Proftpd - с хранением списка пользователей в MySQL и поддержкой квотирования

Опубликовано muff в Ср, 2010-10-13 18:58



Итак, поставленная задача - "поднять" FTP-сервер с хранением списка пользователей в БД MySQL и назначить этим пользователям квоты, используя mod_quota.

Установим Proftpd из системы портов:

```
# cd /usr/ports/ftp/proftpd-mysql && make install clean && rehash
```

При установке набор опций следующий:

```
Options for proftpd-mysql 1.3.3a_1
????????????????????????????????????????????????????????????????????? [X] BAN
     Include mod_ban (Requires CTRLS)          ? ? [X] CLAMAV           Include mod_
clamav                          ?  ? [X] CTRLS            Include controls
             ?  ? [X] EXEC             Include mod_exec                          ?
 ? [ ] HTMLDOCS         Include HTML documentation                ?  ? [X] IFSESSION
        Include mod_ifsession                     ?  ? [ ] IPV6             Use IPv6
                                  ?  ? [ ] LDAP             Use LDAP
                 ?  ? [ ] LDAP_TLS         Use LDAP TLS (Requires LDAP, OPENSSL)
  ?  ? [X] MYSQL            MySQL auth                                  ?  ? [ ] NLS
           Use nls (builds mod_lang)                 ?  ? [ ] ODBC             ODBC
                                    ?  ? [X] OPENSSL          Include mod_tls
                     ?  ? [ ] PGSQL            Postgres auth
      ?  ? [X] QUOTA            Include mod_quota                          ?  ? [ ] Q
UOTATAB_RADIUS  include mod_quotatab_radius              ?  ? [ ] SHAPER
Shaper module                             ?  ? [ ] SQLITE           SQLite auth
                         ?  ? [ ] RADIUS           Include mod_radius
          ?  ? [X] RATIO            Include mod_ratio                          ?  ? [
X] README           Include mod_readme                         ?  ? [X] REWRITE
    Include mod_rewrite                       ?  ? [ ] TLS_SHMCACHE     TLS SHM sess
ion cache (requires OPENSSL)  ?  ? [ ] TDS              Include mod_sql_tds
             ?  ? [ ] SFTP             Include mod_sftp                          ?
 ? [ ] SFTP_SQL         Include mod_sftp_sql                      ?  ? [ ] SFTP_SQL
        Include mod_sftp_sql                      ?  ? [ ] SFTP_PAM         Include
mod_sftp_pam                      ?  ? [ ] SITE_MISC        Include mod_site_misc
                 ?  ? [X] SQL_PASSWD       Include mod_sql_passwd
  ?  ? [ ] UNIQUE           Include mod_unique_id                     ?  ? [X] WRAP
           Include mod_wrap2                         ?  ? [ ] WRAP_FILE        Incl
ude mod_wrap2_file (requires WRAP)    ?  ? [ ] WRAP_SQL         Include mod_wrap2_sq
l (requires WRAP)     ?  ??????????????????????????????????????????????????????
???????
```

Редактируем конфигурационный файл /usr/local/etc/proftpd.conf до следующего состояния:

```
ServerName              "Company_name FTP server"
ServerAdmin             admin [at] domain [dot] com
ServerType              standalone
DefaultServer           on
ServerIdent             on
Port                    21
Umask                   022
MaxClients              50 "Sorry, the maximum number of allowed users are already connected (%m)"
MaxClientsPerHost       10  "Sorry, you may not connect more than one time."
MaxLoginAttempts        3
User                    ftp
Group                   ftp
SyslogLevel             notice
UseReverseDNS           off
IdentLookups off
SystemLog               /var/log/proftpd/proftpd.log
TransferLog             /var/log/proftpd/proftpd-tranfer.log
ExtendedLog             /var/log/proftpd/proftpd-extended.log read,write
ExtendedLog             /var/log/proftpd/proftpd-auth.log AUTH  auth
LogFormat               default "%h %l %u %t \"%r\" %s %b"
LogFormat               auth    "%v [%P] %h %t \"%r\" %s"
LogFormat               write   "%h %l %u %t \"%r\" %s %b"
TimeoutIdle             300
TimeoutLogin            300
TimeoutNoTransfer       360
TimeoutStalled          640
DefaultTransferMode     binary
AllowForeignAddress     off
UseReverseDNS off
RootLogin off
PassivePorts 50000 60000

DisplayConnect /etc/ftp_connect.msg
DisplayLogin /etc/ftp_login.msg
AccessDenyMsg "ATTENTION!!! ALL CONNECTIONS LOGED"
AccessGrantMsg "Now upload/download files"
DisplayGoAway "Go Away"
PersistentPasswd        off
DefaultRoot             ~

<Directory ~ >
        AllowOverwrite        on
        <Limit Write>
        AllowAll
        </Limit>
        <Limit READ>
        AllowAll
        </Limit>
</Directory>

# Если нужен анонимный доступ раскомментировать.
#< Anonymous /path/for/anonymous>       # Директория для анонимов.
#        User                    ftp
#        Group                   ftp
#        UserAlias               anonymous ftp
#        MaxClients              10
#        < Limit WRITE>
#          DenyAll                       # Запрещаем писать.
#        < /Limit>
```

```
#< /Anonymous>

#sql info
SQLAuthTypes          Crypt   # хранить пароли в шифованом виде
SQLAuthenticate       users
SQLConnectInfo        proftpd@localhost proftpd sql-password #  база@хост логин пароль
SQLUserInfo           users username password uid gid homedir shell #    данные которые беруться
из базы
RequireValidShell     off  # непроверять валидность шелла

# config quotas
# ===========
QuotaEngine on        # включить квоту
QuotaDirectoryTally on
QuotaDisplayUnits Mb
QuotaShowQuotas on
SQLNamedQuery get-quota-limit SELECT "name, quota_type, per_session, limit_type, \
    bytes_in_avail, bytes_out_avail, bytes_xfer_avail, files_in_avail, files_out_avail, \
    files_xfer_avail FROM quotalimits WHERE name = '%{0}' AND quota_type = '%{1}'"
SQLNamedQuery get-quota-tally SELECT "name, quota_type, bytes_in_used, bytes_out_used, \
    bytes_xfer_used, files_in_used, files_out_used, files_xfer_used FROM quotatallies \
    WHERE name = '%{0}' AND quota_type = '%{1}'"
SQLNamedQuery update-quota-tally UPDATE "bytes_in_used = bytes_in_used + %{0}, \
    bytes_out_used = bytes_out_used + %{1}, bytes_xfer_used = bytes_xfer_used + %{2}, \
    files_in_used = files_in_used + %{3}, files_out_used = files_out_used + %{4}, \
    files_xfer_used = files_xfer_used + %{5} WHERE name = '%{6}' AND quota_type = '%{7}'"
quotatallies
SQLNamedQuery insert-quota-tally INSERT "%{0}, %{1}, %{2}, %{3}, %{4}, %{5}, %{6}, %{7}"
quotatallies
QuotaLimitTable sql:/get-quota-limit
QuotaTallyTable sql:/get-quota-tally/update-quota-tally/insert-quota-tally
QuotaLog                    /var/log/proftpd/quota.log
```

Создадим пользователя MySQL, базу данных и выставим необходимые права:

```
# mysql -u root -p
 Enter password:

mysql> CREATE DATABASE proftpd;
 Query OK, 1 row affected (0.00 sec)

mysql> grant select,insert,update,delete  on proftpd.* to proftpd@localhost identified by
'sql-password';
 Query OK, 0 rows affected (0.00 sec)

mysql> USE proftpd;
 Database changed

mysql> CREATE TABLE users (
            primary_key int not null auto_increment primary key,
            username varchar(20) not null,
            password varchar(20) not null,
            uid int not null,
            gid int not null,
            homedir varchar(50) not null,
            shell varchar(20) not null
            );
 Query OK, 0 rows affected (0.00 sec)
```

```
mysql> CREATE TABLE quotalimits (
         name VARCHAR(30),
         quota_type ENUM("user", "group", "class", "all") NOT NULL,
         per_session ENUM("false", "true") NOT NULL,
         limit_type ENUM("soft", "hard") NOT NULL,
         bytes_in_avail FLOAT NOT NULL,
         bytes_out_avail FLOAT NOT NULL,
         bytes_xfer_avail FLOAT NOT NULL,
         files_in_avail INT UNSIGNED NOT NULL,
         files_out_avail INT UNSIGNED NOT NULL,
         files_xfer_avail INT UNSIGNED NOT NULL
       );
 Query OK, 0 rows affected (0.00 sec)

mysql> CREATE TABLE quotatallies (
         name VARCHAR(30) NOT NULL,
         quota_type ENUM("user", "group", "class", "all") NOT NULL,
         bytes_in_used FLOAT NOT NULL,
         bytes_out_used FLOAT NOT NULL,
         bytes_xfer_used FLOAT NOT NULL,
         files_in_used INT UNSIGNED NOT NULL,
         files_out_used INT UNSIGNED NOT NULL,
         files_xfer_used INT UNSIGNED NOT NULL
       );
 Query OK, 0 rows affected (0.00 sec)
```

Добавим системного пользователя ftp групы ftp:

```
# pw user add ftp -s /sbin/nologin -d /nonexistent -g ftp
```

Добавляем пользователей и квоты.

Если системный пользователь - необходимо узнать uid и gid:

```
# cat /etc/passwd | grep muff
 muff:*:1001:0:User &:/home/muff:/bin/tcsh
```

Выполним следующие запросы MySQL:

```
mysql> use proftpd;
 Database changed

mysql> insert into users values
(NULL,'muff',ENCRYPT('user_pass'),'1001','0','/home/muff','/sbin/nologin');
 Query OK, 1 row affected (0.00 sec)

mysql> insert into quotalimits values ('muff','user','false','hard','0','0','0','0','0','0');
 Query OK, 1 row affected (0.00 sec)
```

Если пользователь виртуальный, то его файлы все равно должны кому-то принадлежать.
Пусть это будет пользователь ftp групы ftp:

```
# cat /etc/passwd | grep ftp
 ftp:*:1003:14:User &:/nonexistent:/sbin/nologin
```

Добавим виртуального пользователя **virtual** и зададим ограничение для этого пользователя в 150 МБ (квоту необходимо указывать в байтах). Для этого выполним такие SQL-запросы:

```
mysql> use proftpd;
 Database changed

mysql> insert into users values
(NULL,'virtual',ENCRYPT('virtual_pass'),'1003','14','/var/vftp/virtual','/sbin/nologin');
 Query OK, 1 row affected (0.00 sec)

mysql> insert into quotalimits values
('virtual','user','false','hard','157286400','0','0','0','0','0');
 Query OK, 1 row affected (0.00 sec)
```

Следует обратить внимание на тот факт, что для виртуальных пользователей можно использовать любой каталог. Я вот решил использовать каталог **/var/vftp**. Необходимо создать каталог **/var/vftp**, и, соответственно, подкаталог **/var/vftp/virtual**, который будет являться домашним каталогом FTP для пользователя virtual:

```
# mkdir -p /var/vftp/virtual
```

Чтобы не возникало проблем с правами доступа, установим владельцем пользователя ftp:

```
# chown -R ftp:ftp /var/vftp/virtual
```

Создим каталог для логов:

```
# mkdir /var/log/proftpd
```

Добавим в /etc/rc.conf параметры запуска демона Proftpd:

```
# echo '# FTP' >> /etc/rc.conf
 # echo 'proftpd_enable="YES"' >> /etc/rc.conf
```

???????? ????????? FTP-??????:

```
# sh /usr/local/etc/rc.d/proftpd start

Starting proftpd.
```

Сервер запустился...

Перед тем, как проверять результаты работы, комментарии к таблицам MySQL:

Таблица users

- **username**: имя виртуального пользователя
- **passwd**: пароль в шифрованом виде

- **uid**: uid пользователя, которому принадлежат файлы
- **gid**: соответственно, gid пользователя, которому принадлежат файлы
- **homedir**: chroot директория пользователя
- **shell**: shell, выдаваемый пользователю. Рекомендую использовать /sbin/nologin

Таблица quotalimits

- **name**: имя виртуального пользователя
- **quota_type**: тип ограничения по (user,qroup,class или all - для всех)
- **per_session**: ***true*** - использовать квоту только на текущую сессию, в этом случае ни куда не записывается размер использованной квоты и для каждой новой сессии используется указанная квота. ***false*** - в этом случае использование квоты заносится в базу данных.
- **limit_type**: ***soft*** - возможно некоторое превышение квоты. ***hard*** - жестко заданная квота, превышение невозможно
- **bytes_in_avail**: лимит загрузки в байтах (если 150 Мб то 157286400 байт), 0 = нет лемита
- **bytes_out_avail**: лимит скачивания в байтах. 0 = нет лимита
- **bytes_xfer_avail**: Лимит передачи в байтах.0 = нет лимита
- **files_in_avail**: Лимит количества загружаемых файлов. 0 = нет лимита
- **files_out_avail**: Лимит количесва скачиваемых файлов. 0 = нет лимита
- **files_xfer_avail**: Лимит количесва передачи файлов. 0 = нет лимита

Таблицу ***quotatallies*** редактировать не нужно, proftpd это делает сам.

Итак, логинимся к серверу и проверяем квотирование:

```
# telnet localhost 21
Trying ::1...Trying 127.0.0.1...Connected to localhost.Escape character is '^]'.220
ProFTPD 1.3.3a Server (Company_name FTP server) [127.0.0.1]USER virtual
331 ????????? ?????? ??? ??????????? virtualPASS virtual_pass
230 Now upload/download filesSITE QUOTA
200-The current quota for this session are [current/limit]: Name: virtual Quota Type
: User Per Session: False Limit Type: Hard   Uploaded Mb:         0.00/150.00   Down
loaded Mb:       unlimited   Transferred Mb:      unlimited   Uploaded files:      u
nlimited   Downloaded files:    unlimited   Transferred files:   unlimited200 Please
 contact admin [at] domain [dot] com if these entries are inaccurate
```

Закачаем некоторый обьем информации, и проверим квоту:

```
SITE QUOTA
200-The current quota for this session are [current/limit]:Name: virtualQuota Type:
UserPer Session: FalseLimit Type: Hard   Uploaded Mb:         16.34/150.00   Downloa
ded Mb:       unlimited   Transferred Mb:      unlimited   Uploaded files:      unli
mited   Downloaded files:    unlimited   Transferred files:   unlimited200 Please co
ntact admin [at] domain [dot] com if these entries are inaccurate
```

При превышении квоты закачка прерывается и наблюдаем такие сообщения FTP-сервера:

```
552-Передача отменена. Disc quota exceeded
STOR: notice: quota reached: used 150.00 of 150.00 upload Mb
```

На этом можно считать настройку оконченой.

Источник (получено *2026-11-07 18:00*):
http://muff.kiev.ua/content/proftpd-s-khraneniem-spiska-polzovatelei-v-mysql-i-podderzhkoi-kvotirovaniya