Proftp

Intro: The server proftpd and its configuration below can be used for:

- anonymous ftp
  - name is `anonymous` or `ftp` and password can be anything
  - the client is limited (chroot) to the directory `/usr/local/ftp`

- Normal system ftp user
  - users are from the group `users`
  - login name uses normal *system user* and *password*
  - the user is free to move through the entire system

- Web client ftp user
  - users are from the group `www`
  - login name uses normal *system user* and *password*
  - the user is restricted (chroot) to his home directory web page area
    eg. `~/public_html`

Configuration file: `/etc/proftpd.conf`

Notes:

- Contrary to the `wu.ftpd` the `proftpd` does not need to have the directories `/lib` and `/bin` to work on normal (long) directory listings.
- If you want users to login with ftp but not with telnet or ssh then:
  - Make sure that the shell of the concerned users is set to `/bin/false` (in `/etc/passwd`)
  - Make sue that the shell /bin/false is listed in the file `/etc/shells`.

sample of `/etc/proftpd.conf`

```
# This is a basic ProFTPD configuration file. It establishes a single
# server and a single anonymous login. It assumes that you have a
# user/group "nobody"/"nogroup" for normal operation and anon.

#    !!! PLEASE read the documentation of proftpd !!!
#
# You can find the documentation in /usr/doc/packages/proftpd/,
# http://www.proftpd.org/ and don't forget to read carefully
# and _follow_ hints on http://www.proftpd.net/security.html.

ServerName              "powered by SuSE Linux"
ServerType              inetd
ServerAdmin             ftpadm@localhost
#
# uncomment, if you want to hide the servers name:
#
ServerIdent             on    "Michel's Laptop FTP Server ready"
DeferWelcome                  off
DefaultServer                 on

# Enable PAM for authentication...
#
AuthPAM                       on
```

```
# Setting this directive to on will cause authentication to fail
# if PAM authentication fails. The default setting, off, allows
# other modules and directives such as AuthUserFile and friends
# to authenticate users.
#
#AuthPAMAuthoritative        off

# This directive allows you to specify the PAM service name used
# in authentication (default is "proftpd" on SuSE Linux).
# You have to setup the service in the /etc/pam.d/<other_name>.
#
AuthPAMConfig                proftpd

# Port 21 is the standard FTP port.
Port                    21

# disable listen on 0.0.0.0:21 - the port (and IP) should
# be specified explicitly in each VirtualHost definition
#
#Port                           0

# listen for each (additional) address explicitly that is
# specified (via Bind and Port) in a VirtualHost definition
#
#SocketBindTight                        on


# Umask 022 is a good standard umask to prevent new dirs
# and files from being group and world writable.
Umask                   022

# Set the user and group that the server normally runs at.
User                    nobody
Group                   nogroup

# Normally, we want files to be overwriteable.
<Directory /*>
  AllowOverwrite        on
  HiddenStor                  on
  #HideNoAccess               on
</Directory>

# protect .ftpaccess and similar - see also PathDenyFilter
#<Directory /*.ftp*>
#  <Limit ALL>
#    DenyAll
#    IgnoreHidden       on
#  </Limit>
#</Directory>

# It is a very good idea to allow only filenames containing normal
# alphanumeric characters for uploads (and not shell code...)
#PathAllowFilter "^[a-zA-Z0-9_.-]+$"
#PathAllowFilter "^[a-zA-Z0-9~ \*\/,_.-]+$"

# We don't want .ftpaccess or .htaccess files to be uploaded
#PathDenyFilter "(\.ftp)|(\.ht)[a-z]+$"
#PathDenyFilter "\.ftp[a-z]+$"

# Do not allow to pass printf-Formats (security! see documentation!):
#AllowFilter "^[a-zA-Z0-9@~' \*\/,_.-]*$"
DenyFilter  "%"

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
```

```
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances                    30

# Performance: skip DNS resolution when we process the logs...
#UseReverseDNS        off

# Turn off Ident lookups
IdentLookups         off
# Set the maximum number of seconds a data connection is allowed
# to "stall" before being aborted.
#TimeoutStalled                  300

# Where do we put the pid files?
ScoreboardPath       /var/run/proftpd

# Logging options
#
TransferLog          /var/log/xferlog

# Some logging formats
#
#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"

# Log file/dir access
#ExtendedLog          /var/log/proftpd.access_log    WRITE,READ write

# Record all logins
#ExtendedLog          /var/log/proftpd.auth_log      AUTH auth

# Paranoia logging level....
##ExtendedLog          /var/log/proftpd.paranoid_log  ALL default

# Do a chroot for web-users (i.e. public or www group), but
# do not change root if the user is also in the users group...
#
DefaultRoot ~/public_html     www
DefaultRoot ~                 ftpuser

# Limit login attempts
#MaxLoginAttempts                3

# Users needs a valid shell
#RequireValidShell               yes

# Use special Auth files instead....
#AuthUserFile                    /var/proftpd/authfiles/passwd
#AuthGroupFile                   /var/proftpd/authfiles/group

# Use LDAP server - see README.LDAP
#
#LDAPServer         "localhost"
#LDAPPrefix         "dc=your,dc=domain,dc=top"
#LDAPDN             "cn=YourDNUser,dc=your,dc=domain,dc=top"
#LDAPDNPass         "YourDNUserPassword"

# The ratio directives take four numbers: file ratio, initial file
# credit, byte ratio, and initial byte credit.  Setting either ratio
# to 0 disables that check.
#
# The directives are HostRatio (matches FQDN -- wildcards are allowed
# in this one), AnonRatio (matches password entered in an anon login,
# usually an email address), UserRatio (accepts "*" for 'any user'),
```

```
# and GroupRatio.  Matches are looked for in that order.
# Some examples:
#
# Ratios     on                                    # enable module
# UserRatio  ftp 0 0 0 0
# HostRatio  anyhost.domain.top 0 0 0 0            # leech access (default)
# GroupRatio proftpd 100 10 5 100000               # 100:1 files, 10 file cred
# AnonRatio  auser@domain.top 1 0 1 0              # 1:1 ratio, no credits
# UserRatio  * 5 5 5 50000                         # special default case

# Setting "Ratios on" without configuring anything else will enable
# leech mode: it logs activity and sends status messages to the ftp
# client, but doesn't restrict traffic.
```

Anonymous FTP

```
<Anonymous ~ftp>
      # Using '~ftp' the client will land in the home directory of ftp user.
      # just the same as in Apache (http://myserver.com/~username)

     # After anonymous login, daemon runs as:
     User               ftp
     Group              daemon

     # We want clients to be able to login with "anonymous" as well as "ftp"
     UserAlias          anonymous ftp

     # Limit the maximum number of anonymous logins
     MaxClients         10

     # We want 'welcome.msg' displayed at login, and '.message' displayed
     # in each newly chdired directory.
     DisplayLogin       msgs/welcome.msg
     DisplayFirstChdir        .message

     # Deny write operations to all directories, underneath root-dir
     # Default is to allow, so we don't need a <Limit> for read operations.
     <Directory *>
          <Limit WRITE>
               DenyAll
          </Limit>
     </Directory>
     #
     # Only uploads into incomming directory are allowed...
     #<Directory incoming>
     #
     #     Umask  017
     #
     #     # ... so deny read/write
     #     <Limit READ WRITE DIRS>
     #          DenyAll
     #     </Limit>
     #
     #     # ... allow file storing, but not other writes
     #     <Limit STOR CWD CDUP>
     #          AllowAll
     #     </Limit>
     #
     #</Directory>

</Anonymous>
```