Very Secure FTP Server (vsftpd)

Autor: Tomasz Stala [tomek(at)zso.tbg.net.pl]
Napisano: 20.03.2004 r.
Wersja: 1.2 (poprawiona)

Spis treści:

1. Czym jest vsftpd ?

"vsftpd - probably the most secure and fastest FTP server for UNIX-like systems"

Jest to prawdopodobnie najbezpieczniejszy i najszybszy UNIX'owy serwer FTP. Jego zaletami są m.in. prostota konfiguracji (bardzo szybko możemy postawić bardzo wydajny i bezpieczny serwer FTP), szybkość (transfer jest o wiele większy niż w przypadku innych serwerów ftp). Dodatkowo warto wspomnieć, że w jego kodzie nie znaleziono "błędów krytycznych". Używany jest m.in. na serwerach ftp.redhat.com, ftp.openbsd.org, ftp.suse.com, ftp.ximian.com, ftp.kde.org, ftp.debian.org, ftp.gnome.org, ftp.gnu.org i inne, co potwierdza tezę, że vsftpd jest zaufanym i dojrzałym narzędziem. Sama nazwa mówi za siebie - "vs" jest skrótem od Very Secure. Jeżli chcesz mieć bezpieczny, wydajny i stabilny serwer FTP, powiniene. spróbować vsftpd. Opisana tu instalacja i konfiguracja tyczy się systemu FreeBSD, ale jest bardzo podobna w przypadku innych UNIX'owych systemów.

2. Instalacja

Proponowałbym zaopatrzenie się w najnowszą wersję źródeł demona, którą powinieneś znaleźć na stronie http://vsftpd.beasts.org/. Możesz także użyć do jego instalacji portów, wydajemy więc poniższe polecenia:

```
# cd /usr/ports/ftp/vsftpd
# make build && make install && make clean
```

Gdy vsftpd zainstalował się bez żadnych problemów, to możemy teraz przejść do jego konfiguracji, przed tym jednak sprawdź jeszcze czy nie masz już uruchomionego jakiegoś innego serwera FTP, jeżeli tak - wyłącz go.

Wypadało by też utworzyć nowego użytkownika oraz grupę, aby serwer nie był uruchamiany z poziomu root'a (ze względu na bezpieczeństwo). Wydajemy więc następujące polecenia:

```
# pw groupadd -g 75 -n ftp
# pw useradd -u 75 -g ftp -c "FTP Service" -d /home/ftp -m -s /sbin/nologin -n ftp
```

Będziemy też potrzebować pustego katalogu, do którego użytkownik `ftp` nie będzie miał prawa dostępu. Do czego on się przyda opiszę poniżej. Niech tym katalogiem będzie /var/chroot/vsftpd. Aby utworzyć ten katalog wydajemy następujące polecenie:

```
# mkdir /var/chroot/vsftpd/
```

Po wykonaniu powyższych czynności możemy przejść do konfiguracji, która jak już opisałem wcześniej jest bardzo prosta.

3. Konfiguracja

Format, w jakim są zapisywane opcje konfiguracyjne wygląda następująco:

```
opcja=wartość
```

Zauważ, że nie ma spacji pomiędzy znakiem `=`, a nazwą opcji oraz wartością. Takiej koncepcji należy się trzymać przy konfigurowaniu vsftpd.

Aby wszystko w naszym systemie było w miarę uporządkowane, proponuję już na początku utworzyć katalog `vsftpd`, w którym będą znajdować się wszystkie potrzebne nam pliki konfiguracyjne (tj. userlisty, bannery) o tym w dalszej części artykułu. Narazie zajmiemy się konfiguracją. Edytujmy więc plik vsftpd.conf. (np. edytorem VI):

```
# mkdir /usr/local/etc/vsftpd
# vi /usr/local/etc/vsftpd.conf
```

Rozdział ten podzieliłem na 2 podrozdziały, w których opiszę kolejno serwer do zastosowań "domowych" oraz serwer dla anonimowych użytkowników".

3.1. Podstawowa konfiguracja

Poniżej został przedstawiony plik zawierający podstawową konfigurację vsftpd, ze względów bezpieczeństwa serwera zabronimy użytkownikom poruszania się po całym systemie. Inaczej mówiąc ograniczymy możliwość poruszania się do jego katalogu domowego. Oto przykładowa zawartość takiego pliku:

```
--- vsftpd.conf ---

# Ustawiamy tutaj, z poziomu jakiego użytkownika ma być uruchamiany nasz serwer:
nopriv_user=ftp

# Uruchomienie serwera w trybie standalone. Jeśli chcemy aby nasz vsftpd był
# uruchamiany w trybie inetd, rezygnujemy z tej opcji, ponieważ domyślnie jest
# ona ustawiona na "NO":
listen=YES

# Definiujemy, tutaj na jakim porcie ma nasłuchiwać serwer (domyślnie jest to port 21):
listen_port=21

# Zabronienie logowania anonimowych użytkowników:
anonymous_enable=NO

# Zezwolenie logowania dla lokalnych użytkowników
local_enable=YES

# Pozwolenie do zapisu we własnym katalogu
write_enable=YES

# Umask (022 jest używany przez większość serwerów ftp)
local_umask=022

# Włączenie llogowania
xferlog_enable=YES

# ścieżka do pliku z logami
xferlog_file=/var/log/xferlog.log

# Logi w formacie xferlog (jest wykorzystywany m.in. przez wu-ftpd)
xferlog_std_format=YES

# Maksymalna liczba połączonych użytkowników
max_clients=5

# Maksymalna liczba użyktowników mogących się połączyć z tego samego adresu IP
max_per_ip=2

# Banner, który będzie wyświetlany przy każdym połączeniu z serwerem
ftpd_banner=Prywatny serwer FTP - Powered by: vsftpd

# Userzy nie mogą wychodzić poza swój katalog domowy
chroot_local_user=YES

# Ustawiamy katalog dla chroot'a:
secure_chroot_dir=/var/chroot/vsftpd

# Lista użytkowników, którzy mogą wychodzić poza swój katalog domowy,
# musisz utworzyć ten plik.
```

```
# np: touch /var/chroot/vsftpd/vsftpd.chroot_list
# Dodanie użytkownika odbywa się poprzez dopisanie nazwy usera do tego pliku.
# np: echo "tomek" >> /var/chroot/vsftpd/vsftpd.chroot_list
chroot_list_enable=YES
chroot_list_file=/var/chroot/vsftpd/vsftpd.chroot_list

--- end of vsftpd.conf ---
```

Zapisujemy ustawienia (ESC + :wq). Jeśli to nam na razie wystarczy, przechodzimy do kolejnego rozdziału dotyczącego uruchamiania vsftpd. Jeśli chcemy utworzyć drugi serwer, który będzie przeznaczony tylko i wyłącznie dla anonimowych użytkowników - czytamy dalej.

3.2. Konfiguracja ftp dla anonimowych użytkowników

Utworzymy sobie najpierw drugi plik konfiguracyjny, który będzie nosił nazwę np. `vsftpd2.conf`:

```
# touch /usr/local/etc/vsftpd/anonymous.conf
# vi /usr/local/etc/vsftpd/anonymous.conf
```

Następnie edytujemy go i ustawiamy w nim następujące opcje:

```
--- anonymous.conf ---
# Nazwa użytkownika, z pod którego będziemy uruchamiali vsftpd
nopriv_user=ftp

# Uruchamianie w trybie standalone
listen=YES

# Port, na którym będzie nasłuchiwał nasz anonimowy ftp
# (ustawiamy tą wartość według własnych potrzeb):
listen_port=2121

# Nazwa użytkownika, który będzie odpowiedzialny za obsługę anonimowego ftp
# Jego katalog domowy, będzie jednocześnie katalogiem domowym dla anonimowych użytkowników:
ftp_username=ftp

# Katalog dla chroot'a:
secure_chroot_dir=/var/chroot/vsftpd

# Zabraniamy logowanie na lokalnych użytkowników:
local_enable=NO

# Zezwalamy na logowanie się na anonimowego użytkownika (anonymous):
anonymous_enable=YES

# Serwer nie będzie pytał o hasło, podczas logowania na anonymous:
no_anon_password=YES

# Pozwalamy na download plików, które będą miały ustawione prawa do odczytu (readable):
anon_world_readable_only=YES

# Zabraniamy na upload plików:
anon_upload_enable=NO

# Ukrywamy prawdziwych użytkowników oraz grup dla plików lub katalogów
# (vsftpd zamieni je na nazwy użytkownika odpowiedzialnego za anonimowy ftp):
hide_ids=YES

# Ustawiamy komunikat powitalny:
ftpd_banner=Anonimowy serwer FTP - Powered by: vsftpd

# Logowanie w standardzie vsftpd:
xferlog_enable=YES
xferlog_std_format=NO
vsftpd_log_file=/var/log/vsftpd.log

--- end of anonymous.conf ---
```

Tak skonfigurowany serwer jest gotowy do uruchomienia, jak to zrobić opisane jest poniżej w kolejnym rozdziale. Oczywiście możesz powyższy przykład zmodyfikować według własnych upodobań. Jest jeszcze jedna ważna

rzecz, o której warto wspomnieć przy anonimowym serwerze ftp, mianowicie sprawa uploadu plików. Aby użytkownicy mogli wysyłać pliki na nasz serwer musimy utworzyć nowy katalog np. `upload` i nadać mu odpowiednie prawa do odczytu i zapisu. Katalog powinien znajdować się w katalogu domowym użytkownika ftp (odpowiadającego za anonimowy serwer ftp):

```
# mkdir /home/ftp/upload
# chown ftp:ftp /home/ftp/upload
```

Następnie do pliku anonymous.conf dodajemy lub modyfikujemy następujące opcje:

```
# Pozwolenie do zapisu w domowym katalogu:
write_enable=YES
# Zezwolenie do uploadu plików:
anon_upload_enable=YES
# Pozwolenie anonimowemu użytkownikowi do tworzenia nowych katalogów:
anon_mkdir_write_enable=YES
# Pozwolenie do modyfikacji plików/katalogów (nadpisywanie/kasowanie/zmiana nazwy):
anon_other_write_enable=YES
# Domyślny umask dla plików utworzonych przez użytkowników korzystających z anonimowego ftp:
anon_umask=022
```

Oczywiście korzystanie z powyższych opcji będzie możliwe jedynie w katalogu, który będzie zawierał odpowiednie prawa do zapisu w katalogu domowym użytkownika ftp.

Po zapoznaniu się i poprawnym skonfigurowaniu vsftpd zapraszam do przeczytania kolejnego rozdziału poświęconemu uruchamianiu tego demona.

4. Uruchamianie

Uruchamianie vsftpd jest bardzo proste. Są dwa sposoby na jego uruchomienie poprzez "odpalenie" go z poziomu inetd lub w trybie standalone. W drugim przypadku wystarczy wydać następujące polecenie i serwer uruchomi się "w tle":

```
# /usr/local/libexec/vsftpd &
```

Aby ułatwić sobie życie, proponowałbym napisać sobie mały skrypt startowy. Utwórzmy w katalogu /usr/local/etc/rc.d plik `vsftpd.sh`, następnie wstawmy do niego ten fragment:

```
#!/bin/sh

case $1 in
  start)

        /usr/local/libexec/vsftpd &
        echo -n "Uruchamianie vsftpd"
        ;;
  stop)
        killall vsftpd
        echo -n "Zatrzymanie vsftpd"
        ;;
  reload)
        killall vsftpd
          /usr/local/libexec/vsftpd &
        echo -n "Restartowanie vsftpd"
        ;;
  *)
        echo "Usage: $0 {start|stop}"
        exit 1
esac
```

Teraz korzystanie z tego skryptu jest bardzo proste. Mianowicie wystarczy wydać polecenia, odpowiednie do wykonywanych czynności (uruchamianie, zatrzymanie, restartowanie):

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

# /usr/local/etc/rc.d/vsftpd.sh stop
```

```
# /usr/local/etc/rc.d/vsftpd.sh reload
```

Powyższe czynności działają, gdy plik konfiguracyjny znajduje się w domyślnym katalogu, gdzie został zainstalowany (jest to /usr/local/etc/). Jeśli jednak "config" mamy w innym miejscu niż ten domyślny katalog musimy przy uruchamianiu vsftpd podać ścieżkę do tego pliku. Dla przykładu plik znajduje się w katalogu /root i nosi nazwę ftp.conf. W celu uruchomienia naszego serwera ftp wydajemy polecenie o następującej składni (/ścieżka/do/vsftpd/ /ścieżka/do/configu &):

```
# /usr/local/libexec/vsftpd /root/ftp.conf &
```

Podobnie możemy postąpić, gdy chcemy uruchomić więcej niż jeden serwer ftp na naszym serwerze. Musimy jednak pamiętać, że jeśli używamy jedno należy zmienić w każdym z plików konfiguracyjnych port używany przez vsftpd. Opcja odpowiadająca za to to `listen_port`. Jeśli posiadamy parę adresów IP i chcemy uruchomić vsftpd na każdym z tych adresów modyfikujemy jedynie opcję listen_address, we wszystkich plikach konfiguracyjnych. Więcej o tych opcjach przeczytaj w rozdziale "Pozostałe przydatne opcje przy konfiguracji". Przykładowo jeśli chcemy mieć 2 serwery ftp, a configami dla tych serwerów są pliki vsftpd1.conf oraz vsftpd2.conf znajdujące się w katalogu /usr/local/etc/vsftpd, po uprzedniej ich modyfikacji wydajemy następujące polecenia:

```
# /usr/local/libexec/vsftpd /usr/local/etc/vsftpd/ftp1.conf &
# /usr/local/libexec/vsftpd /usr/local/etc/vsftpd/ftp2.conf &
```

Drugim sposobem, jak już wspomniałem jest możliwość "odpalenia" vsftpd z poziomu inetd. Jeżeli już zdecydowaliśmy się skorzystać z tego sposobu, należy zrezygnować (usunąć lub zakomentować) opcję `listen`. W pliku konfiguracyjnym naszego ftp, ponieważ domyślnie jest ona ustawiona na "NO", lub jeśli nie chcesz usuwać tej opcji, możesz wpisać tam wartość "NO". Kolejnym krokiem jest dodanie następującej linijki do pliku /etc/inetd.conf:

```
ftp    stream  tcp     nowait  root    /usr/local/libexec/vsftpd vsftpd
```

Na koniec należy zrestartować proces inetd.

```
# kill -HUP `cat /var/run/inetd.pid`
```

Gdy mamy już uruchomiony serwer ftp, wypadało by sprawdzić, czy działa poprawnie. Możemy użyć do tego programu telnet, lub ftp, który powinien być dostępny w każdym systemie FreeBSD. Jeśli ujżymy komunikat powitalny, wszystko powinno działać poprawnie.

5. Pozostałe przydatne opcje przy konfiguracji

W rozdziale tym chciałem przedstawić inne przydatne opcje, które mogą się Ci przydać podczas konfigurowania vsftpd. Jest ich dużo, niestety mniej niż np. w proftpd, większość możecie znaleźć w manualu, który jest naprawdę obszerny (niestety w języku angielskim). Ja postaram się opisać tylko część z nich.

Opcja ta pokazuje informację o procesie systemowym vsftpd, inaczej mówiąc pokazuje co dany użytkownik robi po połączeniu się z naszym serwerem:

```
setproctitle_enable=YES
```

Za pomocą tej opcji (domyślnie jej wartość jest ustawiona na "NO") możemy sprawić, że użytkownik zamiast numerów PID i GID, będzie widział tekstowe nazwy użytkownika oraz grupy zarządzającymi danym plikiem lub katalogiem:

```
text_userdb_names=YES
```

Czas wyrażony w sekundach, definiujący to, ile użytkownik może być w bezczynności (idle) - standardowo (300 s):

```
idle_session_timeout=300
```

Opcja odpowiadająca za tzw. banner, czyli komunikat, który będzie wyświetlany podczas każdego połączenia z naszym serwerem, działa ona podobnie jak opisana powyżej opcja ftpd_banner, z tym, że tutaj tworzymy osobny

plik do takiego bannera i możemy wstawić dłuższy komunikat (domyślnie ustawiamy tu ścieżkę do tego pliku, po uprzednim jego utworzeniu):

```
banner_file=/usr/local/etc/vsftpd/banner
```

Definiujemy nazwę pliku, który podobnie jak w opcjach ftpd_banner oraz banner_file będzie wyświetlał komunikat powitalny, tyle że najpierw musi on się poprawie zalogować. Plik ten (.message) należy utworzyć w katalogu głównym użytkownika:

```
message_file=.message
```

Definiujemy tutaj nawy katalogów lub rozszeżenia do plików, które będą widoczne, ale nie będzie możliwości na manipulowanie nimi (zmianę nazwy, pobieranie ich z serwera, kopiowanie itd.). Przykładowo, chcemy aby dany użytkownik nie miał dostępu do katalogu files/ i nie mógł nic w nim zmieniać, a także aby nie mógł nic zrobić z plikami z rozszeżeniem *.mp3 oraz *.avi, rozszeżenia te umieszczamy w klamrach i oddzielamy je przecinkami:

```
deny_file={*.mp3,files/,*.avi}
```

Opcją tą możemy ukryć nazwy katalogów / plików, podobnie jak zostało opisane powyżej nazwy rozszeżeń plików lub nazwy katalogów umieszczamy pomiędzy dwoma klamrami i oddzielamy je przecinkami, przykładowo chcemy ukryć przed użytkownikiem wszystkie pliki, które będą miały rozszeżenie *.doc:

```
hide_file={*.doc}
```

Te dwie opcje odpowiadają za listę użytkowników, którzy nie będą mieli pozwolenia na logowanie do serwera, po wpisaniu nazwy użytkownika, który będzie znajdował się na tej liście podczas logowania pojawi się komunikat 'Permission denied.'. Nazwy tych użytkowników możemy dopisywać poprzez użycie komendy echo, lub poprostu edytując ten plik i wpisując jedną pod drugą:

```
userlist_enable=YES
userlist_file=/usr/local/etc/vsftpd/userlist
```

W opcji tej ustawiamy adres ip, na którym vsftpd ma nasłuchiwać. Przydatna jeśli chcemy uruchomić większą liczbę serwerów na jednym komputerze. Oczywiście jeśli mamy odpowiednią ilość adresów ip.

```
listen_address=111.222.333.444
```

Logowanie będzie odbywać się, tylko w tedy gdy w pliku konfiguracyjnym vsftpd ustawimy wartość "YES" przy opcji `xferlog_enable`:

```
xferlog_enable=YES
```

vsftpd obsługuje logowanie w dwóch standardach, pierwszym z nich jest xferlog , wykorzystywany przez wiele analizerów, oraz drugi o wiele czytelniejszy i przyjemniejszy standard vsftpd. Możliwe jest także korzystanie z tych dwóch standardów na raz. Służy do tego opcja `dual_log_enable`, jeśli zdecydowałeś się na to, powinieneś przy tej opcji ustawić wartość "YES":

```
dual_log_enable=YES
```

W przypadku, gdy chcemy skorzystać z pierwszego opisanego przezemnie standardu, powinniśmy do pliku konfiguracyjnego dopisać takie oto opcje:

```
xferlog_std_format=YES
xferlog_file=/var/log/xferlog.log
```

Jeśli jednak chcemy skorzystać z drugiego ze standardów do tego pliku dopisujemy następujące linijki:

```
xferlog_std_format=NO
vsftpd_log_file=/var/log/vsftpd.log
```

Ciekawą opcją jest także `user_config_dir`, która pozwala przyporządkować dowolnemu użytkownikowi w systemie konkretne opcje. Mogą to być np. takie opcje jak listen_address, banner_file, max_per_ip, max_clients, xferlog_file, vsftpd_log_file, itp. Definiujemy więc ścieżkę do takiego katalogu, oraz tworzymy go w systemie. Po

zdefiniowaniu tej opcji w pliku konfiguracyjnym, vsftpd będzie automatycznie szukał pliku, który nosi taką samą nazwę jak użytkownik systemowy. Na przykład dla użytkownika `tomek` takim plikiem będzie /usr/local/etc/vsftpd/user_conf/tomek, w tym właśnie pliku będziemy ustawiać konkretne opcje dla tego użytkownika.

```
user_config_dir=/usr/local/etc/vsftpd/user_conf/
```

6. Na koniec

Niniejszy artykuł dedykuję mojej Wspaniałej i Kochanej Anusi! Za błędy wynikające z mojej strony z góry przepraszam. Życzę miłego korzystania z vsftpd, który mimo, że nie jest tak rozbudowanym serwerem jak np. proftpd, zasługuje na duże uznanie. Myślę, że zdobędzie także dobrą opinię u Ciebie. Oryginalna oraz najnowsza wersja tego artykułu znajduje się na stronie http://zso.tbg.net.pl/~tomek/vsftpd_howto.html. Jeśli chcesz umieścić ten artykuł na swojej stronie, skontaktuj się ze mną poprzez e-mail - tomek(at)zso.tbg.net.pl, podając w nim adres strony, na której będzie się on znajdował. Jedynym ważnym warunkiem, jaki musisz spełnić, jest zamieszczenie tego dokumentu w całości (ma on być zgodny z oryginałem), oraz w miarę możliwości jego aktualizacja, po ukazaniu się najnowszej jego wersji w sieci.

```
$Id: vsftpd_howto.html,v 1.2 2004/06/08 21:55:19 tomek Exp $
```