

Příklad konfigurace vsftpd

Vložil/a [cm3l1k1](#) [1], 2 Srpen, 2005 - 13:53

- [Apple](#) [2]
- [Networks & Protocols](#) [3]
- [Recenze](#) [4]
- [Security](#) [5]

VSFTPD (Very Secure File Transfer Protocol Daemon) je malý FTP server. Jedná se však o nejrychlejší a nejbezpečnější server napsaný světoznámým Chrisem Evansem.

Vsftpd je nenáročný a lehce konfigurovatelný. Jeho hlavním zaměřením je především bezpečnost a to splňuje na jedničku. Sice neumí kvotování a virtuální uživatele z databáze, ale to není velká překážka. Navíc druhý bod je pravdivý z poloviny, protože virtuální uživatele lze vytvořit přes script z Berkeley DB. K tvorbě těchto uživatelů se ještě vrátíme.

V tomto článku vám chci ukázat svůj konfigurační soubor, který jsem sice psal pro verzi 1.2.2 (aktuální je 2.0.3), ale lze ho použít v aktuální. Přibyly pouze položky pro použití DSA a RSA šifrovacích klíčů u SSL komunikace (viz. man vsftpd).

Takže zde je slibovaný vsftpd.conf:

(virtuální uživatelé a podpora SSLka je zakomentovaná, nejdřív vsftpd prozkoumejte, vyzkoušejte a až pak si aktivujte spec. featury)

```
# vsftpd.conf 1.2.2 configuration [by cm3l1k1] also useable in 2.0.3
# mail: cm3l1k1[alt+64]security-portal.cz
#
# --// Standalone mode => ne via xinetd \--
listen=YES
listen_port=21
max_clients=200
max_per_ip=4
ftp_username=ftp
background=YES
#
# --// Access rights \--
# zakazeme anonym prihlasovani
anonymous_enable=NO
local_enable=YES
write_enable=NO
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
anon_world_readable_only=NO
# defaultni adresar pro anon usery
#anon_root=
#
# --// Security \--
local_umask=077
# pri anon uploadovani nebudem defaultne menit ownera
chown_uploads=NO
#chown_username=whoknow
anon_world_readable_only=NO
```

Příklad konfigurace vsftpd

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

```
connect_from_port_20=NO
# pri vypisu adresare bude owner a group zobrazen jako "ftp"
hide_ids=YES
pasv_min_port=50000
pasv_max_port=60000
# Uzivatel s nejmensima pravama v systemu, který bude
# vsftpd obcas pouzivat, defaultne nobody
nopriv_user=nobody
# uplne skryje, nebo znepristupni slozky/soubory
#hide_file=
#deny_file=
# chrootovana slozka, kterou bude vsftpd vyuzivat kdyz
# nebude vyžadovat FS pristup; zakazat pristup userovi "ftp"
secure_chroot_dir=/usr/share/empty
#
# --// Features \--
# bannerik
ftpd_banner=
# Tohle loguje upload/download souboru
xferlog_enable=YES
xferlog_std_format=NO
vsftpd_log_file=/var/log/vsftpd.log
# deaktivuje ls -R (to se bude hodit napr u arxivu)
ls_recurse_enable=NO
# zakazem ascii up/down k ochrane scriptu
ascii_upload_enable=NO
ascii_download_enable=NO
# nebudem rozlisovat ABOR requesty => vetsi bezpecnost
async_abor_enable=NO
# pro active mode conexe
#port_enable=NO
#
# --// Performance \--
one_process_model=NO
idle_session_timeout=20
data_connection_timeout=20
accept_timeout=60
connect_timeout=60
# maximalni prenosova rychlost v B/s pro
# local usery, 0=unlimited
local_max_rate=0
#
# --// SSL \--
# tady jde o to jestli duverujem OpenSSL knihovnam
# pac pak vetsina bezpecnosti lezi na nich, zatim #
#ssl_enable=YES
# povoluje preferovanej protokol TLS v1
#ssl_tlsv1=YES
# cesta k DSA klicum
#dsa_cert_file=
# cesta k RSA certifikatum
#rsa_cert_file=/usr/share/ssl/certs/vsftpd.pem
# povolene sifry (man ciphers)
#ssl_ciphers=DES-CBC3-SHA
#
# --// Virtualni useri \--
# howto: echo cm3l1k1 >> logins.txt | echo tajne >> logins.txt
# info: 1.radek login:cm3l1k1 2.radek pass:tajne
# howto: db_load -T -t hash -f logins.txt /etc/vsftpd_login.db
```

Příklad konfigurace vsftpd

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

```
# info: je nutny mit "Berkeley db" (<a href="http://www.sleepycat.com"
title="www.sleepycat.com">www.sleepycat.com</a>)
# howto: chmod 600 /etc/vsftpd_login.db
# info: nasledujici dva radky do souboru /etc/pam.d/ftp
# auth required /lib/security/pam_userdb.so db=/etc/vsftpd_login
# account required /lib/security/pam_userdb.so db=/etc/vsftpd_login
# howto: useradd -d /ftp/slozka virtual
# howto: chown virtual:virtual /ftp/slozka
# howto: mkdir /etc/vsftpd_user_config
# chrootne virtualni usery
chroot_local_user=YES
# aktivujeme virtualni usery
guest_enable=YES
# uzivatel pod kterym virtual useri pobezi
guest_username=virtual
# virtual useri nebudou mit stejny prava jako local
virtual_use_local_privs=NO
# pro kazdyho virtualniho usera se vytvori chrootovana
# slozka s jeho loginem /ftp/slozka/papa
#user_sub_token=
# slozka ve který budou soubory s login name
# useru /etc/vsftpd_user_config/papa
# v souborech budou definovany prava pro kazdyho
user_config_dir=/etc/vsftpd_user_config
# nazev PAM sluzby /etc/pam.d/xyz
pam_service_name=ftp
# Debug - pokud nejsou s ftp problemy tak nepouzivat
#log_ftp_protocol=YES
```

Pro většinu položek stačí moje stručná nápověda, takže vysvětlím pouze vybrané.

"max_per_ip=" - maximální počet aktuálních spojení z jedné IP adresy. Pokud jsou někteří uživatelé za NATkem tak bude nutné tuto hodnotu navýšit.

Virtuální uživatelé - doufám, že daný popis stačí. Rozchodit virtuální uživatele vám asi zabere nejvíce času a hned na poprvé se to ani nemusí podařit. Chce to zkoušet a nebo je nepoužívat a defaultně nechat uživatele z /etc/passwd.

Asi opravdu k tomu nemám co víc napsat. Všechno najdete v konfiguračním souboru a nebo v manualových stránkách. S instalací také není problém - standard: ./configure && make && make install. Pokud by bylo něco nejasné napiště mi do komentářů. Takže přeju hodně štěstí s bezproblémovostí vsftpd ;o]

Domovskou stránku naleznete na <http://vsftpd.beasts.org/> [6]

URL článku: <https://security-portal.cz/clanky/p%C5%99%C3%ADklad-konfigurace-vsftpd>

Odkazy:

[1] <https://security-portal.cz/users/cm3l1k1>

[2] <https://security-portal.cz/category/tagy/apple>

[3] <https://security-portal.cz/category/tagy/networks-protocols>

[4] <https://security-portal.cz/category/tagy/recenze>

[5] <https://security-portal.cz/category/tagy/security>

[6] <http://vsftpd.beasts.org/>