Wu-FTPd manual page

Wu-FTPd group v1.13 2000년 7월 1일

김정균, admin@oops.org v1.15 2000년 8월 5일

이 문서는 Wu-ftpd의 manual page를 번역한 것이다. Wu-ftpd에 대한 변변한 Manual이 없던 차에 man page를 번역하게 되었고 Internet 상에 올려져 있는 어떠한 Wu-ftpd에 대한 자료 보다도 아주 상세한 내용들이 들어 있다. 단 번역자의 번역 실력이 별로라는 것을 감안해 주기 바란다.

목 차

제 1 절 INSTALLATION INSTRUCTIONS **5**

제 2 절 ftpaccess **11**

2.1 이름 . . . 11

2.2 설명 . . . 11

2.3 접근 방법 설정 . . . 11

2.3.1 autogroup <groupname> <class> [<class> ...] . . . 11

2.3.2 class <class> <typelist> <addrglob> [<addrglob> ...] . . . 11

2.3.3 deny <addrglob> <message_file> . . . 12

2.3.4 User & Group . . . 12

2.3.5 nice <nice-delta> [<class>] . . . 12

2.3.6 defumask <umask> [<class>] . . . 13

2.3.7 tcpwindow <size> [<class>] . . . 13

2.3.8 keepalive <yes|no> . . . 13

2.3.9 timeout accept <seconds> timeout connect <seconds> timeout data <seconds> timeout idle <seconds> timeout maxidle <seconds> timeout RFC931 <seconds> . . . 13

2.3.10 file-limit [<raw>] <in|out|total> <count> [<class>] . . . 13

2.3.11 data-limit [<raw>] <in|out|total> <count> [<class>] . . . 13

2.3.12 limit-time {*|anonymous|guest} <minutes> . . . 14

2.3.13 guestserver [<hostname>] . . . 14

2.3.14 limit <class> <n> <times> <message_file> . . . 14

2.3.15 noretrieve [absolute|relative] [class=<classname>] ... [-] <filename> <filename> 14

2.3.16 allow-retrieve [absolute|relative] [class=<classname>]... [-] <filename> 14

2.3.17 loginfails <number> . . . 14

2.3.18 private <yes|no> . . . 15

2.3.19 group access file . . . 15

2.4 정보에 관한 활용 . . . 15

2.4.1 greeting full|brief|terse greeting text <message> . . . 15
2.4.2 banner <path> . . . 15
2.4.3 hostname <some.host.name> . . . 15
2.4.4 email <name> . . . 15
2.4.5 message <path> {<when> {<class> ...}} . . . 16
2.4.6 readme <path> {<when> {<class>}} . . . 17
2.5 로그 활용 . . . 17
2.5.1 log commands <typelist> . . . 17
2.5.2 log transfers <typelist> <directions> . . . 17
2.5.3 log security <typelist> . . . 18
2.5.4 log syslog+xferlog . . . 18
2.6 여러가지 활용 . . . 18
2.6.1 alias <string> <dir> . . . 18
2.7 Upload/Download 비율 . . . 18
2.7.1 ul-dl-rate <rate> [<class> ...] . . . 18
2.7.2 dl-free <filename> [<class> ...] . . . 18
2.7.3 dl-free-dir <dirname> [<class> ...] . . . 18
2.8 여러가지 활용 . . . 18
2.8.1 alias <string> <dir> . . . 18
2.8.2 cdpath <dir> . . . 19
2.8.3 compress & tar . . . 19
2.8.4 shutdown <path> . . . 19
2.8.5 daemonaddress <address> . . . 20
2.8.6 virtual <address> <root|banner|logfile> <path> . . . 20
2.8.7 virtual <address> <hostname|email> <string> . . . 20
2.8.8 virtual <address> allow <username> [<username> ...] . . . 20
2.8.9 virtual <address> private . . . 20
2.8.10 virtual <address> passwd <file> . . . 21
2.8.11 virtual <address> shadow <file> . . . 21
2.8.12 defaultserver . . . 21
2.8.13 defaultserver private . . . 21
2.8.14 passive address <externalip> <cidr> . . . 21
2.8.15 passive ports <cidr> <min> <max> . . . 21
2.8.16 pasv-allow & port-allow . . . 22
2.8.17 lslong, lsshort, lsplain . . . 22
2.8.18 mailserver <hostname> . . . 22
2.8.19 incmail, virtual incmail, defaultserver incmail . . . 22

2.8.20 mailfrom, virtual mailfrom, defaultserver mailfrom . . . 23
2.9 권한 활용 . . . 23
2.9.1 chmod delete overwrite rename umask . . . 23
2.9.2 passwd-check <none|trivial|rfc822> (<enforce|warn>) . . . 23
2.9.3 deny-email <case-insensitive-email-address> . . . 23
2.9.4 path-filter <typelist> <mesg> <allowed_charset> {<disallowed regexp> ...} . . . 24
2.9.5 upload [absolute|relative] [class=<classname>]... [-] <root-dir> <dirglob> <yes|no> <owner> <group> <mode> ["dirs"|"nodirs"] [<d_mode>] . . . 24
2.9.6 throughput <root-dir> <subdir-glob> <file-glob-list> <bytes-per- second> <bytes-per-second-multiply> <remote-glob-list> . . . 25
2.9.7 anonymous-root <root-dir> [<class>] . . . 25
2.9.8 guest-root <root-dir> [<uid-range>] . . . 26
2.9.9 deny-uid deny-gid allow-uid allow-gid . . . 26
2.9.10 restricted-uid restricted-gid unrestricted-uid unrestricted-gid . . . 27
2.9.11 site-exec-max-lines <number> [<class> ...] . . . 27
2.9.12 dns refuse_mismatch <filename> [override] . . . 27
2.9.13 dns refuse_no_reverse <filename> [override] . . . 28
2.9.14 dns resolveroptions [options] . . . 28
2.10 파일 . . . 28
2.11 관련 항목 . . . 28

제 3 절 ftpconversions **28**
3.1 이름 . . . 28
3.2 설명 . . . 28
3.3 알려진 문제 . . . 29
3.4 파일 . . . 29

제 4 절 ftpcount **29**
4.1 이름 . . . 29
4.2 문법 . . . 29
4.3 설명 . . . 29
4.4 관련 항목 . . . 29

제 5 절 FTPD **29**
5.1 이름 . . . 29
5.2 개요 . . . 29
5.3 설명 . . . 30
5.4 BSD/OS SYSTEM만의 인증 MECHANISM . . . 32
5.5 일반적인 FTP 확장자들 . . . 32

5.6 관련 항목 . . . 33
5.7 버그 . . . 33

제 6 절 ftphosts **33**
6.1 이름 . . . 33
6.2 설명 . . . 33
6.3 접근 사용법 . . . 34
6.4 파일 . . . 34
6.5 관련 항목 . . . 34

제 7 절 ftpshut **34**
7.1 이름 . . . 34
7.2 문법 . . . 34
7.3 설명 . . . 34
7.4 제한 . . . 35
7.5 관련 항목 . . . 35

제 8 절 ftpwho **35**
8.1 이름 . . . 35
8.2 문법 . . . 36
8.3 설명 . . . 36
8.4 제한 . . . 36
8.5 관련 항목 . . . 36

제 9 절 XFERLOG **36**
9.1 이름 . . . 36
9.2 설명 . . . 36
9.2.1 current-time . . . 36
9.2.2 transfer-time . . . 36
9.2.3 remote-host . . . 36
9.2.4 file-size . . . 37
9.2.5 filename . . . 37
9.2.6 transfer-type . . . 37
9.2.7 special-action-flag . . . 37
9.2.8 direction . . . 37
9.2.9 access-mode . . . 37
9.2.10 username . . . 38
9.2.11 service-name . . . 38
9.2.12 authentication-method . . . 38

9.2.13 authenticated-user-id 38
9.2.14 completion-status 38
9.3 파일 38
9.4 관련 항목 38

제 10 절 ftprestart **38**
10.1 이름 38
10.2 문법 39
10.3 출력 예제 39
10.4 관련 항목 39

제 11 절 ftpservers **39**
11.1 이름 39
11.2 설명 39
11.3 ftpservers file 형식 40
11.4 관련 항목 40

제 12 절 Copyright **40**

제 1 절 INSTALLATION INSTRUCTIONS

역자 주

Wu-FTPd 2.6.0 부터는 GNU autoconf를 사용하게 되었다. 그러므로 기존의 build script를 사용하는 것 보다는 configure를 사용하는 것을 권장한다.

./configure [–opeiont] make make install

로 사용하면 된다.

[configure option] 설정:

–cache-file=FILE cache test results in FILE

–help 이 메세지들을 출력

–no-create 출력물을 만들지 않음

–quiet, –silent ‘checking...’ 메세지를 출력하지 않음

–version autoconf의 버젼을 출력

디렉토리와 파일이름:

–prefix=PREFIX PRIFIX에 독립적인 구조로 인스톨 [/usr]

–exec-prefix=EPREFIX EPREFIX에 종속적인 파일구조로 인스톨 [same PREFIX]

–bindir=DIR 유저가 실행할 파일들이 있는 디렉토리 [EPREFIX/bin]

–sbindir=DIR ROOT가 실행할 파일들이 있는 디렉토리 [EPREFIX/sbin]

–libexecdir=DIR 프로그램이 실행할 파일들이 있는 디렉토리 [EPREFIX/libexec]

–datadir=DIR 읽기 속성의 독립적인 data를 가질 디렉토리 [PREFIX/share]

–sysconfdir=DIR 설정파일이 위치할 디렉토리 경로 지정 [PREFIX/etc]

–sharedstatedir=DIR 수정 가능한 독립구조를 가진 데이타가 위치할 경로지정 [PREFIX/com]

–localstatedir=DIR modifiable single-machine data in DIR [PREFIX/var]

–libdir=DIR 라이브러리 파일들이 위치할 디렉토리 경로 [EPREFIX/lib]

–includedir=DIR C 헤더 파일이 위치할 디렉토리 경로 [PREFIX/include]

–oldincludedir=DIR GCC를 위한것이 아닌 C 헤더 파일의 경로 [/usr/include]

–infodir=DIR 문서가 위치할 디렉토리 경로 [PREFIX/info]

–mandir=DIR 메뉴얼 페이지가 위치할 디렉토리 경로 [PREFIX/man]

–srcdir=DIR 소스가 있는 디렉토리 지정 [configure dir or ..]

–program-prefix=PREFIX prepend PREFIX to installed program names

–program-suffix=SUFFIX append SUFFIX to installed program names

–program-transform-name=PROGRAM run sed PROGRAM on installed program names

호스트 형식:

–build=BUILD configure for building on BUILD [BUILD=HOST]

–host=HOST configure for HOST [guessed]

–target=TARGET configure for TARGET [TARGET=HOST]

요소와 패키지:

–disable-FEATURE FEATURE를 포함하지 않음 (–enable-FEATURE=no 와 동일)

–enable-FEATURE[=ARG] FEATURE 포함 [ARG=yes]

–with-PACKAGE[=ARG] PACKAGE를 사용함 [ARG=yes]

–without-PACKAGE PACKAGE를 사용하지 않음 (–with-PACKAGE=no 와 동일)

–x-includes=DIR X include files are in DIR

–x-libraries=DIR X library files are in DIR

–enable 과 –with 옵션 인식:

–with-etc-dir=PATH 설정파일이 위치할 경로 [/etc]

–with-pid-dir=PATH run/pid 파일들의 경로 [/var/run]

–with-log-dir=PATH log 파일 [/var/log]

–disable-upload ftpaccess에서 UPLOAD 키워드를 사용하지 않음

–disable-overwrite ftpaccess에서 OVERWIRTE 키워드를 사용하지 않음

–disable-hostxs ftpaccess에서 ALLOW/DENY 키워드를 사용하지 않음

–disable-logfailed 로그인 시에 로그실패 횟수 지정을 사용하지 않음

–disable-logtoomany 로그인 시에 유저 제한을 사용하지 않음

–disable-private don't support private files (SITE GROUP/SITE GPASS)

–disable-dnsretry DNS lookup을 하지않음

–enable-anononly 익명 접속만 가능함

–enable-paranoid 질의 요소들을 사용하지 않음

–enable-quota 쿼타 지원 (OS에서 지원을 해야 함)

–enable-pam PAM 지원 (PAM 라이브러리가 필요)

–enable-skey S/KEY 지원 (SKEY 라이브러리 필요)

–enable-opie OPIE 지원(OPIE 라이브러리 필요)

–disable-new-cd new-cd causes "cd " to return to chroot-relative dir

–enable-chmod ftp 유저들이 SETUID/SETGID/STICKY bits를 셋팅하는 것을 허락

–enable-rfc931 RFC931 lookups을 함(log 정보를 더 자세히 얻을수 있으나 느림)

–enable-ratios 업로드 다운로드 비율을 지원

–enable-passwd 다른 패스워드 파일을 사용할수 있게 함

–disable-daemon standalone 방식을 사용하지 않음

–disable-map-chdir don't keep track of user's path changes

–disable-throughput don't keep track of user's throughput

–disable-count don't keep track of bytes for statistics

–disable-newlines 공백라인이 작동하지 못하게 함

–enable-crackers 유저이름이 존재하지 않을 경우 password를 기다리지 않음

–disable-verbose 에러로그를 간단하게 함

–enable-noop idle 시간초과시 NOOP명령을 리셋

–disable-log-rp log the relative path rather than the real one

–disable-virtual 가상 호스트를 지원안함

–disable-closedvirt 가상 호스트에 guest log를 허락

–disable-dns 모든 DNS lookup을 안함

–disable-port port mode를 허락하지 않음

–disable-pasv passive mode를 사용하지 않음

–disable-plsm PID lock sleep message를 사용하지 않음(트래픽이 많은sites)

–disable-pasvip don't require require same IP for passive connections

–disable-anonymous 익명 접속을 허락하지 않음

–enable-ls 내부 ls 명령을 사용 (실험적인 요소)

–disable-numericuid 내부 ls사용시 유저이름 대신 UID를 표시 (빠름)

–disable-hidesetuid 내부 ls 사용시 setuid/setgid bits를 출력

–disable-mail 익명 upload시에 통지 메일을 발송하지 않음

–enable-badclients support broken clients (see CHANGES)

–with-bufsize=x set buffer size to x

–with-backlog=x number of incoming processes to backlog in daemon mode

<1a>

source tree의 제일 상위에서 "./build xxx" 를 실행한다. "./build xxx"를 실행 할때 C compiler를 대신하여 "./build CC=yyy xxx" 와 같이 yyy에 cc를 대신할 compiler를 지정하여 실행할수도 있다.

["gcc"를 사용하기 위해서는 다음과 같이 실행한다. "./build CC=gcc xxx".]

"./build xxx" 명령에서 xxx는 아래의 os type중 하나를 선택하면 된다.:

gen : generic make (copy this when porting to a new system)

aix : IBM AIX

aux : AU/X

bdi : BSD/OS

bsd : BSD

dec : DEC Unix 3.X or later

dyn : Dynix

fbs : FreeBSD 2.0 or later

hiu : Hitachi Unix

hpx : HP-UX

lnx : Linux (tested on 2.0.30)

nbs : NetBSD 1.X

nx2 : NeXTstep 2.x

nx3 : NeXTstep 3.x

osf : OSF/1

ptx : ???

sco : SCO Unix 3.2v4.2/SCO OpenServer 5

sgi : SGI Irix 4.0.5a

sny : Sony NewsOS

sol : SunOS 5.x / Solaris 2.x

s41 : SunOS 4.1.x

ult : Ultrix 4.x

uxw : UnixWare 1.1 or later

clean : Clean up object files and such to reduce disk space after building.

install: Install ftpd

<1b>

만약 너의 system이 위의 list에 없거나 에러가 발생한다면...

cp src/config/config.gen src/config/config.xxx

cp src/makefiles/Makefile.gen src/makefiles/Makefile.xxx

cp support/makefiles/Makefile.gen support/makefiles/Makefile.xxx

적당하게 3개의 파일을 편집해야 한다. 다시 step 1a로 돌아간다. 이것은 사소한 것이 아니다. mailling list나 질문을 원할수도 있다.

[wu-ftpd-bugs@academ.com 으로 그런 변화들에 대해 보내면 된다!]

<2>

wu-ftpd의 새로운 version으로 upgrade를 하려 한다면, 예전의 모든 configure file들을 backup 해 놓아야 한다. 그렇지 않으면 새로이 install을 했을 경우에 새 version의 sample file들이 예전의 것들로 대체 되어 버린다.

<3>

super-user의 권한으로 "./build install" 을 실행한다.

<4>

새로운 version의 ftpd를 "/etc/inetd.conf"에 지정을 한다. 대부분의 경우, old version이 설치되어 있다면 이 단계는 생략해도 된다. 만약 이 server의 확장 기능들을 사용하고자 한다면 Ftpd를 실행할때 -a option을 같이 실행해 줘야 한다. 일반적으로 이것은 server를 실행할 때 /etc/inetd.conf의 line의 끝에 "-a"(따옴표는 생략)을 추가해야한다는 것을 의미한다. /etc/inetd.conf를 이용하지 않는 OS 에서는 standalone mode로 실행을 하거나 또는 다른 방법으로 실행시키는 방법을 위하여 OS documentation을 읽어보아야 한다. 기본적으로 inetd로 실행을 하거나 다른 방법으로 실행을 하거나 큰 차이는 없다.

<5>

BSD 계열의 sytem에서는, type "kill -1 `ps t"?" | grep inetd`"

SGI system에서는, type "/etc/killall -HUP inetd"

AIX system에서는, type "refresh -s inetd"

<6>

Ftpd가 directory의 .tar.Z 의 생성을 지원하게 하기 위해서는 GNU tar를 설치 해야 한다. [anonymous ftp 에 copy를 해 줘야 하는 것을 기억해야한다.] GNU tar가 필요 하다면, prep.ai.mit.edu의 /pub/gun directory에서 구할수 있다.

<7>

~ftp/bin/compress로 압축 program을 copy한다. "ls" program을 ~ftp/bin/ls 로 copy를 한다. OS가 공유 librariy를 사용한다면 이 program들은 정적으로 link 되어진 것이 아니다. 새로이 이 link들을 정확한 경로로 설정을 해줄 필요가 있다.

<8>

ftpd를 위한 여러 설정 file들(ftpconversions, ftpusers, ftpgroups)을 위치 할 곳을 조사하기 위한 첫단계를 행할때, ckconfig 를 사용하라. 이 file들의 예제들은 doc/examples directory에 존재한다. ckconfig는 bin direcoty에 있다. ckconfig report로 어떤 문제점들을 수정하도록 한다.

<9>

anonymous user들이 _SITE_EXEC에서 실행이 가능하게 하기를 원하면 어떤 실행 가능한 것을 넣어 줘야 한다. 이것을 넣을때는 매우 주의해야 한다.

<10>

bin/ckconfig로 다시 설정 file들이 제대로 install이 되었는지 확인을 한다.

<11>

virtual ftp를 지원하기 위해서는 Makefile의 CFLAGS에 -DVIRTUAL을 추가하여 compile을 해야 한다.

제 2 절 ftpaccess

2.1 이름

ftpaccess - ftpd 설정 file

2.2 설명

ftpaccess file은 ftpd(1) 를 어떻게 운영할것인지를 설정하는데 사용한다.

2.3 접근 방법 설정

2.3.1 autogroup <groupname> <class> [<class> ...]

Anonymous user가 특정 <clas>의 member일때, ftp server는 <groupname>에 setegid()를 실행할 것이다. 이것은 특정 group의 anonymous user들에게 file과 directory를 group-and-owner-read-only의 권한으로 접근을 허락 하는 것을 말한다. <groupname>은 /etc/group에 존재하는 group이어야 한다.

2.3.2 class <class> <typelist> <addrglob> [<addrglob> ...]

<addrglob> 형식의 source address들로 user의 <class>를 정의한다. <class>는 중복되어 설정을 할수 있으며 "class"를 중복되게 나열하여 class의 추가 member를 정의할수 있다. 이 중복된 "class"들이 현재 session에 적용이 된다면 access file에 나열되어 있는 것들중 가장 먼저 나오는 것이 사용되어 진다. class의 설정을 잘못하면 접속 거부를 당하게 된다. <typelist>는 "anonymous", "guest", "real"의 keyword가 존재하며 이 3개의 keyword는 comma(컴마)로서 구분을 한다. "real"은 real account로 ftp를 사용하는 user를 말하며, "anonymous"는 anonymous FTP를 위한 user(anonymous, ftp)를 말한다. "guest"는 손님 사용자로 처리되는 user를 말한다. ("guestgroup"을 참조 하면 더 많은 정보를 얻을수 있다.)

<addrglob>는 도메인네임 또는 ip address로 설정을 하며, 슬래쉬("/") 로 시작을 하는 file 이름일수도 있다. 이 파일은 address:netmask 또는 address/cidr의 형식과 같은 추가 주소를 포함한다.

<addrglob> 앞에 "!"를 위치시키면, 예를 들어 class rmtuser real !*.example.com rmtuser class처럼 example.com 도메인 외에서 접근할수 있는 실제 유저를 지정 할수 있다.

2.3.3 deny <addrglob> <message_file>

<addrglob>와 비교하여 매치도는 host의 접근을 거절하며 <message_file> 에서 지정할 file의 내용을 출력한다. <addrglob>는 nameserver에 등록되어 있지 않은 site들의 접속을 거부하기 위한 nameser의 역할을 하며 <addrglob>와 같이 슬래쉬("/")로 시작하는 file의 이름을 지정할수도 있으며 이 파일에는 address:netmask 또는 address/cidr의 형식과 같은 추가 주소를 포함한다.

2.3.4 User & Group

guestgroup <groupname> [<groupname> ...]

guestuser <username> [<username> ...]

realgroup <groupname> [<groupname> ...]

realuser <username> [<username> ...]

REAL user가 <groupname>의 한 member라면, guestgroup을 위한 session은 anonymous FTP와 같이 정확하게 설정되어야 한다. 다시 말해, chroot()가 실행되어 져야 하며, USER와 PASS 명령이 제공되어져야 한다. <groupname>은 /etc/group에 존재하는 group이어야 한다.

user의 home directory는 anonymous FTP가 그러한 것 처럼 정확하게 설정 되어야 한다. passwd entry의 home directory field는 두개의 directory 들로 나뉘어져 있다. 첫번째 field는 chroot(2)가 부르는 인자가 될 root directory이다. 두번째 반은 root directory로 연관된 user의 home directory이다. 두 디렉토리의 구분은 "/./"로서 한다.

예를 들어 /etc/passwd에서, real entry:

guest1:<passwd>:100:92:Guest Account:/ftp/./incoming:/etc/ftponly guest1이 log in을 성공적으로 수행했을때 ftp server는 chroot("/ftp") 를 한다음 chdir("/incoming") 을 할 것이다. guest user는 anonymous FTP user가 그러하듯이오직 /ftp 하위의 directory 구조에 접근이 가능하다. (guest1에게는 /로서 보이며 작동한다.)

group name은 이름이나 숫자 ID로 지정되어야 한다. 숫자로 된 group ID를 사용하기 위해서는, 숫자 이전에 "%"를 위치시켜야 한다. 모든 goup을 나타내는 asterisk(*)-를 사용하는 것 처럼 영역을 지정할수도 있다.

guestuser는 user name(또는 숫자 ID)을 사용하지 않는 것을 제외하고는 guestgroup처럼 작동한다.

realuser와 realgroup은 동일한 문법을 가지지만, guestuser와 guestgroup의 영향과는 반대이다. relauser와 realgroup은 원격 접속 user가 guest로 결정 되어지는 것이 아닐때 real user 접속을 허락한다.

예를 들어:

guestuser * realgroup admin

와 같이 설정을 했을때 유일하게 real user 접근을 허락받은 admin group에 있는 user들을 제외 하고는 모든 non-anonymous user들은 guest로 취급이 되어지기 때문이다.

2.3.5 nice <nice-delta> [<class>]

원격 user가 <class>에 정의된 멤버라면 지정된 <nice- dalta> 의해 ftp server process의 process nice value를 조절 한다. 만약 <class>가 지정되지 않으면, ftp server process nice value 는 기본으로 지정된 <nice-delta>를 사용한다. 이 기본 nice value 조정은 ftpaccess file에 존재하는 class-specific "nice" 지시자에 대해 어떤 class에도 속하지 않는 user들을 위해 server process의 nice value를 조정하기 위하여 사용되어 진다.

2.3.6 defumask <umask> [<class>]

원격 user가 class에 정의된 멤버라면, daemon에 의해 만들어진 file들의 umask를 지정한다. <class>가 지정되지 않으면, 어떤 것도 지정되지 않은 class들을 위해 umask는 기본값으로 사용이 된다.

2.3.7 tcpwindow <size> [<class>]

data connection에 대한 TCP window size를 지정한다. 이것은 network traffic을 조정하기 위해 사용할수 있다. 예를 들어 느린 PPP dialin link들은 효율을 높이기 위해 더 작은 TCP window들이 필요하게 된다. 이것에 대해 잘 모르겠다면 그냥 나두도록 한다.

2.3.8 keepalive <yes|no>

data socket을 위하여 TCP SO_KEEPALIVE를 지정하여 네트워크를 끊는 것을 조절할수 있다. Yes: 는 사용을 하는 것이며 No는 system의 기본값을 사용 하겠다는 것을 의미 한다(보통 off이다). 당신은 아마도 이것을 셋팅하는 것을 원할것이다.

2.3.9 timeout accept <seconds> timeout connect <seconds> timeout data <seconds> timeout idle <seconds> timeout maxidle <seconds> timeout RFC931 <seconds>

다양하게 timeout을 지정할수 있다.

Accept (기본 120초): 데몬이 얼마나 incoming(PASV) data 접속을 기다릴지를 설정한다.

Connect (기본 120초): 데몬이 얼마나 outgong(PORT) data 접속을 이루기 위해 위해 시도 하는 것을 기다릴지를 설정하며, 실제 접속 시도에 영향을 미친다. 데몬은 여러번 시도를 하게 되며, 완전히 접속이 되기 전까지 각각의 시도 사이에 텀을 가지게 된다.

Data (기본 1200초): 데몬이 어떤 실제 data접속을 이루기 위해 기다리는 시간을 지정한다. 원격 접속자들이 클라이언트를 통해 아주 작은 데이타 큐와 느린 결합을 가질수 있도록 길게 잡아 줘야 한다.

Idle (기본 900초): 데몬이 새로운 명령을 수행할때 까지 얼마나 기다릴지를 설정한다. 기본으로 ftp 데몬을 실행할때 -a 옵션을 사용하여 지정할수 지정할수 있으며 이때에는 설정파일에서의 값은 무시되어 진다.

MaxIdle (기본 1200초): SITE IDLE 명령은 원격 유저가 idle 시간 초과를 통하여 높은 값을 형성하도록 한다. 이것은 클라이언트가 요청하는 것들을 제한하는 최대값을 지정한다. ftpd 시작시에 -A 옵션으로 지정할수 있으며 이때에는 설정파일에서의 값은 무시되어 진다.

RFC931 (기본 10초): 데몬이 전체 RFC931(AUTH/ident) 소통을 허락할 최대 사간을 지정한다. 0으로 설정을 하면 데몬이 이 프로토콜을 사용하는 것을 완전히 막는다. RFC931을 통해 얻는 정보들은 시스템 로그에 기록이 되고, 실제로 어떠한 인증에도 사용이 되지는 않는다.

2.3.10 file-limit [<raw>] <in|out|total> <count> [<class>]

지정된 class에서 user가 전송할수 있는 data file들의 수를 제한한다. limit는 in, out 또는 둘다 file안에 위치한다. class가 지장되지 않았다면, limit는 limit가 지정되지 않은 class들을 위한 기본값으로 사용된다. 부가적으로 raw parameter는 단지 date file들 보다는 total traffic을 제한하는데 적용을 한다.

2.3.11 data-limit [<raw>] <in|out|total> <count> [<class>]

class에 지정된 user가 전송하는 data를 byte 단위로 제한한다. limit는 in, out 또는 둘다를 byte를 기준으로 한다. class를 지정하지 않으면, limit 는 limit를 지정하지 않은 class들을 위한 기본값으로 사용된다. limit를

지정을 하면 지정한 이상을 초과하여 전송을 할수 없다. 하지만 진행중인 전송에는 적용이 되지 않는다. 부가적으로 raw parameter는 단지 date file들 보다는 total traffic을 제한하는데 적용을 한다.

2.3.12 limit-time {*|anonymous|guest} <minutes>

session이 가질수 있는 총 시간을 제한한다. 기본적으로 제한이 걸려있지 않다. real user들은 제한을 받지 않는다.

2.3.13 guestserver [<hostname>]

anonymous 또는 guest 접속을 위해 사용되어 지는 host들을 조정한다. <hostmane> 없이 사용을 한다면, 모든 guest 나 anonymous 접속은 접근을 거부당한다. 하나 이상의 <hostname>을 지정해야 한다. guest와 anonymolus 접속은 machain들의 이름에 기반해서 허락되어 진다. 접근이 거절되면, user는 먼저 <hostname> list에 등록이 되어져야만 사용이 가능하다.

2.3.14 limit <class> <n> <times> <message_file>

<class>에서 접근을 하는 <n> user들을 <times> 시간에 제한하며, user가 접근을 거절 당할때 <message_file>을 출력한다. Limit check는 login시에만 수행된다. 다중 "limit" 명령이 현재의 session에 적용이 된다면 먼저 설정된 것이 사용되어 진다. limit 정의가 빠지거나 limit가 -1로 설정이 되면 unlimit로 작동을 한다. <times>는 UUCP L.sys file에서의 time과 같은 형식이다.

2.3.15 noretrieve [absolute|relative] [class=<classname>] ... [-] <filename> <filename> ...

설정된 file들의 상대적 기능을 제한한다. file들이 절대 경로 설정을 사용 ("/" character로 시작하는 것 처럼) 한다면, 이 file들은 얻을수 없는 것으로 표기가 되어진다. 다시말해 filename과 매치되는 모든 file들은 전송이 거절된다. 예를들어

noretrieve /etc/passwd core

설정은 /etc/passwd file을 얻어갈수 없게 한다. 이에 반해 이것이 /etc에 있지 않는 다면 "passwd" file을 전송 받아 갈수가 있다. 다른 면에서 "core"라는 이름을 가진 file은 어디서도 전송을 받을수가 없다.

슬래쉬("/")로 끝나는 절대 경로는 그 directory안의 모든 file들을 전송 할수 없게 표기되어 지는 것을 의미한다.

<filename>은 하나의 file 또는 일반적인 표현으로서 정의되어 진다.

부가적인 첫번째의 매개변수는 현재의 chroot'd 환경에 절대적 또는 상대적으로 해석되어지는 이름들인지 아닌지를 선택한다. 기본은 slash로 시작하는 절대경로로 해석을 한다.

noretrieve 제한은 특정 class들의 member들을 기반으로 한다. 어떤 class가 지정되어져 있고 현재 user가 어떤 주어진 class들의 member들이라면 지정된 file들은 상대적인 것이 아니다.

2.3.16 allow-retrieve [absolute|relative] [class=<classname>]... [-] <filename> ...

noretrieve에 의해 거절되어진 file들의 복구를 허락한다.

2.3.17 loginfails <number>

<number> login 실패후에, "repeated login failusers" message를 출력한 후, FTP 연결을 종료한다. 기본값은 5이다.

2.3.18 private <yes|no>

user login 후, SITE GROUP과 SITE GPASS 명령은 강화된 접속 group과 연결된 password를 지정 하기 위해 사용되어 진다. group name과 password가 지정되면, user는 setgid()를 통해서 group 접근 file /etc/ftp/groups에 정의된 group의 member가 된다.

2.3.19 group access file

group access file의 형식은 access_group_name:encrypted_password:real_group_name access_group_name은문자 숫자식(alphanumeric)과 구둣점(punctuation) 으로 이루어진 임의의 문자열이며, encrypted_password는 /etc/passwd 와 같이 정확하게 crypt(3) 를 통해서 암호화 되어진 password이다. real_group_name 은 /etc/group 에 속해있는 유효한 group 이름이다.

주의:anonymous FTP user들에 대한 작업을 하기 위하여 이 option들을 통해 ftp server는 /etc/group 을 계속 참고를 하며, group access file은 memory에 load가 되어져 있어야 한다. 이것은 (1) ftp server는 additional file descriptor open을 가져야 하며, (2) necessary password들과 접근 권한들은 FTP session의 지속을 위해 SITE GROUP을 통해 정적으로 user들에게 주어 진다는 것을 뜻한다.만약 access group들 과/또는 password를 변경하기 위해서는 작동하고 있는 모든 FTP server들을 죽여야 한다.

2.4 정보에 관한 활용

2.4.1 greeting full|brief|terse greeting text <message>

remote user가 login 하기 전에 얼마나 많은 정보를 보여줄지를 설정할수 있다. "greeting full"이 기본이며, hostname과 daemon version을 보여준다. "greeting brief"는 hostname을 보여준다. 비록 full이 기본이지만 brief도 많이 사용되어 진다.

원한다면 "text" 형태로도 지정을 할수가 있다. <message>는 어떠한 문자열도 사용할수있다. whitespace(공백문자와 tab)은 하나의 single space로 변환된다.

2.4.2 banner <path>

banner는 user가 username/password를 입력하기 전에 출력이 된다는 것을 제외하고는 message 명령과 유사하게 작동을 한다. <path>는 anonymous FTP directory 의 base(/home/ftp)가 아니라 real system root를 기준으로 한다.

경고: 이 명령을 사용하는 것은 FTP server의 사용을 표시하는 것으로 부터 좋지 않은 의도의 FTP client들을 완전하게 막을수 있다. 모든 client들이 multi-line 응답들을 조정할수 있는 것은 아니다. (어떻게 banner들이 출력 되어지는지)

2.4.3 hostname <some.host.name>

ftp server의 기본 host name을 정의한다. 이 string은 magic cookie %L을 사용할 때마다 greeting message에 출력이 되어 진다. virtual server들의 host name은 이 값을 덮어쓰게 된다. 지정을 하지 않으면, local machine의 기본 host name이 사용되어 진다.

2.4.4 email <name>

ftp main 관리자의 email address를 정의한다. 이 string은 magic cookie %E를 사용할때 마다 출력이 되어 진다.

2.4.5 message <path> {<when> {<class> ...}}

<path>와 함께 file을 지정하며 user가 login을 할때나 working directory를 변경할때 ftpd가 user에게 이 file의 내용을 출력하게끔 한다. <when> parameter는 "LOGIN" 또는 "CWD=<dir>"을 이용한다. <when>이 "CWD=<dir>"이면 <dir>에는 공지를 보여줄 새로운 기본 directory를 지정을 한다.

<class>는 부가적으로 사용이 되어 지며, 오직 특정 class의 member 들에게 출력이 되어질 message를 지정을 한다. 하나이상의 class가 지정되어 질수 있다.

readmi file에서 지정된 text string로서 cookie를 대체하기 위해 "magic cookie"를 사용할수가 있다.

%T local time (form Thu Nov 15 17:12:42 1990)

%F free space in partition of CWD (kbytes) [모든 system에서 적용되지는 않음]

%C 현재 작업중인 directory

%E ftpaccess 에서 정의한 admin의 Email address

%R 원격 host name

%L local host name

%u RFC931 인증을 통해 결정된 username

%U login time때 주어진 username

%M 해당 class의 최대 접속자수

%N 해당 class에서의 현재 접속자 수

%B disk block들에 할당되어진 절대적 limit

%b disk block들에 할당되어진 limit

%Q 현재 block 수

%I inode (+1)에 할당된 최대 값

%i 할당된 inode limit

%q inode에 할당된 현재 값

%H excessive disk use 에 대한 시간 제한

%h texcessive files에 대한 시간 제한

ratios:

%xu 업로드 bytes

%xd 다운로드 bytes

%xR 업로드/다운로드 비율 (1:n)

%xc Credit bytes

%xT 시간 제한 (분)

%xE Elapsed time since login (minutes)

%xL 남은 시간

%xU 업로드 한계

%xD 다운로드 한계

이 message는 user들을 귀찮게 하는 것을 피하기 위하여 오직 한번만 출력이 된다. 메세지들이 익명 FTP user에 의해서 수행되었을때 <path>는 익명 FTP directory tree의 root로 변경이 됨을 기억해야 한다.

2.4.6 readme <path> {<when> {<class>}}

ftp가 login시나 file들이 존재하고 그 file들의 date가 변경된 working directory로 이동을 할때 user들에게 공지할 file들을 <path>로서 정의 한다. <when> parameter는 "LOGIN" 또는 "CWD=<dir>" 중에 하나를 선택한다. <when>이 "CWD=<dir>" 이면, <dir>은 공지가 실행될 새로운 기본 directory를 지정한다. message는 user들을 귀찮게 하는 것을 피하게 하기 위하여 오직 한번만 출력이 될것이다. README message들이 익명 FTP user에 의해 수행이 될때, <path>는 익명 FTP directory tree의 root로 변경이 됨을 기억해야 한다.

<class> option 지정은 message들이 오직 특정 class의 member 들에게만 출력이 되어지도록 할수 있다. 하나 이상의 class가 지정될수 있다.

2.5 로그 활용

2.5.1 log commands <typelist>

user들에 의해 개별적인 명령의 logging을 가능케 한다. <typelist>는 "anonymous", "guest", "real" 이라는 keyword들의 list를 쉼표(comma) 로서 분리하여 지정할수 있다. "real" keyword가 포함되어 있다면, logging은 real account로 접근하기 위해 FTP를 사용하는 user들을 위해 작동을 할 것이다. 그리고 "anonymous" keyword가 포함되어 진다면, logging은 anonymous FTP를 사용하는 user들을 위해 작동할 것이다. "guest" keyword는 guest 접근 계정들과 매치가 된다. (더 많은 정보를 얻기 위해서는 "guestgroup"을 참조하라)

2.5.2 log transfers <typelist> <directions>

real user나 anonymous user들 모두를 위한 file 전송의 logging을 가능케 하며, inbound와 outbound를 분리하여 logging을 할수가 있다. <typelisst>는 "anonymous", "guest", "real"과 같은 keyword의 list들을 쉼표(comma)로서 구분을 한다. "real" keyword가 포함되어 있다면, logging은 real account로 접근하기 위해 FTP를 사용하는 user들을 위해 작동을 할 것이다. 그리고 "anonymous" keyword가 포함되어 진다면, logging은 anonymous FTP를 사용하는 user들을 위해 작동할 것이다. "guest" keyword는 guest 접근 계정들과 매치가 된다. (더 많은 정보를 얻기 위해서는 "guestgroup"을 참조하라) <directions>은 "inbound"와 "outbound" 두개의 keyword를 쉼표로서 구분을 하여 지정을 하며, 이 option으로서 server로 보내고 받는 file들을 위한 전송 log를 기록한다.

2.5.3 log security <typelist>

real, guest, anonymous user들을 위한 보안 rule들(noretrieve, .notar, 등)을 어기는 것들의 log를 기록하도록 한다. <typelist>는 "anonymous", "guest", "real" 이라는 keyword들의 list를 쉼표(comma)로서 분리하여 지정할수 있다. "real" keyword가 포함되어 있다면, logging은 real account로 접근하기 위해 FTP를 사용하는 user들을 위해 작동을 할 것이다. 그리고 "anonymous" keyword가 포함되어 진다면, logging은 anonymous FTP를 사용하는 user들을 위해 작동할 것이다. "guest" keyword는 guest 접근 계정들과 매치가 된다. (더 많은 정보를 얻기 위해서는 "guestgroup" 을 참조하라)

2.5.4 log syslog+xferlog

incoming, outgoing 전송들에 대한 logging message들을 syslog로 향하게 한다.

2.6 여러가지 활용

2.6.1 alias <string> <dir>

directory에 대한 alias와 <string>을 정의한다. 논리적 directory의 개념을 추가하여 사용할수 있다. 이 옵션이 없으면 메세지들은 xferlog에 기록된다.

syslog+xferlog는 system log와 xferlog 양쪽에 메세지를 기록한다

2.7 Upload/Download 비율

이 명령들을 사용하기 위해서는 WU-FTPD 컴파일 시에 –enable-ratios 옵션을 줘야 한다.

2.7.1 ul-dl-rate <rate> [<class> ...]

업로드/다운로드 비율을 지정한다. (1:rate) ftp user가 1 byte를 업로드 할때 <rate> byte를 얻게 된다. 기본값으로는 비율이 없다.

2.7.2 dl-free <filename> [<class> ...]

<filename> file은 다운로드가 ratio에 적용받지 않는다.

2.7.3 dl-free-dir <dirname> [<class> ...]

<dirname> 디렉토리에 있는 모든 파일들은 ratio에 적용을 받지 않는다. dl-free and dl-free-dir는 chroot() 환경이 아닌 시스템 root를 사용하여 제한을 하게 된다는 것을 주의해야 한다.

2.8 여러가지 활용

2.8.1 alias <string> <dir>

directory에 대한 alias와 <string>을 정의한다. 논리적 directory의 개념을 추가하여 사용할수 있다.

예를 들어:

alias rfc: /pub/doc/rfc

은 user들이 명령어 "cd frc:"에 의해 어떤 directory로 부터 /pub/doc/rfc로 access하는 것을 가능케 한다.

2.8.2 cdpath <dir>

cdpath안에 entry를 정의한다. 이것은 directory 변경시에 사용되어 지는 search path를 정의한다.

예를 들어:

cdpath /pub/packages cdpath /.aliases

은 user들이 /pub/packages 또는 /.aliases directory들 하위에 있는 어떤 directory로 직접 cd를 하는 것을 허락한다. search path는 ftpaccess file에 기록된 line들의 순서에 의해 정의되어진다.

user들이 명령을 실행하면:

cd foo

directory들은 아래의 순서를 통해 찾아 질것이다.

./foo an alias called "foo" /pub/packages/foo /.aliases/foo

cd path는 오직 cd 명령어로서만 가능하다. 만약 많은 수의 alias들을 가지고 있다면 아마 user들에게 사용가능하게 만들고 싶은 모든 곳으로 링크를 하는 것으로 alias들을 설치하기를 원할것이다.

2.8.3 compress & tar

compress <yes|no> <classglob> [<classglob> ...] tar <yes|no> <classglob> [<classglob> ...]

<classglob>와 매치하는 class를 위해 compress와 tar 사용을 가능하게 한다. 실제 전환은 외부 file FTPLIB/ftpconversions에 의해 정의가 되어 진다.

2.8.4 shutdown <path>

<path>에 file이 지정이 되면, 서버는 정기적으로 이 file의 내용을 확인을 하여 셧다운을 하도록 한다. 셧다운 계획이 존재하면 user는 서버로 부터 이에 대한 통보를 받게 된다. 셧다운 전의 지정된 시간 이후에는 새로운 접속이 거절되며, 셧다운 이전의 지정된 시간에는 현재 접속자들의 연결이 해제된다. <path>에 지정된 파일의 구조는 아래와 같다 :

<연도> <월> <일> <시> <분> <거절_offset> <해제_offset> >

<연도> 1970년도 이후로 지정을 한다.

<월> 1-12월을 0-11로 지정을 한다.

<일> 0-23

<분> 0-59

<거절_offset> 와 <해제_offset> 은 셧다운을 하기 전에 새로운 접속을 거절하는 것과 현재 존재하는 접속을 해제하는 offset을 HHMM 형식으로 지정을 한다. 0120은 1시간 20분을 의미한다.

<text>는 "message"의 rule들을 따르며, 아래에 나열되어 있는 추가적인 magic cookie를 사용할수도 있다.

%s 시스템이 셧다운 되는 시간

%r 새로운 접속이 거부되는 시간

%d 현재 사용자들이 강제 logout되는 시간

모든 시간들은 ddd MMM DD hh:mm:ss YYYY 의 형태로 사용이 된다. 설정 file에는 오직 하나의 "shutdown" 명령만 가능하다.

설정 file에서의 shutdown 명령은 외부 프로그램인 ftpshut(8)을 자동으로 사용을 하게 된다.

2.8.5 daemonaddress <address>

이 값이 지정이 되어 있지 않으면, 서버는 모든 IP address에서의 접속에 귀를 귀울이게 된다. 반면에 지정이 되어 있으면 오직 지정된 IP address 에만 귀를 귀울이게 된다.

이 절의 사용은 안하는 것이 좋다. 이것은 하나의 site만을 지원할때 추가가 되어진다. 이것은 virtual hosting 설정을 무시하며, 구문은 아마도 daemon의 다음 버젼에서는 변화할것 같다.

2.8.6 virtual <address> <root|banner|logfile> <path>

virtual ftp server를 가능하게 한다. <address>는 virtual server의 ip address를 지정한다. 두번째 인자중 root는 virtual server를 위한 ftproot의 경로를 지정을

하며, banner 는 virtual server에 접속을 할때 user에게 출력을 할 내용의 경로를 지정을 하며 logfile 은 virtual server를 위한 전송을 기록하기 위한 file의 경로를 지정을 한다. 만약 logfile 를 지정하지 않으면 기본적인 ftp logfile이 사용이 되어진다. virtual server들에 적용이 되어 지는 message file들의 문법과 permission들은 다른 message file에서 사용하는 것과 같다.

주의: OS에서 이 요소가 지원이 안될수도 있다. 이것은 BSD/OS, Solaris 2.X 와 Linux 에서 테스트가 되어졌다.

<address>는 IP number보다는 hostname으로 지정이 되어져야 한다. 만약 FTP session이 시작 되어질때 DNS check가 불가능하다면 hostname이 match가 되어 지지 않으므로 이때는 사용을 하지 말아야 한다.

나(번역자 ^^)의 경험으로는 hostname보다는 ip address로 지정을 하는 것이 좋다. 특히 ip address 하나로 name-based virtual server를 운영하기를 원한다면 wu-ftpd 에서는 지원을 하지 않는 다는 점을 주의하도록 하자.

2.8.7 virtual <address> <hostname|email> <string>

환영 message와 status 명령에 hostname을 보여주도록 설정을 한다. 또한 message file과 HELP 명령에서 주어진 <string> 에 email address를 사용 하도록 한다.

2.8.8 virtual <address> allow <username> [<username> ...]

virtual <address> deny <username> [<username> ...] 일반적으로, real과 guest 유저들은 이들이 guest들이고 virtual root로 chroot가 지정이 되기 전까지는 virtual server로 접근이 허락되지 않는다. virtual allow line들의 list에 있는 user 들은 접근을 허락된다. username에 "*"를 지정하면 모든 user들이 접속을 허락한다는 의미로 사용이 되어진다. virtual deny 절들은 virtual allow 절들 이후에 진행이 되며, 모든 user들이 허락되어 졌을때 deny access를 지정을 하기 위하여 사용되어 진다.

2.8.9 virtual <address> private

일반적으로, 익명 사용자들은 virtual server에 log가 허락되어 진다. 이 option은 그들의 접근을 거절하는데 사용을 한다.

2.8.10 virtual <address> passwd <file>

가상 도메인마다 다른 패스워드 파일을 사용할수 있다. 이 옵션을 사용하기 위해서는 컴파일시에 –enable-passwd(또는 다른 PASSWD)를 주고 컴파일을 해야 한다.

2.8.11 virtual <address> shadow <file>

가상 도메인마다 다른 쉐도우 파일을 사용할수 있다. 이 옵션을 사용하기 위해서는 컴파일시에 –enable-passwd(또는 다른 PASSWD)를 주고 컴파일을 해야 한다.

2.8.12 defaultserver

defaultserver deny <username> [<username> ...]

defaultserver allow <username> [<username> ...]

일반적으로, 모든 user들은 default FTP server (virtual FTP server가 아닌)로의 접근이 허락되어 진다. defaultserver 는 특정 user들의 접속을 거부를 하는데 사용을 한다; "*"를 지정을 하면 모든 user들의 접근을 거절 한다. 특정한 user들은 defaultserver allow를 사용함으로서 접근이 가능 하게 된다.

2.8.13 defaultserver private

일반적으로, 익명 user들은 virtual FTP가 아닌 기본 FTP server로 접근이 허락되어 진다. 이 문장은 익명 접근을 거부하는데 사용을 한다.

virtual과 defaultserver의 allow, deny, private절은 어떤 user들이 어떠한 FTP server들에 접근이 허락되어 지는 것을 조절할수 있다는 의미를 제공한다.

2.8.14 passive address <externalip> <cidr>

PASV 명령으로 온 응답으로 리포트된 주소의 조절을 허락한다. 어떤 control connection이 <cidr> 이 요구하는 passive data connection (PASV)와 매치를 할때 <externalip> 주소가 리포트 되어진다. 주의: 이것은 daemon이 실제로 귀를 귀울이는 주소를 변화 시키는 것은 아니다. 오직 client로 리포트 되는 주소일 뿐이다. 이 요소는 IP-renumbering firewall들 뒤에서 daemon들이 정확하게 동작하게 하는 것을 허락을 한다.

예를 들어:

passive address 10.0.1.15 10.0.0.0/8

passive address 192.168.1.5 0.0.0.0/0

모든 곳으로 부터의 접속이 192.168.1.5에 귀를 귀울이고 있는 동안 A class의 network 10으로 부터의 client의 접속은 passive connection 이 ip address 10.0.1.15에 귀를 귀울이고 있다는 것을 의미한다.

Multiple passive address들은 complex의 조정으로 정의가 되거나, multi-gateway 또는 network들의 조정으로 정의가 되어 진다.

2.8.15 passive ports <cidr> <min> <max>

passive data connection을 통해 사용되어 지는 TCP port number들의 control을 허락한다. control connection이 <min> 에서 <max> 까지의 영역에 있는 <cidr> 포트와 매치된다면, daemon이 귀를 귀울이는 것을 통해 마구 잡이로 선택이 될 것이다. 이 요소는 remote client들이 안전장치가 되어 있는 network에 접근을 할때 사용을 하는 port들을 제한 하는 firewall들을 허락한다.

<cidr> 은 machine address와는 반대되는 slash뒤에 4자리로 표기되고 또는 각 자리의 bit의 합으로 표시되는 network address를 통해 표시된다. 예를 들어, 10대의 A class로 예약된 대역을 사용한다면, netmask 255.0.0.0 대신 CIDR "/8"을 사용할수 있으며 network를 10.0.0.0/8 로 표현을 할수가 있다.

2.8.16 pasv-allow & port-allow

pasv-allow <class> [<addrglob> ...]

port-allow <class> [<addrglob> ...]

일반적으로 데몬은 지정지 않은 주소에서는 PORT 명령을 허락하지 않는다. 그리고 이것은 다른 주소로 부터 PASV 접속을 허락하지 않는다는 것을 의미한다.

port-allow 절은 PORT 명령이 주어진 유저 class로 지정된 주소의 리스트들을 규정한다. 이 주소들은 비록 클라이언트쪽의 IP address가 매치가 되지 않는다 해도 허락이 된다.

pasv-allow 절은 데이터 접속을 만드는 유저 클래스로 지정된 주소 리스트를 규정한다. 이 주소들은 비록 클라이언트쪽의 IP address가 매치가 되지 않는다 해도 허락이 된다.

2.8.17 lslong, lsshort, lsplain

lslong <command> [<options> ...]

lsshort <command> [<options> ...]

lsplain <command> [<options> ...]

lslogn, lsshort, lsplain 절은 commnad와 options들을 열거하여 directory listing을 사용하는 것을 허락한다. option들은 공백을 포함할수 없으며, 기본적인 것들은 이 절들을 통해 일반적으로 조정이 된다는 것을 주의해야 한다; 절대적으로 필요할 경우에만 lslong, lsshort 또는 osplain 을 사용한다.

2.8.18 mailserver <hostname>

FTP 데몬이 어떠한 upload가 발생했을 경우 메일을 보낼 메일 서버를지정한다. 한줄에 하나씩 써서 여러개의 메일 서버를 지정할수 있다; 데몬은 하나의 메세지가 받아질 까지 각 업로드 통지의 배달을 시도하게 된다. 메일 서버를 지정하지 않으면 로컬 호스트로 보내게 된다. 이 옵션은 익명 업로드의 공지를 의미한다. (incmail을 참조하라)

2.8.19 incmail, virtual incmail, defaultserver incmail

incmail <emailaddress>

virtual <address> incmail <emailaddress>

defaultserver incmail <emailaddress>

익명 업로드시 통지를 할 메일 어드레스를 기록한다. 여러개를 지정하여 각각 통지를 받을수가 있다. 지정하지 않으면, 통지를 보내지 않는다.

가상 호스트에 대해 지정을 하면, 오직 이 주소만이 익명 업로드에 대한 통지를 받게 된다. 반대로 지정하지 않으면 전체 주소로 통지가 보내진다.

Defaultserver 주소는 오직 FTP session이 하나의 가상 호스트로만 사용되지 않을 경우에만 적용된다. 이 경우에는 기본 익명 영역에 대해서만 통지를 받게 되며 통지를 지정하지 않은 가상 호스트들에게는 통지를 볼수가 없다.

2.8.20 mailfrom, virtual mailfrom, defaultserver mailfrom

mailfrom <emailaddress>

virtual <address> mailfrom <emailaddress>

defaultserver mailfrom <emailaddress>

익명 업로드 통지를 위한 보내는 사람의 메일 주소를 지정한다. 하나의 주소는 지정이 되어 있어야 한다. mailfrom이 적용되어 있지 않다면, 메일은 기본 메일박스 이름인 "wu-ftpd"로 메일을 보재게 된다. 통지에 답장을 시도 하는 것을 피하기 위해서는 또는 반송이 되는 것을 막기 위해서, mailfrom 주소를 반드시 지정하는 것이 좋다.

2.9 권한 활용

2.9.1 chmod delete overwrite rename umask

chmod <yes|no> <typelist>

delete <yes|no> <typelist>

overwrite <yes|no> <typelist>

rename <yes|no> <typelist>

umask <yes|no> <typelist>

특정 function들을 수행할수 있는 권한들을 허락하고 불허한다. 기본적으로, 모든 user들에게 허락이 되어진다.

<typelist>는 keyword "anonymous", "guest", "real", "class=" 들을 컴마(",")로서 구분하여 나열한다. "class="를 나타낼때는, classname 이 꼭 따라와야 한다. 어떤 "class=" 를 나타낼때, <typelist> 제한은 오직 class의 user들에게만 적용이 된다.

2.9.2 passwd-check <none|trivial|rfc822> (<enforce|warn>)

anonymous ftp를 통해 server에 접근을 할때 level과 password check 의 형태를 정의한다.

none password check를 하지 않는다.

trivial password에 "@"이 반드시 포쪘좟되어 있는지를 check한다.

rfc822 password가 rfc822에 의거한 주소로 되어 있는지를 확인한다.

warn user에게 경고는 하되, login은 허락한다.

enforce user에게 경고를 하며 login은 허락하지 않는다.

2.9.3 deny-email <case-insensitive-email-address>

e-mail 주소를 효력이 없는 요소로서 검토를 하게 한다. 만약 passwd-check가 enforce로 셋팅되어 있으면, 익명 user들은 이 주소를 password로 사용하여 login할수가 없다. 이것을 이용하여 IEUser@ or mozilla@ 와 같은 어리석을 WWW brosers가 사용을 하는 거짓된 주소들을 사용하는 user들을 막을수가 있다. (이것을 사용함으로서, ftp를 위해 WWW browser를 사용하는 user들을 막는 것에 대해 고심할 필요가 없다. 단 그들이 사용을 하는 browser를 정확하게 setting을 해야 한다.) 오직 한 line당 하나의 주소만 설정이 되지만, 원하는 만큼의 deny-email address를 가질수가 있다.

2.9.4 path-filter <typelist> <mesg> <allowed_charset> {<disallowed regexp> ...}

<typelist>의 user들을 통해, path-filter는 정규 표현식을 filename으로 할지 안할지를 정의한다. 다중으로 정규 표현식들을 허락하지는 않는다. 만약 filename이 정규 표현식의 척도와 매치하지 않는 다면, <mesg>가 user 들에게 출력이 되어 질 것이다. 예를 들어:

path-filter anonymous /etc/pathmsg ^[-A-Za-z0-9._]*$ ^\. ^-

는 익명 사용자들을 통한 모든 upload filename 들은 반드시 A-Z, a-z, 0-9, "._- "으로 으로 이루어 져야 하며 시작시에 "."와 "-" 는 사용할 수가 없다는 것을 정의한다. 만약 filename이 위의 내용과 부합하지 않는다면 /etc/pathmsg 이 user들 에게 출력이 될것이다.

2.9.5 upload [absolute|relative] [class=<classname>]... [-] <root-dir> <dirglob> <yes|no> <owner> <group> <mode> ["dirs"|"nodirs"] [<d_mode>]

<dirlob>로서 upload를 허락하거나 허락하지 않을 directory를 지정한다.

upload를 허락한다면, 모든 file들은 <owner>와 <goupr>으로 소유권을 가질것이며, permissions들은 <mode>에 따른다. directory들은 가장 매치가 잘되는 원칙에 따른다.

예를 들어:

```
upload /var/ftp * no

upload /var/ftp /incomingyes ftp daemon 0666

upload /var/ftp /incoming/gifs yes jlc guest 0600 nodirs
```

이것은 /incoming 과 /incoming/gifs 에만 upload를 허락한다. /incoming 에 upload 된 file들은 ftp/daemon의 소유권을 가지며, 퍼미션은 0666을 가지게 된다. /incoming/gifs에 upload 되어진 file은 jlc/guest의 소유권을 가지며, 0600의 퍼미션을 가지게 된다. 여기서 <root-dir>은 passowrd file에서 "ftp" user에게 지정된 directory와 반드시 매치가 되어야 한다는 것을 명심해야 한다.

부가적으로 "dirs" 와 "nodirs" keyword는 mkdir 명령을 사용하여 어떠한 새로운 subdirectory를 만드는 것을 허락 하거나 허락하지 않는 것을 지정한다.

upload 명령을 사용할때, directory 생성은 default로 허락이 되어 진다는 것을 주의해야 한다. default 값을 off로 바꾸기 위해서는 이 config file에서 upload 명령을 사용하고 있는 line중 가장 윗줄에 user, group, mode를 지정해야 하며, "nodirs"가 반드시 뒤에 따라와야 한다.

directory 생성을 허가할때 부가적으로 <d_mode>라는 지시자를 사용할수 있으며 이것은 directory를 생성할 시의 direcotory permission을 지정한다. <d_mode>를 생략하면, permission은 <mode>를 따라가며, <mode> 마져 생략되어 있으면 0777이 된다.

upload keyword는 오직 <root-dir>의 (chroot()가 적용이 되는)home directory를 가지고 있는 user(즉 anonymous)에게만 적용이 된다. <root-dir>은 어떠한 home directory와 매치 시키기 위하여 "*" 로서 지정을 할수도 있다.

<owner> 와/또는 <group>은 어떤 upload file이나 directory 들이 그들이 만들어진 directory의 자신의 소유권으로서 생성을 시키고자 할 경우에는 "*" 로서 각각 지정을 할수도 있다.

부가적으로 첫번째 parameter는 현재 chroot 환경에 따라서 절대적으로나 상대적으로 해석하여 선택을 한다. 기본값으로는 <root-dir>을 절대값으로 해석을 한다.

한다면, 이 upload절은 오직 현재 user가 어떤 class의 member 일때 만 영향을 받는다.

서버에 업로드 파일을 허락하도록 설정을 하기 위해서는 upload.cofiguration.HOWTO 를 꼭 읽어 보기 바란다.

2.9.6 throughput <root-dir> <subdir-glob> <file-glob-list> <bytes-per- second> <bytes-per-second-multiply> <remote-glob-list>

remote hostname 또는 remote IP address가 comma로 분리된 <remote-glob-list>와 매치가 될때, <root-dir> 아래의 <subdir-glob>와 매치가 되는 subdir에서 comma로 구분된 <file-glod-list>를 통하여 다운로드에서 <byte- per-second>의 전송 처리량이 제한되는 file들을 지정할수 있다.

Entry들은 가장 부합되는 원칙에 매치가 되어진다.

예를 들어:

```
throughput /e/ftp * * oo - *

throughput /e/ftp /sw* * 1024 0.5 *

throughput /e/ftp /sw* README oo - *

throughput /e/ftp /sw* * oo - *.foo.com
```

이것은 defalut로 최대 전송량을 지정한다. 하지만 README라는 이름 지어지지 않은 e/ftp/sw/ 아래의 어떤 file들에 대해서 초당 1024byte로 download를 제한한다. domain foo.com의 도메인을 가진 네트웍에서 오는 remote host들은 예외로 항상 최대 전송량을 얻을수 있다.

매 시간 remote client들은 /e/ftp/sw 아래의 file을 제한 받으며, entry line과 매치가 되는 byte per second는 내부적으로 계수(여기서는 0.5)만큼씩 증가 되어진다. 그리고 remote client가 두번째 파일을 제한 할때, 이것은 512byte/s로 제공이 되며 세번째 시도시에는 254byte/s, 4번째 시도시에는 128byte/s 등으로 제한이 되어진다.

byte per second field의 "oo"는 전송량 제한을 하지 않는 것을 의미한다. 1.0 씩의 계수 증가나 "-" 는 매번 성공적인 전송후에 전송량의 변화가 없음을 의미한다.

여기서 <root-dir>은 password database에 있는 "ftp" user에게 지정 되어진 home directory와 반드시 매치가 되어야 한다는 것을 주의해야 한다. throughput(전송량) keyword는 오직 <root-dir>의 (chroot()가 적용이 되는) home directory를 가지고 있는 user(즉 anonymous)에게만 적용이 된다.

2.9.7 anonymous-root <root-dir> [<class>]

<root-dir> 은 anonymous user들의 chroot() path를 지정한다. anonymous-root 가 매치가 되지를 않으면, 전통적으로 내려오는 구문의 방법으로 "ftp" user의 home directory를 사용을 한다. <class>가 지정이 되지 않으면, 어떤 anonymous-root 지정이 되지 않은 anonymous user들의 root directory가 된다. 라인에 여러개의 class를 지정할수도 있다. user들을 위한 anonymous root가 선택이 되면, <root-dir>/etc/passwd file에 잇는 "ftp" user들의 home directory가 사용되어 지며, 최초의 directory와 system 전반적인 /etc/passwd의 "ftp" user들의 home directory는 사용이 되지 않는다.

예를 들면:

```
anonymous-root /home/ftp

anonymous-root /home/localftp localnet
```

는 모든 anonymous user들의 chroot()를 /home/ftp로 지정을 하며, 최조의 CWD는 이 home directory가 된다. 그러나 class localnet의 anonymous user들의 chroot()는 /home/localftp가 되며, 그들의 최초 CWD는 /home/localftp/etc/passwd 에 있는 "ftp" user들의 home directory로 부터 영향을 받게 된다.

2.9.8 guest-root <root-dir> [<uid-range>]

<root-dir>은 guest user들의 chroot() path를 지정한다. guest-root가 매치가 되지 않으면 전통적으로 내려오는 구문의 방법으로 user들의 home directory가 사용되어 진다. <uid-range>가 지정이 된 않으면, 어느 다른 guest-root가 지정이 되지 않은 guest user들을 위한 root directory가 된다. 한 라인에 여러개의 uid range들을 지정할수도 있다. user들을 위한 guest- root가 선택이 되면, <root-dir>/etc/passwd file에 있는 user들의 home directory가 사용이 되어지며, 최초의 directory와 system 전반적으로 사용이 되어지는 /etc/passwd의 home directory는 사용이 되지 않는다.

<uid-range>는 UID값의 숫자로 지정을 한다. range들은 dash에 의해 구분되어 지는 상,하 경계가 주어짐에 따라 지정되어 진다. 하계(lower bound)를 생략하는 것은 "all up to"를 뜻하며, 상계(upper bound)를 생략하는 것은 "all starting from"을 의미한다.

예를 들어:

```
guest-root /home/users

guest-root /home/staff %100-999 sally

guest-root /home/users/frank/ftp frank
```

는 모든 user들의 chroot()를 /home/users로 하고, /home/users/etc/passwd 에서 지정된 그들의 home directory 에서 시작하게 한다. range 100 부터 999까지에 포함되는 user들과 user sally는 /home/staff로 chroot()가 되어 지며, /home/staff/etc/passwd의 그들의 entry에로 부터 CWD가 영향을 받는다. single user frank는 /home/users/owner/ftp가 chroot()로 되며, CWD는 /home/users/owner/ftp/etc/passwd의 그의 entry로부터 영향을 받는다.

anonymous-root 와 guest-root를 위한 명령들은 매우 중요하다는 것을 주의해야 한다. user가 여러개의 구문에 중복되어 매치가 된다면, 오직 처음 것만 적용이 된다. <class> 나 <uid-range>가 없는 구문은 제외되며, 어떤 구문도 매치가되지 않을 경우에만 적용이 된다.

2.9.9 deny-uid deny-gid allow-uid allow-gid

deny-uid <uid-range> [...]

deny-gid <gid-range> [...]

allow-uid <uid-range> [...]

allow-gid <gid-range> [...]

이 절들은 UID와 GID 값으로 ftp server 로의 접근 거부를 지정한다. allow-uid 와 allow-gid 절은 거부와는 달리 uid/gid 를 통해 접근 허락한다. 이 체크들은 모든 다른 설정들 이전에 이루어진다. deny는 allow 이전에 체크가 된다. defalut로는 모두 접근을 허락을 한다. 모든 경우에서, 이것은 /etc/ftpusers file을 통한 필요성을 제거 할수 있다. 예를 들어:

```
deny-gid %-99 %65535

deny-uid %-99 %65535

allow-gid ftp

allow-uid ftp
```

anonymous "ftp" user/group을 제외한 Linux Box의 모든 특권을 가졌거나 특정한 user들과 group들의 ftp 접근을 거부한다. 많은 경우, 이것을 이용하여 /etc/ftpusers file의 역할을 대신할수 있만 이것은 /etc/ftpaccess file의 변경을 바라지 않을때 사용하기 위하여 존재를 한다.

ftpaccess file을 통해 single UID와 GID를 사용할때 이름이나 숫자 둘다 사용을 할수가 있다. 숫자를 사용하기 위해서는, 숫자 이전에

2.9.10 restricted-uid restricted-gid unrestricted-uid unrestricted-gid

restricted-uid <uid-range> [...]

restricted-gid <gid-range> [...]

unrestricted-uid <uid-range> [...]

unrestricted-gid <gid-range> [...]

이 절들은 real 또는 guest user들이 자신들의 home directory 이외의 FTP site 영역에 접근 하는 것을 조절한다. 이것은 guestgroup과 guestuser의 사용을 대신하는 것을 뜻하지는 않는다. 대신, guest들의 작용을 보완하는데 사용할수는 있다. unrestricted-uid와 unrestircted-gid 절은 restricted와는 달리 그들의 home directory들 이외의 directory에 user들의 접근을 허락한다.

이 절의 사용의 예는 그들의 사용경향을 보여준다. user "dick"의 home directory가 /home/dick 이고, "jane"이 /home/jane 이라고 가정을 하면 :

guest-root /home dick jane

restricted-uid dick jane

dick과 jane의 chroot'd가 /home일 동안, 그들의 home directory 들을 제한 받기 때문에 각각 다른 file들을 access 할수가 없다. Whereever possible, in situations such as this example, try not to rely solely upon the ftp restrictions. 다른 모든 ftp aceess 법칙에서, ftpaccess 설정의 작동을 보완하기 위해 directory와 file의 퍼미션을 사용하도록 노력도 해야 한다.

2.9.11 site-exec-max-lines <number> [<class> ...]

SITE EXEC 의 특징은 전통적으로 원격 client로 보내지는 line들의 출력의 수를 제한한다. 이 구문은 제한을 셋팅할수 있게끔 한다. 생략하면 20 line들로 제한이 된다. limit 0은 제한을 하지 않는다는 것을 의미한다; limit를 없애려고 한다면 조심해야 한다. 이 구문이 원격의 user class와 매치가 된면 limit가 바로 적용이 된다. 반면에 "*" class나 class가 주어지지 않은 구문 역시 사용되어 질수 있다. 예를 들어;

site-exec-max-lines 200 remote

site-exec-max-lines 0 local

site-exec-max-lines 25

Limits는 "remote" class의 user들에게 SITE EXEC (와 그결과 SITE INDEX) 로 부터 200 line을 출력하며, local class의 user들에게는 제한을 하지 않는다. 그리고 모든 다른 user들에게는 25 line의 제한을 적용한다.

2.9.12 dns refuse_mismatch <filename> [override]

원격 사이트의 forward와 reverse lookup이 맞지 않을때, FTP 세션을 거부하며, 메세지 파일과 같은 파일을 접근 유저에게 출력을 한다. 옵션으로 [override]를 지정을 할 경우에는 메세지를 출력한 후에 접근을 허락한다.

2.9.13 dns refuse_no_reverse <filename> [override]

원격 사이트가 DNS 항목에 들어 있지 않을 경우 FTP세션을 거부하며, 메세지 파일 과 같은 파일을 접근 유저에게 출력한다. 옵션으로 [override]를 지정을 할 경우에는 메세지를 출력한 후에 접근을 허락한다.

2.9.14 dns resolveroptions [options]

resolveroptions 옵션은 name server 옵션들을 피하는 것을 허락한다. 이 라인은 resolver(3) 의 문서처럼 플래그의 종류를 취한다. 부가적으로 + 나 - 에 의해 설정을 해 나갈수 있다. 예를 들어

dns resolveroptions +aaonly -dnsrch

는 aaonly 옵션을 활성화 하고(오직 믿을수 있는 응답들만), dnsrch 옵션 (도 메인 경로를 찾는것)은 비활성화 하게 된다.

2.10 파일

FTPLIB/ftpaccess

2.11 관련 항목

ftpd(8), umask(2), ftplog(5), ftpconversions(5), ftpshut(8)

제 3 절 ftpconversions

3.1 이름

ftpconversions - ftpd 변환 목록

3.2 설명

ftpd(8) 에 의해 알려진 conversions와 그들의 속성은 아래와 같이 구성된 ASCII file안에 저장되어 있다. file의 각 line은 콜론(:)으로 구분되어진 하나의 conversion. field 에 대한 설명을 보여준다.

%s:%s:%s:%s:%s:%s:%s:%s

1 2 3 4 5 6 7 8

Field Description

1 strip prefix

2 strip postfix

3 addon prefix

4 addon postfix

5 외부 명령

6 형식

7 옵션

8 설명

3.3 알려진 문제

conversions mechanism에서 strip prefix와 addon prefix field는 아직까지 지원되지 못한다.

3.4 파일

참조 ftpd(1), ftpaccess(5)

제 4 절 ftpcount

4.1 이름

ftpcount - 각 class의 현재 user수를 보여준다.

4.2 문법

ftpcount

4.3 설명

명령은 ftpaccess file에서 정의된 각 class에 대한 user의 수 또는 제한된 user의 현재 접속수를 보여준다.

4.4 관련 항목

ftpwho(1)

제 5 절 FTPD

5.1 이름

ftpd - DARPA 인터넷 파일 전송 프로토콜 서버

5.2 개요

ftpd [-d] [-v] [-l] [-ttimeout] [-Tmaxtimeout] [-a] [-A] [-L] [-i] [-o] [-pctrlport] [-Pdataport] [-q] [-Q] [-rrootdir] [-s] [-S] [-uumask] [-V] [-w] [-W] [-X]

5.3 설명

Ftpd 는 DARPA internet file 전송 프로토콜 server의 역할을 한다. server는 TCP protocol을 사용하며 'ftp" service로 지정 된 특정한 prot에 귀를 기울인다.; 자세한 것은 services(5) 을 참조하라.

-d 또는 -v options을 지정하면, syslog에 디버깅 정보가 기록된다.

-l option은 syslog에 각 ftp의 session을 기록한다.

ftp server는 15분이 지나도록 아무 입력이 없으면(inactive session이 발생하면) timeout이 된다. -t option으로 inactive timeout 시간을 지정할수 있다. 설정은 단위로 하며 options과 초를 붙여서 쓴다. -t option을 지정하지 않았을때의 기본값은 900초이다. 또한 이와는 다른 timeout period가 있는데 이는 -T option을 이용하여 최대로 열어 놓을수 있는 session timeout period를 지정할수 있다. 이것은 inactive session과 무관하다. 설정은 -t 와 동일하며 default는 2시간 이다.

-a option은 ftpaccess(5) 설정 file을 사용하도록 한다.

-A option은 ftpaccess(5) 설정 file을 사용하지 않도록 한다. 이 option은 기본 option이다.

-L option은 syslog에 ftpd(8) server에 보내지는 명령들을 기록하도록 한다. -L option은 ftpaccess(5) file의 사용에 의해 무시되어 질수도 있다. -L flag가 사용되어 진다면, 기본적으로 ftp server가 요청 될때마다 명령이 logging 되어질 수 있다. 이것은 모든 USER들의 명령이 기록되는 것을 뜻하며 만약 user가 우연히 username을 대신하는 명령으로 password를 보냈을때 syslog를 통해서 password가 누출될수도 있다.

-i option을 지정하면 ftpd(8) server에 의해 받아들였던 file들이 xferlog(5) 로 log되어 진다. -i option은 ftpaccess(5) file을 사용하면 무시되어 진다.

-o option을 지정하면 ftpd(8) server에 의해 전해진 file들이 xferlog(5) 로 log되어 진다. -o option은 ftpaccess(5) file을 사용하면 무시되어 진다. 만약 -X option을 지정하면, -i 와 -o options에 의해 생성된 output은 xferlog에 저장되지 않는다. 그러나 하나의 중앙 loghost에 여러 host들로 부터의 output을 받아들이는 경우에는 syslog를 통해 저장이 된다.

-u option은 umask 를 기본 umask로 setting을 한다.

-W option은 user login을 wtmp file에 기록하지 않게 한다. Default (-w) 로는 모든 login과 logout이 기록이 된다.

-s 와 -S option들은 standalone 작동 모드로 daemon을 실행하게 한다. -S option은 daemon을 background로 실행을 하며, system booting시에 startup srcitps(ie., in rc.local)를 이용할때 사용한다. -s option은 daemon을 foreground로 실행을 시키며, init로 부터 실행 될때 주로 사용을 한다. (ie., /etc/inittab)

-p 와 -P option들은 daemon에 의해 사용되어지는 port number를 무시한다. 일반적으로 daemon은 "ftp"와 ftp-data"에 대해 /etc/services 를 참조하여 port number를 결정한다. 만약 /etc/services에 "ftp-data"가 지정되어 있지 않고 -P option이 지정되어 있지 않다면 daemon은 control connection port 보다 앞선 port를 사용한다. -p option은 standalone mode로 실행될때만 사용을 할수가 있다.

-q and -Q option들은 daemon이 PID file들의 사용여부를 결정한다. 이 file들은 각 접근 class마다 현재 user의 수를 결정하는 limit 지시자에 의해 요구되어 진다. PID file들의 사용을 안하면 user limit를 사용할수 없다. Default (-q) 로는 PID file들을 사용을 한다. access permission이 PID file의 사용을 막을때 일반 user로서 server를 test할때 -Q 를 지정한다. 좀더 나아가서 동시 사용자의 수를 제한하는 것을 막고 싶은 busy site에서는 PID file의 사용을 불가능하게 하는 것을 고려해 볼만하다.

-r option은 이미 loading시에 rootdir로 지정되어진 거을 chroot로 daemon을 지정한다. 이것은 daemon을 통해 발생한 손상을 입은 file들을 제한함으로서 system security를 증진시킬수 있다. Set is much like anonymous FTP, with additional files needed which vary from system to system.

ftp server는 현재 아래에 나열된 ftp reuest들을 지원을 한다.; case는 구별되어 있지 않다.

Request 설명 ABOR 이전 명령을 중지 ACCT 지정한 account를 무시 ALLO 비어있는 저장공간을 할당 APPE file에 첨가 CDUP 현재 작업 directory를 부모 directory로 이동 CWD 작업 directory를 이동 DELE file

삭제 HELP help 정보 출력 LIST directory의 file list 출력 (‘ls -lgA”) MKD directory 생성 MDTM file의 마지막 변경시간 출력 MODE data transfer mode 를 지정 NLST directory의 file list name만 보여준다. NOOP do nothing PASS password를 지정 PASV server와 server간은 전송 비교 PORT data connection port를 지정 PWD 현재 작업중인 directory를 출력 QUIT session 마침 REST 불완전한 전송을 재시도 RETR file 정정 RMD directory 제거 RNFR filename으로 부터 rename 지정 RNTO filename으로 rename 지정 SITE 일반적이지 않은 commands (다음 section 참조) SIZE file size 출력 STAT server 상태 출력 STOR file 저장 STOU 특정한 이름으로 file 저장 STRU data transfer structure 지정 SYST server system의 OS type 출력 TYPE data transfer type 지정 USER user name 지정 XCUP 현재 작업 directory를 부모 directory로 이동 (deprecated) XCWD change working directory (deprecated) XMKD directory 생성 (deprecated) XPWD 현재 작업 directory 출력 (deprecated) XRMD directory 제거 (deprecated)

아래에 나열된 것은 일반적인 명령이 아니거나 UNIX 특수 명령 들이며 SITE 명령에 수반되어 사용되어진다.

Request 설명 UMASK umask를 변경. E.g. SITE UMASK 002 IDLE idle-timer를 지정. E.g. SITE IDLE 60 CHMOD file의 mode을 변경. E.g. SITE CHMOD 755 filename HELP help 정보를 출력. E.g. SITE HELP NEWER 특정 날짜 이후의 file을 출력 MINFO SITE NEWER와 유사, 하지만 좀더 자세한 정보를 출력 GROUP 특정 gourp 접근을 요구. E.g. SITE GROUP foo GPASS 특정 group 접근 암호를 지정. E.g. SITE GPASS bar EXEC program을 실행. E.g. SITE EXEC program params

여기서 생략된 Internet RFC 959에 지정된 몇몇의 ftp request들은 인식은 되지만 그리 쓸모있지는 않다. MDTM과 SIZE는 RFC 959에 지정되어 있지는 않지만 다음 FTP RFC에 update될 예정이다.

ftp server는 internet RFC 959에 기술되어진 것 처럼 telnet ”Interrupt Porcess” (IP) signal과 Telnet stream 명령의 Telnet ”Synch” signal에 의해서 ABOR 명령이 진행될때 active file 전송은 중지될 것이다. 만약 STST 명령이 data 전송중에 받아진다면, Telnet IP와 Synch에 의해 진행된 transfer status는 되돌려 질것이다.

Ftpd interpret file name들은 csh(1) 에 의하여 사용되어지는 ”golbbing” 규약에 따른다. 이것은 user들이 metacharacter ”*?[]{}˜”를 이용할수 있도록 한다.

인증된 Ftpd user들은 4가지 규칙을 따른다.

1. username은 password data base, /etc/passwd, 또는 OS를 통새 접근할수 있는 무엇에 존재해야 한다. 이 경우 password는 어떤 file 작용이 실행되어지기 전에 client에 의해서 준비 되어야 한다.
2. user name이 /etc/ftpusers 에 있어서는 안된다.
3. user는 getusershell(3) 에 의해 반환되어지는 stan? dard shell을 가져야 한다.
4. username이 ”anonymous” 또는 ”ftp” 일때, anonymous ftp 계정이 password file(user ”ftp”)에 존재해야만 한다. 이 경우 client의 hostname이나 e-mail address를 password로 하여 login을 허락을 한다.

마지막의 경우 ftpd 는 client의 접근 권한을 제한하기 위해 특별한 작업을 수행한다. server는 보안의 침해를 막기 위하여 ”ftp” user의 home directory로 chroot(2) 명령으로 변경시켜 버린다. (anonymous의 를 file에 존재하는 ”ftp”라는 user의 home directory-보통은 /home/ftp-로 바꿔 버린다는 의미이다.) 이것은 ”ftp” subtree는 조심해서 구성되어 진다는 것을 의미하며 아래에 나열된 규칙을 따른다.

˜ftp)

home directory의 소유권을 super-user와 쓰기 권한이 없는 다른 user로 지정을 한다.

˜ftp/bin)

home directory의 소유권을 super-user와 쓰기 권한이 없는 다른 user로 지정을 한다. ls(1) program은 list 명령을 지원하기 위하여 반드시 존재해야 한다. 이 program은 mode 111의 소유권을 가져야 한다.

˜ftp/etc)

home directory의 소유권을 super-user와 쓰기 권한이 없는 다른 user로 지정을 한다. passwd(5) 와 group(5) file은 ls 명령을 실행했을때 숫자(UID, GID)가 아닌 사용자명이 나오도록 하기 위해서 이다. OS에 의존하

며, 다른 요구되는 file들이 있다. libary rutine getpwent(3) 에 대한 man page를 check하도록 한다. passwd의 password field는 사용되지 않으며 실제의 암호화된 password들이 포함되어 있지 않다. 이 file들은 mode 444의 permision을 가지며 super- user에게 소유권이 있다. ~ftp/etc directory안의 group, passwd file들을 system의 /etc/passwd와 /etc/group file로 복사를 하여 사용하면 안된다.

~ftp/pub)

~ftp/pub에서 일반 user들에게 file upload를 허락하려면 적당히 mode 777 또는 mode 733의 permi? sion으로 directory를 만들면 된다. 하지만 pub dirc? tory는 read permision만을 주는 것을 권장하며 upload는 ~ftp/incoming 이라는 directory를 만들어 사용하기를 권장하며 upload directory의 소유권은 super-user가 아닌 ftp에 있어야 한다는 것을 명심한다. 또한 ftp user의 권한 으로 upload 한 file은 지울수가 없으므로 file만 올리는 것 보다는 설명서도 같이 올리도록 message file을 이용하여 권고하도록 한다.

5.4 BSD/OS SYSTEM만의 인증 MECHANISM

ftpd에 의해 사용되어 지는 인증 machanism은 /etc/login.conf 에 있는 users class와 match되는 "auth-ftp" entry에 의해 결정된다. (login.conf(5) 를 참조하라) 만약 class에 대한 "auth-ftp" entry가 없다면 대신에 일반적인 "auth" entry가 사용되어 질것이다. 교차하는 인증 machanism은 "joe:skey" 처럼 콜론(":")이 첨가되어 지정이 된다.

5.5 일반적인 FTP 확장자들

FTP server에는 아래와 같이 특정한 file 확장자로서 몇가지 기능을 수행할수 있다:

실제 Filename 지정한 Filename 실행

———— ———— ————————

<filename>.Z <filename> 압축을 풀고나서 전송

<filename> <filename>.Z 전송전 file을 압축

<filename> <filename>.tar 전송전 file을 Tar로 묶음

<filename> <filename>.tar.Z 전송전 file을 Tar로 묶고 압축

또한 FTP server는 확실한 e-mail 주소를 위한 check를 시도하며, 이 test를 통과하지 못하면 user에게 경고 mes? sage를 출력한다. FTP client가 "long replies" (i.e multi? line responses)에 걸려 있는 user들을 위해 password의 첫번째 character를 dash를 사용하는 것은 server의 lreply() 함수를 불가능 하게 한다.

FTP server는 또한 모든 file의 전송과 수신을 log 할수 있으며, 발생되는 각 file의 전송에 대한 정보에 따라서 관리를 한다.

Mon Dec 3 18:52:41 1990 1 wuarchive.wustl.edu 568881 /files.lst.Z a _ o a chris@wugate.wustl.edu ftp 0 *

%.24s %d %s %d %s %c %s %c %c %s %s %d %s

1 2 3 4 5 6 7 8 9 10 11 12 13

1 DDD MMM dd hh:mm:ss YYYY 형식의 현재시간

2 초 단위의 전송시간

3 remote host name

4 byte 단위의 file size

5 name of file

6 전송 type (a>scii, b>inary)

7 특수 action flags (필요에 따라 연계):

C file이 압축되어짐

U file이 압축되어지지 않음

T file이 tar로 묶임

- 아무것도 발생하지 않음

8 file 이 user에게 보내지거나 (o>utgoing), user로 부터 받음 (i>ncoming)

9 접근한 방식 (r>eal, a>nonymous, g>uest) – mostly for FTP

10 local username 또는 "ftp" user의 경우 login시에 password로 입력한 e-amil address

11 service 명 ('ftp", other)

12 인증방식 (bitmask)

0 none

1 RFC931 인증

13 인증되어진 user id (if available, "*" otherwise)

5.6 관련 항목

ftp(1), getusershell(3), syslogd(8), ftpaccess(5), xfer? log(5), umask(2)

5.7 버그

anonymous 계정은 안전하지가 못하며 가능한 막는 것이 좋다.

server는 지정된 port number로서 socket들을 만들기 위하여 super-user로서 실행이 되어져야 한다. 이것은 login 되어진 user의 영향력 있는 user id를 지속하며 socket에 address를 속박할때 super-user의 권한을 얻을 수가 있기 때문이다. 가능한 보안 구멍에 대해서 세밀히 조사되어 져야 하지만 아무리 해도 불가능하다.

제 6 절 ftphosts

6.1 이름

ftphosts - ftpd에 접근하는 각 host에 대한 제한을 설정

6.2 설명

ftphosts file은 여러 host로 부터 어떤 계정으로 접근을 하는 것을 허락하거나 거절하는데 사용이 된다.

6.3 접근 사용법

allow <username> <addrglob> [<addrglob> ...]

allow host(s)는 오직 <username> 으로 로그를 하기 위한 <addgolb> 만을 비교한다.

deny <username> <addrglob> [<addrglob> ...]

deny host(s)는 항상 <username> 으로 log를 하기 위한 <addglob> 를 비교한다.

anonymous 또는 ftp 와 같은 username은 익명 login user를 의미한다.

<addrglob>는 또한 address/cidr 또는 address:netmask 로서 지정될수도 있다.

예를 들면 : 10.0.0.0/8 or 10.0.0.0:255.0.0.0

6.4 파일

FTPLIB/ftphosts

6.5 관련 항목

ftpd(8), ftpaccess(5), ftplog(5), ftpconversions(5), ftpshut(8)

제 7 절 ftpshut

7.1 이름

ftpshut - 지정한 시간에 ftp server를 다운시킨다.

7.2 문법

ftpshut [-V] [-l min] [-d min] time [warning-message ...]

7.3 설명

ftpshut 명령은 ftp server가 shut down을 할때 superuser가 ftp user 에게 공지할수 있는 자동 shutdown 진행을 준비한다.

-V 옵션은 저작권과 버젼 정보를 출력한다.

time 은 ftpshut 이 ftp server를 다운시킬 시간을 말한다. "now"라는 단어를 사용하여 즉시 shutdown을 할 수 있으며 또한 아래와 같은 하나 또는 두개의 형식으로서 미래의 시간을 지정할 수도 있다. : + number 또는 HHMM.

첫번째 형식은 ftp server down 시간을 minutes(분) 으로서 지정을 한다. 두번째는 24-시간 형식을 사용하여 지정할 날의 시간에 ftp server의 shutdown을 지정한다.

shutdown 10분전 또는 ftpshut 이 10분이 안남았다면 새로운 ftp 접근은 즉시 거부된다. 이 시간은 -l flag 를 통해서 정의되어 진다.

shutdonw 5분전 또는 ftpshut 이 5분이 남지 않았다면 현재 접속이 되어 있는 connections 들은 즉시 끊어지게 된다. 이 시간은 -d flag를 통해서 지정이 된다.

[warning-message ...] 은 75 문자의 길이의 형식을 취한다. ftpshut 은 magic cookie의 실제 문자열 길이 역시 포함을 해서 인식을 한다.

shutdown을 하려 할때 어떠한 file을 생성하여 이 file의 유무에 대해 명령을 실행시킬수가 있다. 일단 shutdown이 되면 이 file이 제가 될때 까지 접속은 거부가 될 것이다. 이 file은 ftpaccess file의 shutdown 지시자에 의해서 위치와 file명이 지정된다.

아래와 같이 macig cookie를 사용가능하다 :

Cookie 설명

%s system이 다운되는 시간

%r 새로운 접속이 거부되는 시간

%d 현재 사용자들이 강제 logout 되는 시간

%C 현재 작업중인 directory

%E ftpaccess에서 지정한 서버 관리자의 Email address

%F CWD 파티션의 남은 공간 (kbytes) [모든 system을 지원하지는 않음]

%L local host name

%M 현 class의 최대 접속 user 수

%N 현 class의 현재 접속 user 수

%R remote host name

%T system의 시간 (form Thu Nov 15 17:12:42 1990)

%U login시 주어진 username

7.4 제한

만약 절대 시간을 사용한다면, server는 현재부터 23:59, 만약 절대 시간을 사용한다면, server는 현재부터 23:59 사이에만 shutdown을 할수 있다.

7.5 관련 항목

shutdown(1), ftpaccess(5), ftprestart(8)

제 8 절 ftpwho

8.1 이름

ftpwho - 각 ftp user에 대한 현재의 process 정보를 보여준다.

8.2 문법

ftpwho [-V]

8.3 설명

ftpwho 명령은 ftp server에 login 해 있는 각 user들에 대한 현재 process 정보를 보여준다. -V 옵션은 저작권과 버전 정보를 출력한다.

8.4 제한

SETPROCTITLE 없이 compile 한다면 별로 유용하지 못할 것이다.

8.5 관련 항목

ftpcount(1)

제 9 절 XFERLOG

9.1 이름

xferlog - FTP server logfile

9.2 설명

The xferlog file은 FTP server daemon (ftpd(8)) 의 log? ging 정보를 포함한다. 이 file은 보통 /usr/adm 에서 볼수 있으나, ftpd(8) 의 options을 사용함에 따라 어디든지 위치되어 질수 있다. Each server entry is composed of a single line of the following form, with all fields being separated by spaces. 각 server 항목은 아래의 form으로 이루어진 한줄로 구성되어 지며, 모든 field는 space로 구분 되어 진다.

current-time transfer-time remote-host file-size filename transfer-type special-action-flag direction access-mode username service-name authentication-method authenticated-user-id completion-status

9.2.1 current-time

"DDD MMM dd hh:mm:ss YYYY" 형식의 현재 local 시간이다. DDD는 주중의 요일을, MMM은 월을, dd는 날짜를, hh는 시를, mm은 분을, ss는 초를, 그리고 YYYY는 년도를 나타낸다.

9.2.2 transfer-time

전송을 위한 총 시간을 말하며 초단위로 표시한다.

9.2.3 remote-host

원격 host 이름이다.

9.2.4 file-size

byte단위의 전송된 file의 크기이다.

9.2.5 filename

전송된 file의 이름이다.

9.2.6 transfer-type

전송의 형태를 나타내는 하나의 character이다.

a 는 ascii 전송을 뜻한다.

b 는 binary 전송을 뜻한다.

9.2.7 special-action-flag

어떤 특정한 action이 발생하는 것을 나타내는 하나 또는 그 이상의 character flag 이다. 아래에 나열된 것 중의 하나 또는 그 이상으로 사용할수 있다.

C file은 압축되어져 있다.

U file은 압축이 되어져 있지 않다.

T file이 tar로 묶여져 있다.

_ 아무런action이 발생하지 않았다.

9.2.8 direction

전송의 지시이다.

o outgoing

i incoming

9.2.9 access-mode

user가 어떻게 login을 하는가에 대한 방법이다.

a (anonymous) 는 익명 손님 user들을 위한 것이다.

g (guest) is for an passworded guest user (see the (guest) 는 password를 소유한 손님 user들을 위한 것이다. (ftpaccess(5) 의 guestgroup 명령을 참조하라)

r (real) 은 인증이 가능한 local user를 위한 것이다.

9.2.10 username

local username 이다. 만약 손님 이라면, 주어진 ID 문자열을 뜻한다.

9.2.11 service-name

발생되어지는 service의 이름이며 보통은 FTP이다.

9.2.12 authentication-method

인증에 사용되어 지는 방법이다. 아래중의 하나를 사용한다.

0 none

1 RFC931 Authentication

9.2.13 authenticated-user-id

인증 방법에 의해 되돌려지는 user id 이다. 인증되어진 user id가 사용불가 하다면 * 이 사용되어 진다.

9.2.14 completion-status

전송 상태를 나타내는 하나의 character이다.

c 완전한 전송

i 불완전한 전송

9.3 파일

/usr/adm/xferlog

9.4 관련 항목

ftpd(8), ftpaccess(5)

제 10 절 ftprestart

10.1 이름

ftprestart - ftp server를 shutdown한후 재시작을 하게 함

10.2 문법

ftprestart [-V]

ftprestart 명령은 ftp server들을 shutdown 이후에 restart를 자동을 하는 방법을 제공한다. **ftprestart** 는 FTP server를 재지삭을 하려고 준비를 할때 사용이 되어진다. 이것은 ftpshut의 반대이며 ftpshut에 의해 생성된 shutdown message를 삭제한다. 이것은 anonymous ftp 영역과 모든 가상 ftp server 영역의 shutdown message file들을 삭제하게 된다.

-V option은 프로그램 수행후에 copyright와 version 정보를 출력하게 한다.

10.3 출력 예제

ftprestart: /servers/some.domain/ftp/etc/shutmsg removed.

ftprestart: /servers/other.domain/ftp/etc/shutmsg removed.

ftprestart: /etc/shutmsg removed.

10.4 관련 항목

shutdown(1), ftpshut(8), ftpaccess(5)

제 11 절 ftpservers

11.1 이름

ftpservers - ftpd 가상 호스트 설정을 정의하는 file

11.2 설명

ftpservers file은 ftpd(8) server가 사용하던 가상호스트 설정 파일을 지정하는데 사용되어 진다. 가상 호스트 지원을 가능하게 compile했을때, wu-ftpd는 각 virtual domain에 대한 설정 파일을 분리해서 사용이 가능하게 되어 있다.

현재, 설정 파일들은 분리되어진 가상 domain 디렉토리에 위치해 있다. 설정 파일에서 사용되어 지는 directory 경로와 IP address는 ftpservers file에 나열이 된다. 실제 설정 파일들은 해당 디렉토리 안에 아래의 이름을 가진 파일들을 포함하고 있어야 한다:

ftpaccess - 가상 doamin 접근 파일

ftpusers - 접근을 거부할 계정들을 설정

ftpgroups - SITE GROUP and SITE GPASS 지원

ftphosts - 가상 도메인에 접근 가능한 대역을 설정

ftpconversions - 가상 도메인에서 사용 가능한 전환 명령을을 최적화

각 가상 domain directory에 모든 설정 파일들을 가지고 있을 필요는 없다. 만약 주 도메인의 설정을 그대로 사용하려 한다면, ftpconversions file 같은 것들을 예를 든다면, 가상 도메인 directory에 구태여 이 파일을 넣을 필요는 없다는 것이다. 이렇게 가상 도메인 directory에 포함되어 있지 않은 설정파일들은 주 도메인의 설정 파일을 불러들이게 된다.

주의!!!: 가상 도메인 directory에 들어가는 파일들은 위의 list와 정확하게 match되어져야 한다. 만약 이름에 오타가 있을 경우에는 해당 파일을 찾지 못하게 되며 주 도메인 설정 파일로 대체를 하게 된다.

11.3 ftpservers file 형식

각 entry에는 2개의 field가 존재한다.

ipaddr/hostname directory-containing-configuration-files

예제:

```
10.196.145.10 /etc/ftpd/ftpaccess.somedomain/

10.196.145.200 /etc/ftpd/ftpaccess.someotherdomain/

some.domain INTERNAL
```

ftp client가 server로 접속을 할때, ftpd는 ftpservers file에서 발견한 ftp client가 접속을 할 ip address를 매치시키려 한다.

매치가 되는 것을 발견을 하면, 해당 도메인에 대한 디렉토리 경로와 설정 파일들을 반환하게 된다. ftpd는 이 디렉토리에 들어 있는 설정 파일들을 사용하게 된다.

설정 파일에 match되는 것이 없거나, directory 경로가 정의가 잘못 되어 있을 경우, 설정 파일의 기본 경로를 사용하게 된다. 위의 예제중 INTERNAL의 사용은 주 도메인의 설정 파일을 사용하도록 하게 한다.

가상 도메인을 지정할때 실제 IP address와 hostname 모두 설정이 가능하다. 다만 hostname으로 지정할 경우 DNS lookup이 필요하고 또한 DNS 버그와도 관련이 되어 질수 있으므로 왠만하면 ip address로 지정을 하는 것을 권장한다.

```
10.196.145.20 /etc/ftpd/config/faqs.org/

ftp.some.domain /etc/ftpd/config/faqs.org/
```

주석처리시에는 # 표시를 사용하며, 중복 주석 라인과 공백 라인은 무시되어 진다.

11.4 관련 항목

ftpd(8) , ftpaccess(5) ftplog(5) , ftpconversions(5) , ftphosts(5)

제 12 절 Copyright

Copyright (c) 1999,2000 WU-FTPD Development Group. All rights reserved.

Portions Copyright (c) 1980, 1985, 1988, 1989, 1990, 1991, 1993, 1994 The Regents of the University of California. Portions Copyright (c) 1993, 1994 Washington University in Saint Louis. Portions Copyright (c) 1996, 1998 Berkeley Software Design, Inc. Portions Copyright (c) 1998 Sendmail, Inc. Portions Copyright (c)

1983, 1995, 1996, 1997 Eric P. Allman. Portions Copyright (c) 1989 Massachusetts Institute of Technology. Portions Copyright (c) 1997 Stan Barber. Portions Copyright (C) 1991, 1992, 1993, 1994, 1995, 1996, 1997 Free Software Foundation, Inc. Portions Copyright (c) 1997 Kent Landfield.

Use and distribution of this software and its source code are governed by the terms and conditions of the WU-FTPD Software License ("LICENSE").

$ Id: ftpcount.1,v 1.5 2000/07/01 17:49:09 wuftpd Exp $