FTP Setup Tips

Will Harris, wil@redhat.com
Vertaler: Reggy Ekkebus, reggy@zeelandnet.nl
v1.1, 20 april 1999.

Inhoudsopgave

1 Inleiding

"Red Hat Tipsïs documentatie die bedoeld is om Red Hat gebruikers te helpen met bepaalde taken. Enkele van deze documenten zijn voor beginnende gebruikers, andere zijn voor gevorderde gebruikers. Als je een bijdrage wilt leveren, zend die dan naar tech-sup@redhat.com. Als je veranderingen hebt voor een individueel Tips document, zend die dan naar de auteur van dat document.

2 Introductie

Dit document beschrijft de configuratie voor wu-ftpd en proftpd voor gewone gebruikers en anonieme gebruikers. Je moet root zijn voor dit gehele proces.

Het eerste deel gaat over het instellen van wu-ftpd en anonieme ftp. Het tweede deel gaat over het instellen van proftpd.

3 Voorbereiding

Installeer de NetKit-B en anonftp RPM's. NetKit-B heeft de FTP server daemon; anonftp heeft de binaries, libraries en dingen die in de FTP directory gaan.

/home/ftp is de root directory van je FTP server. Anonftp zet het meeste voor je op, maar er zijn nog een paar dingen die je zelf moet doen.

Je moet een kopie van /etc/passwd en /etc/group in /home/ftp/etc zetten, zodat het /ls commando de gebruikersnamen en groepnamen ook weergeeft. Voor de veiligheid van je systeem moet je de gecodeerde wachtwoorden vervangen door sterretjes. Om /etc/passwd naar /home/ftp/etc/passwd te kopieëren en de wachtwoorden te vervangen door sterretjes, gebruik je dit commando:

```
sed -e 's/:[^:]*:/:*:/' /etc/passwd >~ftp/etc/passwd
```

In /etc/group staan onder Red Hat Linux geen wachtwoorden, dus deze kun je gewoon kopieëren:

```
cp /etc/group ~ftp/etc/group
```

Een andere optie (en een goed idee voor veiligheid) is het gebruik van shadow passwords. Onder linux kun je dit doen door simpelweg het volgende uit te voeren:

```
pwconv
```

Dit commando converteert het password bestand naar shadow, vernieuwt de pam libs om shadow passwords te gebruiken en een permissie te zetten op /etc/shadow. Als je dit doet, dan kun je gewoon de bestanden /etc/passwd en /etc/group kopieëren:

```
cp /etc/passwd /etc/group ~ftp/etc/
```

Dat is dat, kijk het voor de zekerheid nog even na voor je verder gaat.

Notitie: De enige regels die we eigenlijk nu nodig hebben zijn die van de root.

4 Beveiligen

De anonftp RPM plaatst enkele binaries en libraries in de /home/ftp directory om Ftp gebruikers dingen te laten doen zoals: automatisch bestanden unzippen als ze worden opgehaald of het ophalen van een hele directory met tar bestanden. Er zijn een paar extra bestanden geplaatst door de anonftp RPM die bijna nooit gebruikt worden en die moeten worden verwijderd om de veiligheid te bevorderen.

```
cd /home/ftp/bin
rm cpio sh zcat
cd ../etc
rm ld.so.cache
cd ../lib
rm ld.so* libtermcap*
```

Tot slot moet je de permissies van bestanden veranderen om de veiligheid te bevorderen.

```
chmod 111 ~ftp/bin/* ~ftp/bin ~ftp/etc ~ftp/lib
chmod 444 ~ftp/etc/*
chmod 555 ~ftp ~ftp/lib/*
```

Als je klaar bent moet je het volgende hebben:

```
bin:
total 164
---x--x--x   1 root     root        14776 Oct 31 09:54 compress
---x--x--x   1 root     root        45277 Oct 29 21:59 gzip
---x--x--x   1 root     root        22977 Oct 29 20:07 ls
---x--x--x   1 root     root        77873 Oct 25 17:49 tar
```

```
etc:
total 2
-r--r--r--   1 root     root          495 Mar 20 19:46 group
-r--r--r--   1 root     root          921 Mar 20 19:45 passwd

lib:
total 702
-r-xr-xr-x   1 root     root        20994 Oct 30 18:58 ld-linux.so.1
-r-xr-xr-x   1 root     root        20994 Oct 30 18:58 ld-linux.so.1.7.5
lrwxrwxrwx   1 root     root           13 Mar 20 19:43 libc.so.5 -> libc.so.5.0.9
-r-xr-xr-x   1 root     root       669157 Oct 30 19:53 libc.so.5.0.9
```

Als er bestanden ontbreken, begin dan opnieuw en herinstalleer de anonftp RPM. Om de permissies te zien als hierboven typ:

```
ls -al
```

Nu alles veilig is moet je de `/pub` directory aanmaken waar je de bestanden zet voor de anonieme ftp.

```
mkdir ~ftp/pub
chmod 555 ~ftp/pub
```

Plaats elk bestand dat je wilt aanbieden via FTP in de `/pub` directory. Je mag ook subdirectory's aanmaken in de `/pub` directory.

Voor de veiligheid en om zeker te weten dat anonieme gebruikers ook de bestanden kunnen lezen, doe dan dit met elk bestand en elke directory:

```
chmod 444 (naam van het bestand)
chmod 555 (naam van de directory)
```

Een 'incoming' directory is af te raden, omdat je dan last kunt hebben van software piraterij. Sommige mensen zetten dan software op je site, waar je voor moet betalen en de houder van de site krijgt dan een bekeuring, omdat die verantwoordelijk is voor de dingen die op de site staan. Als het echt nodig is doe dan dit:

```
mkdir ~ftp/incoming
chmod 333 incoming
```

De mode 333 betekent dat ze alleen in de directory kunnen schrijven en niet lezen.

Dat was het! Voor de veiligheid: zorg dat alles in `/home/ftp` niet te schrijven is.

```
chmod -R a-w ~ftp
```

(Je mag als root nog wel in de directory schrijven).

5 ProFTPd Setup

OK, voor degenen die ProFTPd willen: eerst kijken of je de nieuwste versie hebt.

ProFTPd <ftp://ftp.proftpd.org>

voor de RPM (Opmerking: Deze worden niet onderhouden door RedHat Software).

ProFTPd RPM <ftp://rhcn.redhat.com/pub/rhcn/RPMS/>

Als je het pakket eenmaal gedownload en geïnstalleerd hebt via een van de methoden.

(Onthoud: Om proftpd te installeren via rpm moet je de wu-ftpd en anonftp wegdoen.) Je moet het configuratiebestand aanpassen voor je site. Als je de RHCN rpm gebruikte, staat het configuratiebestand in `/etc/proftpd.conf`. Als je hem zelf gecompileerd hebt, staat het configuratiebestand in: `/usr/local/etc/proftpd.conf`.

Nu voor de configuratie: open het configuratiebestand met een editor naar keuze. Het bestand ziet er ongeveer uit als hieronder:

```
# This is a basic ProFTPD configuration file (rename it to
# 'proftpd.conf' for actual use.  It establishes a single server
# and a single anonymous login.  It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.

ServerName                      "ProFTPD Default Installation"
ServerType                      standalone
DefaultServer                   on

# Port 21 is the standard FTP port.
Port                            21
# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
Umask                           022

# 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

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

# Normaal gesproken willen we dat bestanden overschrijfbaar zijn.
<Directory /*>
  AllowOverwrite                on
</Directory>

# A basic anonymous configuration, no upload directory's.
<Anonymous ~ftp>
User                          ftp
Group                         ftp
# We want clients to be able to login with "anonymous" as well as "ftp"
UserAlias                     anonymous ftp

# Beperk het aantal anonieme logins
MaxClients                    10

# We want 'welcome.msg' displayed at login, and '.message' displayed
```

```
# in each newly chdired directory.
DisplayLogin                   welcome.msg
DisplayFirstChdir              .message

# Limit WRITE everywhere in the anonymous chroot
<Limit WRITE>
   DenyAll
</Limit>

</Anonymous>
```

Het eerste wat we doen is onze server configureren voor onze eigen site. We beginnen met de volgende regel:

```
ServerName                              "ProFTPD Default Installation"
```

Verander het in een zelfgekozen server naam. Bijvoorbeeld "Reggy's Ftpsite". Dan zal het er zo uitzien:

```
ServerName                               "Reggy's Ftpsite""
```

Daarna gaan we kijken welk servertype we nemen. Je kunt kiezen tussen een die altijd draait of een net als de inetd deamon, dat betekent dat de server start en stopt als de connecties komen en gaan. inetd heeft mijn voorkeur, dus ik verander het en dan ziet het er zo uit:

```
ServerType                       inetd
```

Onthoud: Als je het wilt starten met inetd dan moet je ook een regel aanmaken in `/etc/inetd.conf`:

```
ftp     stream  tcp     nowait  root    /usr/sbin/proftpd       proftpd
```

Voor stand alone moet je jezelf hier niet druk over maken. Je moet niets veranderen aan de Port en Umask, het mag wel. Ik laat de User nobody en verander de group ook in nobody. Dus dit gaat er zo uitzien:

```
User                             nobody
Group                            nobody
```

Nu moet je een beslissing nemen over de bestanden. Ik vind het niet leuk dat bestanden overschrijfbaar zijn, dus ik verander het in:

```
<Directory /*>
  AllowOverwrite                 off
</Directory>
```

De setup voor anonymous laat ik met rust. Dit staat standaard aan, zonder dat ze kunnen schrijven.Er zijn nog veel meer andere opties voor ProFTPd. Kijk in de overige documentatie voor meer opties.

6 Overige documentatie

Zie Garfinkel en Spafford, "Practical Unix Security" *O'Reilly and Associates.* <http://www.oreilly.com>, 1996, pagina's 487-494 voor meer info. En

wu-FTPd <http://www.landfield.com/wu-ftpd/>

ProFTPd <http://www.proftpd.org/>

7 Copyright Gegevens