ASL Serwer FTP – „dokumentacja”

Usługa FTP (File Transfer Protocol) służy do przesyłania plików pomiędzy komputerami. Umożliwia pobieranie plików do lokalnego systemu plików oraz ich wysyłanie do odległego systemu plików. Pracuje w architekturze klient-serwer i bazuje na protokole połączeniowym TCP.

Przesyłanie plików możliwe jest dwoma sposobami: binarnie oraz w trybie ASCII. Pierwszym sposobem przesyłamy plik nie dokonując w nim żadnych zmian, za pomocą drugiego natomiast niektóre bity są kodowane innym systemem. Nie należy, więc przesyłać plików typowo binarnych (archiwów ZIP, plików wykonywalnych EXE) przy pomocy trybu ASCII, gdyż zmiany, jakie zostaną wprowadzone spowodują niemożność odczytania takiego pliku.

Dane przy pomocy FTP są przesyłane w dwóch trybach: zwykłym i anonimowym. Zwykły tryb, to tryb, w którym korzystamy z zasobów konta chronionego. Aby użyć tego trybu należy mieć odpowiednie uprawnienia(tzn. własne konto i hasło). Tryb anonimowy służy do korzystania z informacji na serwerach ogólnodostępnych.

Protokół FTP został zaprojektowany w początkowej fazie działania Internetu i cechuje się niskim poziomem bezpieczeństwa – hasło przesyłane jest otwartym tekstem. FTP jest usługą wieloplatformową dostępną na każdy system operacyjny.

Każdy plik na serwerze posiada swój własny adres URL w formacie ftp://<host>/<katalog>/<plik>. Do obsługi można używać klienta ftp lub przeglądarki internetowej.

FTP wymaga do działania portu służącego do przesyłania komunikatów oraz portu, przez który odbywać się będzie transfer danych. Może działać w dwóch trybach pracy: aktywnym i pasywnym.

Tryb aktywny polega na tym, że klient łączy się z portu >1023 na port 21 serwera i następnie serwer sam inicjuje połączenie przesyłania danych z portu 20 na port klienta >1023. Administratorzy przeważnie blokują ruch przychodzący i niemożliwe jest nawiązanie połączenia z zewnątrz sieci przez serwer FTP. W tym celu stworzono drugie rozwiązanie – tryb pasywny, w którym klient wysyła zapytanie do serwera FTP, który następnie otwiera port >1023 i informuje o tym klienta. Skutkuje to jednak większą podatnością serwera na ataki.

Do obsługi FTP stosowany jest program ftp. Przydatne komendy:

- **!** – wywołanie interaktywnej powłoki na lokalnym komputerze
- **open 1.2.3.4** – nawiązanie połączenia z serwerem FTP
- **close** – zakończenie sesji
- **cd [katalog]** – zmiana katalogu
- **pwd** – aktualny katalog
- **ascii** – tryb ascii przesyłania danych
- **binary** – tryb binarny przesyłania danych
- **ls [katalog], dir [katalog]**– wyświetlenie listy plików w katalogu
- **get zdalny [lokalny]** – pobranie pliku zdalny i zachowanie jako lokalny
- **put lokalny [zdalny] -** wysłanie pliku lokalny i zapisanie jako zdalny
- **mget plik1 plik2 plik3** – pobieranie wielu plików
- **mput plik1 plik2 plik3** – wysyłanie wielu plików
- **status** – pokazuje obecny stan ustawień
- **delete plik** – usuwa plik
- **mdelete plik1 plik2 plik3** – usunięcie wielu plików
- **help [polecenie] -** pomoc

Dla Linuksa istnieje wiele serwerów realizujących funkcję FTP:

- proftpd
- wu-ftpd
- pureftpd
- vsftpd
- …
-

ProFTPd - http://www.proftpd.org/

Jest to najbardziej popularny serwer FTP na Linuksa, wzorowany na serwerze HTTP Apache. Zawiera pliki konfiguracyjne z dyrektywami i grupami dyrektyw, wspiera pliki .ftaccess oraz wirtualne hosty. Posiada moduły rozszerzające jego funkcjonalność – standardowe oraz contrib. Serwer proftpd może pracować w jednym z dwóch trybów działania: inetd, standalone w zależności od jego obciążenia. Inetd stosowany jest przy małym ruchu i niskim poziomie zużycia zasobów. W tym trybie istnieje daemon odpowiedzialny za obsługę nadchodzących połączeń (połączenie=osobny proces). Tryb standalone przeznaczony jest do dedykowanych maszyn z dużym ruchem oraz obciążeniem. W tym trybie nie istnieje powoływanie procesów dla każdego nowego połączenia. Plik konfiguracyjny serwera znajduje się w /etc/proftpd.conf.

Instalacja
Instalacji możemy dokonać na kilka sposobów, najlepszym jest udanie się na stronę projektu ProFTPD (http://www.proftpd.org/) i ściągnięcie stamtąd programu. Pobrać program można np. z serwera ftp://ftp.proftpd.org/distrib/. W zależności od używanego systemu możemy ściągnąć odpowiednią wersje pakietową (rpm'y lub source rpm'y) – z katalogu packages/, lub wersje źródłowe (spakowane jako proftpd-****.tar.gz lub proftpd-****.tar.bz2) - katalog source/. W dystrybucjach Debian można użyć polecenia **apt-get install proftpd**

Po ściągnięciu tego pliku należy go rozpakować. Jeśli posługujemy się Midnight Commanderem to wystarczy wejść do pliku archiwum i skopiować jego zawartość w wybrane przez nas miejsce. Jeżeli nie mamy Midnight Commandera należy rozpakować archiwum komendą:
tar -xzvf proftpd-1.2.7rc3.tar.gz
co spowoduje rozpakowanie naszego archiwum do katalogu "proftpd-1.2.7rc3". Po wejściu do tego katalogu (komend_ cd <nazwa katalogu> o ile nie używamy MC) należy skompilować program.
Robimy to w następujący sposób wpisując polecenia:
./configure
make
make install
Spowodowało to zainstalowanie ProFTPD z domyślnymi opcjami, umieszczając pliki programu w następujących katalogach:
proftpd i ftpshut w katalogu "/usr/local/sbin/"
ftpcount i ftpwho w katalogu "/usr/local/bin/"

plik konfiguracyjny *proftpd.conf* w katalogu "/usr/local/etc/"
oraz pliki pomocy (manual) w katalogu "/usr/local/man/man?/"
Jeśli będziemy chcieli dodać jakieś moduły do programu to należy ponownie skompilować program,przy czym należy pamiętać, aby najpierw wyczyścić katalog instalacyjny (jeśli używamy tego samego katalogu w którym kompilowaliśmy po raz pierwszy) poleceniem make distclean.

Przed omówieniem podstawowej konfiguracji musimy sobie zadać pytanie: *"kogo ma obsługiwać nasz serwer plików i jakie zasoby udostępniać?"*
Mamy do wyboru:

- **użytkownicy systemowi** - użytkownicy mający dostęp do kont shell na naszym serwerze (zaufani)
- **użytkownicy ftp** - użytkownicy posiadający tylko dostęp do konta na ftp (mniej zaufani)
- **użytkownicy anonimowi** - użytkownicy posiadający dostęp to tzw.nonymous ftp, czyli przeważnie mogący ściągać pliki udostępnione przez administratora bez podawania loginu ani hasła

Tworzenie użykowników realizujemy za pomocą narzędzia **ftpasswd**:

ftpasswd --passwd --file /etc/proftpd/ftpd.passwd --name nazwa_usera --home /home/ftep/nazwa_katalogu -p --uid id_usera_ftp --gid id_grupy_ftp --shell /bin/false.

W chwili obecnej ProFTPD posiada siedem różnych kontekstów konfiguracyjnych: główny serwer,

<Anonymous>, <Directory>, <Global>, <Limit>, <VirtualHosts> i pliki .ftpaccess.

Serwer główny
Kontekst ten kieruje wszystkim co nie jest zawarte w pozostałych kontekstach (np. każdą dyrektywą konfiguracyjną która nie jest wyraźnie zawarta w innym kontekście konfiguracyjnym.

<Anonymous>
Sekcja ta jest używana do skonfigurowania serwera z dostępem anonimowym. Po zalogowaniu użytkownik jest domyślnie przenoszony (*chroot*) do katalogu użytkowników anonimowych i wyłączone jest wymaganie poprawnego hasła - wymagane jest podanie adresu e-mail. W katalogu <Anonymous>'a nie powinno być plików systemowych ani innych ważnych plików.
Należy zwrócić uwagę na to, że sekcja <Anonymous> nie jest osobnym serwerem, lecz raczej "podzbiorem" serwera w którego konfiguracji jest uwzględniona. Jakiekolwiek dyrektywy konfiguracyjne ustawione dla tego serwera będą uwzględnione równie(w sekcji <Anonymous> chyba, że zostaną zmienione w tej sekcji.

Przykład konfiguracji typowego serwera FTP dla użytkowników anonymous:

<Anonymous /home/ftp>

Po załogowaniu użytkownika anonymous, serwer działa jako użytkownik ftp.

User ftp

Po załogowaniu użytkownika anonymous, serwer działa jako grupa ftp.

Group ftp

Klient logujący się jako 'anonymous' pracuje jako 'ftp'.

UserAlias anonymous ftp

Zakaz operacji zapisu w stosunku do wszystkich katalogów począwszy od root-dir

Wartością domyślna jest allow, wiec nie trzeba ustawiać <Limit> dla operacji odczytu

<Directory *>

<Limit WRITE>

DenyAll

</Limit>

</Directory>

<Directory>
Kontekst ten jest przeznaczony do konfiguracji katalogów. Uwzględnia to wyświetlanie zawartości katalogu bazujące na loginie zalogowanego użytkownika lub jego przynależności do grupy lub też zależy od nazwy pliku (np. pliki ukryte w systemie Unix), plik *.ftpaccess* podlega temu kontekstowi z definicji. Często w tym kontekście występuje również sekcja <Limit>.

Przyklad:

<Directory ~/anon-ftp>

<Limit WRITE>

DenyAll

</Limit>

</Directory

<Global>
Ten blok konfiguracyjny służy do tworzenia zestawów dyrektyw konfiguracyjnych, które odnoszą się uniwersalnie i do konfiguracji głównego serwera jak i do konfiguracji wirtualnych hostów. Mo(na tworzy) wielokrotne bloki <Global>. Podczas uruchomienia programu wszystkie te bloki są łączone w jeden a następnie wstawiane w sekcje konfiguracyjne każdego z serwerów. Należy jednak pamiętać, że jeżeli w tym bloku została użyta jaką dyrektywa, a pó6niej w sekcji głównego serwera lub w <VirtualHost> została użyta ta sama dyrektywa, ale z innymi parametrami, to ta ostatnia ma pierwszeństwo nad dyrektyw z sekcji <Global>. Pozwala to na ujednolicenie konfiguracji dla wszystkich serwerów a następnie na dostrojenie każdego z nich osobno.

<Limit>
Kontekst ten jest używany do ustanawiania ograniczę; jak i które z poszczególnych komend i grup komend FTP mogą być użyte.

Komendy do których odnosi sie <Limit>

- CWD (Change Working Directory)- Wysyłane przez klienta gdy zmienia katalog. Ten limit dotyczy takze komendy CDUP (Change Directory UP).
- MKD (MaKe Directory) - Wysyłane przez klienta gdy tworzy nowy katalog.
- RNFR (ReName FRom), RNTO (ReName TO) - Wysyłane przez klienta jako para komend gdy client to zmienia położenie pliku miedz katalogami.
- DELE (DELEte) - Wysylane przez klienta gdy kasuje plik.
- RMD (ReMove Directory) - Wysyłane przez klienta gdy usuwa katalog
- RETR (RETRieve) - Transfer pliku z serwera do klienta.
- STOR (STORe) - Transfer pliku od klienta do serwera.

Grupy komendy do których odnosi sie <Limit>

- READ - wszystkie komendy FTP wiążące się z czytaniem pliku (ale nie listing katalogu), np. RETR, STAT, itd.
- WRITE - wszystkie komendy FTP wiążące ie. z zapisem, tworzeniem, kasowaniem (obejmuje m.in. MKD i RMD).
- DIRS - wszystkie komendy FTP wiążące się z wyświetleniem zawartości katalogu np. LIST i NLST.
- ALL - wszystkie komendy FTP (identycznie zadziałałoby połączenie READ WRITE DIRS). Ta grupa komend ma najniższy priorytet ze wszystkich i nie powoduje nadpisania limitów określonych przez wymienione powyżej grupy komend (np. DIRS)

Allow

Dyrektywa Allow jest używana wewnątrz bloku <Limit> do wyspecyfikowania które hosty i/lub sieci mogą mieć dostęp do odpowiednich komend. Hosty i sieci mogą być opisane nazwami lub przez numeryczne określenie ich adresów ip

Adresy podawane numerycznie mogą obejmować cale sieci, np. wpis 192.168.0. będzie dotyczył wszystkich hostów z podsieci 192.168.0

Operowanie nazwami także może dotyczyć całych sieci lub domen np. wpis .proftpd.org będzie dotyczył całej domeny proftpd.org.

Istnieje także możliwość określenia negacji dokonanego wpisu poprzez użycie znaku !.

Przyklad:

<Limit LOGIN>

Order Allow,Deny

Allow from 128.44.26.,128.44.26.,myhost.mydomain.edu,.trusted-domain.org

Deny from all

</Limit>

Deny

Dyrektywa Deny jest używana wewnątrz bloku <Limit> do wyspecyfikowania które hosty i/lub sieci maja miec zabroniony dostęp do odpowiednich komend. Szczegóły dotyczące stosowania identyczne jak dla Allow

AllowAll

Używana wewnątrz bloku <Limit> do udostępnienia wszystkim danej komendy lub (grupy komend) opisanej w <Limit>. Może występować jednocześnie z dyrektywa Deny

DenyAll

Używana wewnątrz bloku <Limit> do zabronienia wszystkim danej komendy lub (grupy komend) opisanej w <Limit>. Może występować jednocześnie z dyrektywa Allow

.ftpaccess

Pliki te s_ podobne do plików *.htaccess* serwera Apache, które są analizowanymi w locie plikami konfiguracyjnymi - z ograniczonymi deklaracjami - które użytkownik może umieszczać w odpowiednich katalogach.

Tryby pracy serwera ProFTPD

Program ProFTPD potrafi pracować w dwóch trybach: jako usługa uruchamiana przez inetd oraz jako samodzielny demon. Te dwa różne tryby pracy MUSZA być odzwierciedlone w pliku konfiguracyjnym proftpd.conf. Służy do tego parametr: ServerType który dla pierwszego trybu powinien być ustawiony na inetd, a dla drugiego standalone

Ważniejsze parametry:

- **ServerName –** nazwa serwera
- **ServerAdmin** –adres e-mail administratora
- **ServerType** – typ serwera
- **UseIPv6** – obsługa protokołu IPv6
- **DeferWelcome** – informacja o serwerze po zalogowaniu
- **User** – konto z jakiego uruchomiono serwer
- **Group** – grupa, do której należy konto uruchamiające
- **MaxClients** – maksymalna liczba obsługiwanych połączeń
- **MaxInstances** – maksymalna liczba procesów w trybie inetd
- **DefaultRoot** – katalog główny serwera
- **Port** – port, na którym działa serwer
- **PassivePorts** – zakres portów dla trybu pasywnego
- **MasqueradeAddress** – publiczny adres w przypadku NAT
- **Umask** - maska dla tworzonych plików i katalogów
- **TimeoutIdle** – czas bezczynności do rozłączenia
- **AllowOverwrite** – nadpisywanie plików
- **AuthUserFile** – alternatywny plik z danymi identyfikacji użytkowników
- **TransferLog** – plik z logami dotyczącymi transferu
- **SystemLog** – plik z logami dotyczącymi działania serwera FTP
- **DisplayLogin** – wiadomość powitalna użytkownika
- **DisplayChdir** –wiadomość wyświetlana przy zmianie katalogu
- **RequireValidShell** – wymuszenie popranego shella
- **DirFakeUser** – wyświetlanie innego właściciela katalogu
- **DirFakeGroup** – wyświetlanie innej grupy katalogu

Przykładowy plik konfiguracyjny "/usr/local/etc/proftpd.conf"

```
# This is a ProFTPD configuration file
Po pierwsze ustawienia globalne
ServerName "Moj Serwer FTP"                 nazwa serwera
ServerAdmin admin@moja.domena.pl            email administratora
ServerType standalone                       typ serwera
```

DeferWelcome on	dyrektywa opóźniająca wyświetlanie nazwy i adresu serwera do momentu autentykacji użytkownika
DefaultServer on	
DefaultRoot ~	ustawienie jako korzenia katalogu domowego użytkownika
Port 21	nr portu
Umask 002	maska ustawiana nowo tworzonym plikom i katalogom

Ustawienia użytkownika i grupy serwera

User ftpdemon	użytkownik na jakim uruchomiony jest serwer FTP
Group ftp	grupa do której należy ten użytkownik
(przypuszczalnie	musisz ja sobie stworzyć)

Timeouty - różne

TimeoutIdle 300
TimeoutStalled 300
TimeoutLogin 60
TimeoutNoTransfer 300

Logi

ExtendedLog /var/log/proftp.log	miejsce składowania logów
ExtendedLog /dev/tty11	konsola na której są wyświetlane logi
DisplayLogin .welcome.msg	wiadomość powitalna
MaxInstances 20	maksymalna ilość procesów potomnych, tylko dla trybu standalone
MaxLoginAttempts 2	maksymalna ilość prób logowania

Ograniczenia obci,)enia serwera

MaxClients 20 ">>> Za duzo uzytkownikow <<<"
maksymalna liczba użytkowników zalogowanych w danej chwili i w cudzysłowie wiadomość

MaxClientsPerHost 40 ">>> Za duzo polaczen z jednego IP <<<"
maksymalna liczba połączeń z jednego IP

Ograniczenia IP/hostów z których można się zalogować

Opcja a) Możesz zalogować się z każdego miejsca poza tymi, które są w polach >
Deny from
<Limit LOGIN>
Order allow,deny
Deny from host.domena1.pl

Deny from w3cache.pwr.wroc.pl
Deny from w3cache.tpnet.pl
Deny from w3cache.
Deny from .cst.tpsa.pl
Deny from .gov.pl
Deny from .gov
Deny from .pol.co.uk
</Limit>
Opcja b) możesz zalogować się z każdego miejsca (poza .lame.net)
<Limit LOGIN>
Order deny,allow
Deny from .lame.net
AllowAll
</Limit>

Ustawienia dla poszczególnych użytkowników
##########################
A N O N Y M O U S
##########################

Dotyczy np. użytkownika ftp czyli tzw. anonymousa

<Anonymous ~ftp>	początek ustawień użytkownika ftp
User ftp	użytkownik
Group ftp	grupa
AnonRequirePassword off	logowanie bez hasła
UserAlias anonymous ftp	aliasy tego użytkownika, może się logować i ftp i anonymous
DisplayLogin .welcome.msg	powitalna wiadomość odczytywana z pliku
DisplayFirstChdir .message	wiadomość która pokazuje się po wejściu do katalogu
GroupOwner ftp	
Umask 002	
HideUser root	ukrywa przed użytkownikiem wszystkie katalogi/pliki użytkownika root
HideGroup root	ukrywa przed użytkownikiem wszystkie katalogi/pliki grupy root
HideNoAccess on	ukrywa przed użytkownikiem wszystkie katalogi/pliki do których nie ma on dostępu

Ograniczenia obciążenia serwera (j.w)
MaxClients 10 ">>> Za duzo uzytkownikow <<<"
MaxClientsPerHost 5 ">>> Za duzo polaczen z jednego hosta <<<"

Ograniczenia mówiące o braku praw do uploadu

<Limit WRITE>	ograniczenie zapisywania
DenyAll	zabroń jakiegokolwiek zapisywania
</Limit>	
<Limit READ DIRS>	ograniczenie odczytywania zawartości katalogów
IgnoreHidden on	ignorowanie ukrytych plików/katalogów
</Limit>	
</Anonymous>	to jest koniec ustawień dla tego użytkownika

```
######################
# DLA WYBRANYCH #
######################
```

<Anonymous ~wybrany> użytkownik wybrany - należy go dodać do systemu

```
User wybrany
Group ftp
AnonRequirePassword on
DisplayLogin .welcome.msg
DisplayFirstChdir .message
GroupOwner wybrany
Umask 002
HideUser root
HideGroup root
HideNoAccess on
MaxClients 10 ">>> Za duzo uzytkownikow <<<"
MaxClientsPerHost 5 ">>> Za duzo polaczen z jednego IP <<<"
```

Zezwalamy na logowanie się tylko z IP w polach Allow from i z domen *.pl - pozostałe zabronione

```
<Limit LOGIN>
Order allow,deny
Allow from .pl
Allow from 127.0.0.1
Allow from 192.168.1.
Allow from 212.160.79.
Allow from 212.160.254.10
Allow from 212.160.254.2
DenyAll
</Limit>
```

Opcja a) bez prawa do UPLOADu

```
<Limit WRITE>
DenyAll
</Limit>
<Limit READ DIRS>
IgnoreHidden on
```

</Limit>

ProFTPD nie działa

Podczas uruchamiania ProFTPD w trybie standalone nie widać procesu przy użyciu "ps". Może to być spowodowane wieloma czynnikami, prawdopodobnie czymś takim jak nie uruchamianie ProFTPD jako root (program musi być uruchomiony początkowo z konta root'a, ale później przełączy się na nie uprzywilejowanego użytkownika). Niezależnie ProFTPD zapisuje wszystkie błędy poprzez standardowy mechanizm zapisu błędów (syslog). Nalezy sprawdzić logi systemowe, aby ustalić gdzie tkwi problem.

To nie działa!
Wielokrotnie może się zdarzyć, że wystąpi całkowicie przypadkowy problem wydający się nierozwiązywalnym. Najlepszym miejscem by spytać o pomoc jest zdecydowanie lista mailingowa (proftpd-l) ale bezproduktywnym jest proszenie o pomoc bez podania wystarczającej ilości informacji na temat problemu.
Czy:
sprawdziłeś logi systemowe?
próbowałeś uruchomi) serwer w trybie debugowania?
przeczytałeś FAQ?
sprawdziłeś archiwum listy mailingowej?
używasz najnowszej wersji programu?

Jeśli wysyłasz zapytanie na listę mailingową spróbuj podać wystarczającą ilość informacji na temat problemu. Informacje te mogą zawierać:
-system operacyjny i wersję serwera (proftpd -vv),
-listę zainstalowanych modułów (proftpd -l),
-odpowiednie wycinki z logów,
-wynik uruchomienia ProFTPD w trybie debug,
-fragment pliku konfiguracyjnego.