Konfiguracja vsftpd (Very Secure FTP Server)

Pliki konfiguracyjne serwera są zlokalizowane w katalogu /etc/vsftpd. Głównym plikiem konfiguracyjnym jest vsftpd.conf. Opcje konfiguracyjne są zapisywane w formacie opcja=wartość. Między nazwą opcji a znakiem „=" oraz wartością opcji nie należy umieszczać spacji. W pliku konfiguracyjnym istotna jest również wielkość liter. Wszystkie linie rozpoczynające się od znaku # są komentarzami. które nie mają wpływu na działanie serwera. a służą tylko do wyjaśnienia do czego służą poszczególne opcje.

Po instalacji w plik konfiguracyjnym vsftpd są gotowe ustawienia.
Polecam zmienić nazwę /etc/vsftpd.conf np. na /etc/vsftpd.conf.old i stworzyć go od nowa. Gdyby po dokonaniu zmian w konfiguracji serwer nie mógł się uruchomić, będzie można przywrócić wcześniejsze jego ustawienia.

Konfiguracja serwera FTP do obsługi użytkowników lokalnych.
Użytkownicy lokalni to tacy użytkownicy, którzy mają na serwerze swoje konta. Aby posiadać takie konto, należy zwrócić się do administratora o jego założenie. Użytkownicy lokalni na ogół posiadają uprawnienia do zapisywania danych w swoich katalogach lokalnych (usługa niedostępna dla użytkowników anonimowych). W konfiguracji dostarczanej z dystrybucją opcja korzystania z kom lokalnych jest standardowo włączona. Jeżeli serwer ma być dostępny tylko dla użytkowników lokalnych, należy wyłączyć opcję zezwalającą na logowanie się użytkowników anonimowych.

Konfiguracja serwera FTP do obsługi użytkowników anonimowych.
Z konta anonimowego korzystać może każdy, ale uprawnienia na ogół są ograniczone tylko do pobierania danych. Hasłem dla konta anonimowego jest adres e-mail użytkownika. Niektóre serwery sprawdzają, czy wpisane hasło jest poprawnym adresem poczty elektronicznej. W konfiguracji dostarczanej z dystrybucją opcja korzystania z konta anonimowego jest standardowo włączona. Jeżeli serwer ma być dostępny tylko dla użytkowników anonimowych, należy wyłączyć opcję zezwalającą na logowanie się użytkowników lokalnych.

Zapisywanie danych na serwerze przez użytkowników anonimowych.
Standardowo użytkownicy anonimowi mają uprawnienia ograniczone tylko do pobierania danych. W szczególnych okolicznościach można umożliwić zapisywanie danych na serwerze również użytkownikom anonimowym. ale tylko w wybranym przez administratora, przeznaczonym do tego celu katalogu. Programy i dokumenty umieszczone na serwerze przez użytkowników anonimowych mogą stanowić poważne zagrożenie dla bezpieczeństwa (wirusy, konie trojańskie irp.). Trzeba zadbać również o to, aby administrowany serwer nie stał się punktem dystrybucji nielegalnego oprogramowania lub innych niedozwolonych treści. Jeżeli użytkownik anonimowy skopiuje na serwer dowolny plik. to nie może mieć prawa do jego ponownego pobrania. skasowania lub modyfikacji. Najlepiej, aby w ogóle nie mógł przeglądać zawartości tego katalogu. Każdy z takich plików powinien zostać sprawdzony przez administratora pod kątem legalności i zawartych w nim treści - jeśli administrator uzna plik za bezpieczny. może udostępnić go wszystkim użytkownikom. przenosząc go do katalogu, skąd będzie mógł być pobierany. Aby umożliwić użytkownikom anonimowym zapisywanie

danych w wybranym katalogu, należy taki katalog utworzyć w miejscu, do którego anonimowi użytkownicy usługi FTP będą mogli uzyskać dostęp. Dobrym miejscem może być katalog domowy użytkownika FTP (konto takie jest tworzone podczas instalacji serwera vsftpd i wykorzystywane przez serwer do uzyskiwania dostępu do systemu). Katalog domowy tego użytkownika jest zlokalizowany w /var/ftp.

Jednoczesne uruchamianie wielu serwisów FTP.
Na jednym serwerze można uruchomić wiele usług FTP pod warunkiem. że każda usługa korzysta z innego portu, dzięki temu zyskujemy możliwość uruchomienia serwera anonimowego osobno konfigurowalnego obok serwera produkcyjnego. Zmiana konfiguracji jednego lub wyłączenie nie zakłóci pracy drugiego.
Aby uruchomić wiele usług FTP, należy dla każdej usługi utworzyć oddzielny plik konfiguracyjny, np: konfiguracja domyślna - vsftpd.conf, konfiguracja dla użytkowników anonimowych - vsfcpd_anon.conf, konfiguracja dla użytkowników lokalnych - vsftpd_local.conf, pliki te muszą znajdować się w katalogu /etc/vsftpd i kończyć się .conf. Po restarcie serwera FTP są uruchamiane trzy usługi FTP.

Niektóre z najważniejszych opcji jakie możemy wykorzystać podczas budowania własnego configa.:

Poziom z którego zostaje uruchomiony serwer

nopriv_user=

Uruchamianie serwera w trybie standalone

listen=

Określenie portu, na którym serwer ma nasłuchiwać (domyślnym jest port 21)

listen_port=

Zabronienie na logowanie się użytkownikom anonimowym, domyślnie jest to YES

anonymous_enable=

Zezwolenie na logowanie się użytkownikom lokalnym, domyślnie jest to NO

local_enable=

Zezwolenie na zapis w katalogu użytkownika lokalnego

write_enable=

Umask (w większości serwerów używany jest 022)

local_umask=

Umask dotyczący anonimowych

anon_umask=022

limit szybkości podawany jest w bajtach na sekundę, jeśli jest ustawiony na 0 to brak jakiegokolwiek limitu.

local_max_rate=

Włączenie logowania

xferlog_enable=

Ścieżka do pliku z logami

xferlog_file=/var/log/vsftpd.log

Maksymalna liczba połączonych użytkowników

max_clients=

Maksymalna liczba użytkowników mogących się połączyć z tego samego adresu IP

max_per_ip=

Banner, który będzie wyświetlany podczas logowania. W jego stworzeniu może być pomocny program app-misc/figlet.

banner_file=/etc/vsftpd/vsftpd.banner

Ograniczenie użytkownikom do poruszania się jedynie w obrębie katalogu domowego

chroot_local_user=

Katalog dla chroot’a

secure_chroot_dir=/var/chroot/vsftpd

Dodanie użytkowników, którzy mogą poruszać się poza katalogiem domowym

chroot_list_enable=YES

Dodajemy użytkownika z przywilejami poruszania się poza katalogiem domowym np:

echo „użytkownik” >> /etc/vsftpd/chroot.list

chroot_list_file=/etc/vsftpd/chroot.list

Serwer nie będzie pytał o hasło, podczas logowania na anonymous:

no_anon_password=

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

anon_world_readable_only=

Zabraniamy na upload plików:

anon_upload_enable=

Ukrywamy prawdziwych użytkowników oraz grup dla plików lub katalogów

(vsftpd zamieni je na nazwy użytkownika odpowiedzialnego za anonimowy ftp):

hide_ids=

Pozwala na tworzenie katalogów

anon_mkdir_write_enable=

Pozwala na kasowanie i zmienianie nazw katalogów przez anonimowych

anon_other_write_enable=

Pozwala ograniczyć transfer dla anonimowych

anon_max_rate=

Maxymalny czas bezczynności

idle_session_timeout=300

Jeżeli jest ustawione na YES pozwala na ściąganie metodą ASCII

ascii_download_enable=

Jeżeli jest ustawione na YES pozwala na wysyłanie metodą ASCII

ascii_upload_enable=NO

Sam decydujesz czy mogą się łączyć Aktywnie czy Pasywnie

connect_from_port_20=NO

Ustawione na NO zablokuje polecenia PORT i ustawi serwer w tryb pasywny (lepiej YES)

port_enable=YES

Ustawione na YES loguje polecenia FTP wydawane przez użytkowników

log_ftp_protocol=NO

Pozwala ograniczyć możliwość wydawania komand do minimum(możemy zabronić ściągania, sprawdzania wielkości plików itp), pełna lista możliwość tutaj -> http://www.nsftools.com/tips/RawFTP.htm

cmds_allowed=

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 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/

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

setproctitle_enable=YES

Przykładowe pliki vsftpd.conf

Przykład nr 1

Poniższa konfiguracja serwera FTP umożliwia łączenie użytkowników do swoich katalogów domowych. Mogą oni pobierać i wysyłać na swoje konta dane z prędkością do 5 KB/s w każdą stronę. Po poprawnym zalogowaniu się do swoich kont nie będą mogli wychodzić poza swój katalog domowy ze względów bezpieczeństwa. Istnieje możliwość dodania użytkowników którzy będą mogli poruszać się poza swoim katalogiem domowym. Zabronione jest również logowanie się anonimowych użytkowników.

nopriv_user=ftp

listen=YES

listen_port=21

anonymous_enable=NO

local_enable=YES

write_enable=YES

local_umask=022

local_max_rate=5120

xferlog_enable=YES

xferlog_file=/var/log/vsftpd.log

max_clients=500

max_per_ip=2

banner_file=/etc/vsftpd/vsftpd.banner

chroot_local_user=YES

secure_chroot_dir=/var/chroot/vsftpd

chroot_list_enable=YES

chroot_list_file=/etc/vsftpd/chroot.list

Przykład nr 2

Poniższy przykład pozwala na logowanie się użytkowników anonimowych, serwer działa na porcie 2121. Anonimowi oraz normalni mogą pobierać i wysyłać na swoje konta dane bez ograniczeń. Wszyscy mają zakaz opuszczania własnego katalogu. Dla anonimowych będzie to /var/ftp . Maksymalna ilość połączeń wynosi 5 a dla jednego IP jest to 2. Pliki zakazane na serwerze to *.mp3 i *.avi a katalog files. A pliki niewidoczne dla userów do *.doc i *.xls

nopriv_user=ftp

listen=YES

listen_port=2121

anonymous_enable=YES

local_enable=YES

ftpd_banner="Serwer vsFTPd wita"

xferlog_enable=YES

xferlog_file=/var/log/xferlog.log

xferlog_std_format=YES

chroot_local_user=YES

secure_chroot_dir=/var/ftp

no_anon_password=YES

write_enable=YES

anon_upload_enable=YES

anon_mkdir_write_enable=NO

hide_ids=YES

local_umask=022

anon_umask=022

#limity liczby równoczesnych połączeń

max_clients=5

max_per_ip=2

idle_session_timeout=120

data_connection_timeout=900

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

hide_file={*.doc,*.xsl}

Przykład nr 3

Konto z możliwością logowania się tylko anonimowo. Można jedynie pobierać pliki bez ingerencje w nie.

listen=YES

anonymous_enable=YES

ftp_username=ftp

write_enable=NO

anon_upload_enable=NO

anon_mkdir_write_enable=NO

anon_other_write_enable=NO

anon_world_readable_only=YES

anon_max_rate=0

idle_session_timeout=300

ascii_download_enable=NO

ascii_upload_enable=NO

connect_from_port_20=NO

port_enable=YES

hide_ids=NO

log_ftp_protocol=NO

syslog_enable=NO

max_per_ip=0

cmds_allowed=

local_root=/usr/share/empty

nopriv_user=nobody

ftpd_banner=(vsFTPd 1.2.0)

Uruchamianie

Jeżeli posiadamy tylko jeden plik konfiguracyjny to możemy po prostu wydać polecenie /etc/init.d/vsftpd start lub service vsftpd start

Jeżeli posiadamy parę plików konfiguracyjnych to musimy każdy osobno załadować :

vsftpd /etc/vsftpd.conf.annonymus

vsftpd /etc/vsftpd.conf.normalny

vsftpd /etc/vsftpd.conf.bartek