сокету pure-authd (смотрите README.Authentication-Modules)

# ExtAuth /var/run/ftpd.sock

# Если нужно подключить PAM аутентификацию раскомментируйте
#следующую линию
```

 # PAMAuthentication yes

Если нужна системная, Unix аутентификация (/etc/passwd),
раскомментируйте следующую линию (default: yes)

 # UnixAuthentication yes

Пожалуйста, отметтьте, что LDAPConfigFile, MySQLConfigFile,
PAMAuthentication и UnixAuthentication могут использоваться только
один раз, но они могут использоваться вместе. Например, если вы
используете MySQLConfigFile, затем UnixAuthentication, то идёт запрос
к MySQL. Если в БД такой пользователь не найден, то пробуется
системный пользователь в /etc/passwd и /etc/shadow. Если SQL
аутентификация неудачна по причине неправильного пароля, то происходит
остановка дальнейшего поиска пользователя. Методы аутентификации
будут ипользоваться в порядке в которм они заданы
Пределы рекурсии команды 'ls'. Первй аргумент - максимально число файлов,
которое будет показано. Второе - максимальное число подкаталогов

LimitRecursion 2000 8

Имеют ли право анонимоусы создвать новые директории?

AnonymousCanCreateDirs no

Если система загружена более, чем указанное тут значение, то
анонимоусы не могут что-либо скачивать

MaxLoad 4

Диапазон портов для пассивного соединения. Если у вас файрволл рубает
стандартный диапазон

 # PassivePortRange 30000 50000

Принудительный IP адрес в PASV/EPSV/SPSV ответах. - для NAT.
Символические имена хостов такде приняты для шлюзов с динамическим IP

 # ForcePassiveIP 192.168.0.1

Соотношение upload/download для анонимоусов.

 # AnonymousRatio 1 10

Соотношение upload/download для всех юзеров.
Эта директива не перекрывает предыдущую.

 # UserRatio 1 10

Запретить скачку файлов владельцем которых является "ftp", т.е.
файлы были загружены но не одобрены местным (локальным) админом.

 # AntiWarez yes

IP адрес/порт на которых слушаем (дефолт = все IP и порт 21).

#Bind 192.168.254.254,21

Максимальная скорость для анонимоусов в KB/s

 # AnonymousBandwidth 8

Максимальная скорость для всех юзеров (включая анонимов) в KB/s
Используйте AnonymousBandwidth или UserBandwidth, использовать оба,
не имеет смысла.

 # UserBandwidth 8

Маска для создаваемых файлов. :.

 # 177:077

umask - это такое число, при вычитании которого из максимума (777) и
получается нужная маска. т.е. для случая ниже маски будут, соответственно:
644 для файлов, и 755 для директорий

Umask 133:022

Минимальный UID с которым юзер будет пущен.
Если вы будете использовать фтп сервер для загрузки файлов на веб сервер,
#поправьте значение MinUID, поставьте 80 вместо значения по умолчанию, так как
#ето дефолтное айди пользователя www.

MinUID 100

Разрешить передачу FXP для авторизованных юзеров.
(Это передача файлов прям между серверами - т.е. если вам надо
скопировать файл с одного сервака на другой, вы его вначале тащите
к себе, затем кладёте куда надо. При включении этой опции сервера
сами перекинут файл между собой.

AllowUserFXP no

Разрешить передачу FXP для анонимоусов и не-анонимоусов
(видимо, для всех вообще).

AllowAnonymousFXP no

Пользователи не могут удалять и изменять файлы начинающиеся на точку('.')
даже если они их владельцы. Если TrustedGID включена, эта группа имеет
доступ к этим файлам.

ProhibitDotFilesWrite no

Запретить чтение файлов начинающихся с точки (.history, .ssh...)

ProhibitDotFilesRead no

Никогда не перезаписывать файлы. Когда имя, для закачиваемго файла уже
существует, он будет автоматически переименован в file.1, file.2, file.3, ...

AutoRename no

Запретить анонимным юзерам загружать новые файлы (no = аплоад разрешён)

AnonymousCantUpload no

Только подключения к этому IP адресу могут быть не анонимными. Вы

можете использовать эту директиву чтобы использовать несколько IP
для анонимного FTP, и оставить приватный, зафаерволленый IP для
удалённого администрирования. также вы можете разрешить нероутабельный
локальный IP (типа 10.x.x.x) для аутентификации и оставить публичный
(для анонимоусов) FTP-сервер на другом IP.

#TrustedIP 10.1.1.1

Если вы хотите чтобы PID добавлялся в каждую линию лога, # то раскомемнтируйте следующую линию.

#LogPID yes

Создавать дополнительный лог-файл с логом в формате типа "apache":
fw.c9x.org - jedi [13/Dec/1975:19:36:39] "GET /icap.tar.bz2" 200 21808
Этот лог-файл может быть обработан программами для
анализа логов апача.

 # AltLog clf:/var/log/pureftpd.log

Создавать дополнительный лог-файл в формате оптимизированном для
статистических отчётов (х.з. как это. Надо будет посмотреть)

 # AltLog stats:/var/log/pureftpd.log

Создавать ещё один лог с переданными файлами в стандарте W3C
(совместим с многими коммерческими анализаторами)

 # AltLog w3c:/var/log/pureftpd.log

Отключить команду CHMOD. Пользователи не смогут менять разрешения
на файлы.

#NoChmod yes

Позволить юзерам закачивать но не удалять файлы.

#KeepAllFiles yes

Автоматически создавать домашнюю директорию пользователя,
если она отсутствует

#CreateHomeDir yes

Включить виртуальную квоту. Первое число - максимальное число файлов.
Второе число - максимальный размер, в мегабайтах.
#Так 1000:10 ограничивает каждого пользователя 1000 файлов и 10-ю мегами.

#Quota 1000:10

Если pure-ftpd скомпилен с поддержкой standalone режима, вы можете изменить
местоположение pid-файла. Дефолтовое положение - /var/run/pure-ftpd.pid

#PIDFile /var/run/pure-ftpd.pid

Если pure-ftpd скомпилен с поддержкой pure-uploadscript,
то этот пункт позволяет писать информацию о новых загруженных
файлах в /var/run/pure-ftpd.upload.pipe так что pure-uploadscript может
прочесть их и обработать загруженный файл.

#CallUploadScript yes

Эта опция полезна на серверах, гда позволен аплоад анонимоусам.
Если /var/ftp находится в отдельном разделе /var, это позволяет
сохранить свободное место и защитить файлы логов. Когда процент
заполнения больше чем указанный тут, аплоад автоматом запрещается.

MaxDiskUsage 99

Установите 'yes' в этой опции если хотите разрешить юзерам
переименовывать файлы.

#NoRename yes

Включить 'customer proof': какая-то ошибка, типа 'chmod 0 public_html',

CustomerProof yes

Число параллельных процессов. Работает тока если сервер был
скомпилен с опцией '--with-peruserlimits' (тут чё-то про то, что
в большинстве бинарных дистрибов так оно и есть).
Формат:<максимум сессий на юзера>:<максимум сеансов анонимоусов>
Например, 3:20 значит что аутентифичированный юзер может иметь три
активных сеанса. А на всех анонимов - максимум 20 сеансов.

#PerUserLimits 3:20

Когда загружен файл на сервер, и есть предыдущая версия (с тем же именем),
то старый файл не будет ни удалён ни усечён. Загрузка будет произведена
во временный файл и по окончании загрузки будет произведено атомарное
переключение к новой версии файла. Например, при загрузке большого PHP
сценария, апач будет работать со старой версией до полной загрузки
и немедленно переключится на новый как тока он будет полностью передан
Эта опция несовместима с виртуальными квотами.

#NoTruncate yes

Эта опция может принимать три значения:
0 - отключить SSL/TLS шифрование (по-умолчанию).
1 - принимать и шифрованные и обычные подключения.
2 - отклонять подключения которые не используют SSL/TLS,
включая анонимные соединения.
Не раскомментируйте это вслепую. Проверьте, что:
1) Сервер скомпилен с поддержкой SSL/TLS (--with-tls),
2) Положен валидный сертификат,
3) Только совместимые клиенты залогинятся.

 # TLS 1

Слушается тока IPv4 адрес в режиме standalone (т.е. IPv6 отключен)
По дефолту, IPv4 и IPv6 включены.

IPV4Only yes

Слушается тока IPv6 адрес в режиме standalone (т.е. IPv4 отключен)
По дефолту, IPv4 и IPv6 включены.

 # IPV6Only yes

```
# Поддержка UTF-8 для имён файлов (RFC 2640)
# Определите кодировку для файловой системы сервера и, опционально,
# дефолтовую кодировку для клиентов, которые не юзают UTF-8.
# Работает тока если pure-ftpd скомпилен с '--with-rfc2640' FileSystemCharset koi8-r

#ClientCharset cp1251
```

"Обретаем зрение" с помощью логов:

```
# touch /var/log/pureftpd.log &&  chmod 777 /var/log/pureftpd.log
```

Интегрируем поддержку мускула, редактируя edit /usr/local/etc/pureftpd-mysql.conf до следующего состояния:

```
MYSQLServer 127.0.0.1
MYSQLSocket /tmp/mysql.sock
MYSQLUser pureftpd
MYSQLPassword
FtpPasswd1991
MYSQLDatabase pureftpd
MYSQLCrypt md5
MYSQLGetPW SELECT Password FROM users WHERE User="\L" AND Status="1" AND (Ipaddress =
"*" OR Ipaddress LIKE "\R")
MYSQLGetUID SELECT Uid FROM users WHERE User="\L" AND Status="1" AND (Ipaddress = "*" OR
Ipaddress LIKE "\R")
MYSQLGetGID SELECT Gid FROM users WHERE User="\L" AND Status="1" AND (Ipaddress = "*" OR
Ipaddress LIKE "\R")
MYSQLGetDir SELECT Dir FROM users WHERE User="\L" AND Status="1" AND (Ipaddress = "*" OR
Ipaddress LIKE "\R")
MySQLGetQTAFS SELECT QuotaFiles FROM users WHERE User="\L" AND Status="1" AND (Ipaddress
= "*" OR Ipaddress LIKE "\R")
MySQLGetQTASZ SELECT QuotaSize FROM users WHERE User="\L" AND Status="1" AND (Ipaddress
= "*" OR Ipaddress LIKE "\R")
MySQLGetRatioUL SELECT ULRatio FROM users WHERE User="\L" AND Status="1" AND (Ipaddress =
"*" OR Ipaddress LIKE "\R")
MySQLGetRatioDL SELECT DLRatio FROM users WHERE User="\L" AND Status="1" AND (Ipaddress
= "*" OR Ipaddress LIKE "\R")
MySQLGetBandwidthUL SELECT ULBandwidth FROM users WHERE User="\L" AND Status="1" AND
(Ipaddress = "*" OR Ipaddress LIKE "\R")
MySQLGetBandwidthDL SELECT DLBandwidth FROM users WHERE User="\L" AND Status="1" AND
(Ipaddress = "*" OR Ipaddress LIKE "\R")
IPV4Only              yes
```

И опять коменты:

```
# ????, ?? ??????? ????????? ?????. ?? ???????? ???? ?????, ???? ??????????? ??????
??? unix ?????.MYSQLServer     127.0.0.1
# ????, ?? ??????? ????? MySQL. ?? ???????? ???? ?????, ???? ??????????? ?????????
unix ?????.# MYSQLPort       3306
# ???????? ??? ??????, ???? ?????? ?? ???? ?? ?????.MYSQLSocket     /tmp/mysql.sock
# ???? ??MYSQLUser       pureftpd# ?????? ?????MYSQLPassword    PASSWORD
# Собственно сама БД.MYSQLDatabase  ftp
# Как сохраняются пароли юзеров в БД# Значения : "cleartext", "crypt", "md5" and "password"
# ("password" = MySQL password() function)# Пожно использовать "any" чтобі попробовать "cry
pt", "md5" *and* "password"MYSQLCrypt     md5
# В последующих директивах части строк заменены до выполнения запроса.# \L заменяэтся
именем пользователя, который логинится.# \I заменяется айпишником сервера, к которому к
онектится юзер.# \P номер порта.# \R айпи юзера.# \D айпи юзера в виде long decimal number
```

(например, 192.168.254.1=3232300545).# Запрос на пароль
MYSQLGetPW SELECT Password FROM users WHERE User="\L" AND Status="1" AND /-> (Ipaddress = "*" OR Ipaddress LIKE "\R")# Запрос на uid
MYSQLGetUID SELECT Uid FROM users WHERE User="\L" AND Status="1" AND /-> (Ipaddress = "*" OR Ipaddress LIKE "\R")# Опционально: дефолтний uid.
#MYSQLDefaultUID 1000# Запрос на gid.
MYSQLGetGID SELECT Gid FROM users WHERE User="\L" AND Status="1" AND /-> (Ipaddress = "*" OR Ipaddress LIKE "\R")# Опционально: дефолтний gid.
#MYSQLDefaultGID 1000# Запрос на директорию
MYSQLGetDir SELECT Dir FROM users WHERE User="\L" AND Status="1" AND /-> (Ipaddress = "*" OR Ipaddress LIKE "\R")
Опционально: запрос на максимальное число файлов у юзера# Сервер должен быть скомилирован с virtual quotas support.
MySQLGetQTAFS SELECT QuotaFiles FROM users WHERE User="\L" AND Status="1" /-> AND (Ipaddress = "*" OR Ipaddress LIKE "\R")
Опционально: запрос на квоту, в мегабайтах (virtual quotas)# Обязателен virtual quotas support.
MySQLGetQTASZ SELECT QuotaSize FROM users WHERE User="\L" AND Status="1" AND /-> (Ipaddress = "*" OR Ipaddress LIKE "\R")# Опционально: соотношения download/upload
MySQLGetRatioUL SELECT ULRatio FROM users WHERE User="\L" AND Status="1" AND /-> (Ipaddress = "*" OR Ipaddress LIKE "\R")MySQLGetRatioDL SELECT DLRatio FROM users WHERE User="\L" AND Status="1" AND /-> (Ipaddress = "*" OR Ipaddress LIKE "\R")
Опционально: ширина канала юзера, KB/s .
MySQLGetBandwidthUL SELECT ULBandwidth FROM users WHERE User="\L" /-> AND Status="1" AND (Ipaddress = "*" OR Ipaddress LIKE "\R")MySQLGetBandwidthDL SELECT DLBandwidth FROM users WHERE User="\L" /-> AND Status="1" AND (Ipaddress = "*" OR Ipaddress LIKE "\R")
Выпускать юзера из хомяка. Никогда не дедайте этого, если:# 1) Вы не знаете что делаете.# 2) Совпадают реальные и виртуальные юзеры.**# MySQLForceTildeExpansion 1**
Если вы обновили таблицы до трансакционных, (Gemini,# BerkeleyDB, Innobase...), можна включить SQL трансакцию to# Оставть закоменченними, если юзаете MyIsam ДБ или версию мускула(< 3.23.x).**# MySQLTransactions On**

И, наконец, проверяем работоспособность:

```
 # ftp localhost
Trying 127.0.0.1...
Connected to localhost.
220---------- Welcome to Pure-FTPd [privsep] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 21:12. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.
Name (localhost): test
331 User test OK. Password required
Password:
230-Your bandwidth usage is restricted
230-User test has group access to: ftp
230 OK. Current restricted directory is / Remote system type is UNIX. Using binary mode to transfer files.
ftp>
```

Удачной работы!

Источник (получено *2024-04-25 21:48*):
http://muff.kiev.ua/content/pure-ftpd-nastroika-ftp-servera-pure-ftpd-s-khraneniem-polzovateli-v-bd-mysql

Ссылки:
[1] http://www.pureftpd.org/documentation.shtml