FTP 서버 구축

Ⅰ. 개요

p663

- FTP(File Transfer Protocol)는 네트워크상에서 컴퓨터간에 파일을 전송할 때 사용되는 프로토콜
- 클라이언트에게 파일을 전송할 수 있도록 해주는 서버를 FTP 서버라 함
- FTP 서버를 구축하는데 이용되는 대표적인 서버 프로그램으로는 vsftpd, proftpd 등이 있음

2. vsFTP 설치

2.2 vsFTP 설치

- yum 으로 설치

```
# yum -y install vsftpd
```


2.3 vsFTP 서버 실행

```
# systemctl start(restart, enable) vsftpd
```

2.3 vsFTP 서버 실행 (계속)

- vsFTP 작동 유무 확인

```
# ftp localhost
```

```
[root@seokj ~]# ftp localhost
Connected to seokj.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (localhost:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```


3. vsFTP 서버 설정

3.1 vsFTP 서버 관련 파일

파일명	설명
/etc/vsftpd/vsftpd.conf	vsftpd 환경 설정 파일
/usr/sbin/vsftpd	vsfptd 바이너리 파일
/etc/pam.d/vsftpd	vsftpd PAM 인증 파일
/etc/vsftpd/ftpusers	로그인 불가능한 유저 파일
/etc/vsftpd/user_list	userlist_deny 값에 따라 로그인 허용여부 결정
/etc/xinetd.d/vsftpd	xinetd 서비스 파일

3.2 /etc/vsftpd/vsftpd.conf

- 익명 접속 설정 관련 옵션

```
anonymous_enable = YES
```

- 익명(anonymous) 로그인 허용 여부 설정 옵션
- 기본값 : YES

```
anon_upload_enable = NO
```

- write_enable 옵션이 허용될 경우 익명 사용자가 업로드 가능한 디렉토리에서 업로드 가능 여부 설정 옵션
- 기본값 : NO

```
anon_mkdir_write_enable = NO
```

- write_enable 옵션이 허용될 경우 익명 사용자가 쓰기 가능한 디렉토리내에서 새로운 디렉토리 생성 여부 설정 옵션
- 기본값 : NO

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 익명 접속 설정 관련 옵션 (계속)

```
deny_email_enable = NO
```

- 익명 계정이 로그인할 때 banned_email_file 옵션으로 지정된 파일에 포함된 이메일 주소 형태로 로그인 유무 설정 옵션
- 기본값 : NO

```
banned_email_file = /etc/vsftpd/banned-emails
```

- 익명 접속시 허용하지 않을 이메일 패스워드 형태를 담고 있는 파일을 명시하는 옵션
- deny_email_enable 옵션과 함께 작동
- 지정한 파일에 로그인 불허 이메일 주소 형태를 한줄씩 삽입

```
secure_email_list_enable = NO
```

- 익명 로그인시 패스워드로 유효한 이메일 적용할 것인가를 설정하는 옵션
- 활성화하게 되면 /etc/vsftpd/vsftpd.email_passwords 파일에 명시된 패스워드만 익명 로그인 가능
- 패스워드 파일은 email_password_file 옵션으로 변경 가능

3.2 /etc/vsftpd/vsftpd.conf (계속)

익명 접속 설정 관련 옵션 (계속)

```
email_password_file = /etc/vsftpd/vsftpd.email_passwords
```

- secure_email_list_enable 옵션이 활성화 될 때 사용될 익명 로그인에 필요한 이메일 패스워드를 담고 있는 파일을 지정해주는 옵션
- 기본값 : /etc/vsftpd/vsftpd.email_passwords

```
anon_other_write_enable = NO
```

- 파일 업로드 및 디렉토리 생성 이외의 파일 삭제 및 파일명 변경 등과 같은 쓰기 기능을 익명 사용자들이 가능하도록 할 것인지에 대한 설정 옵션
- 기본값 : NO

```
anon_world_readable_only = YES
```

- 읽기 모드로 되어 있는 FTP 계정 소유의 파일을 다운로드 할 수 있게 할 것인지에 대한 설정 옵션
- 기본값 : YES

3.2 /etc/vsftpd/vsftpd.conf (계속)

익명 접속 설정 관련 옵션 (계속)

```
no_anon_password = NO
```

- 익명 접속시 패스워드를 묻지 않고 로그인을 허용할 것인지를 설정하는 옵션
- 기본값 : NO

```
anon_max_rate = 0
```

- 익명 접속시 다운로드 가능한 최대 전송율 지정 옵션
- 단위 : bps(bytes/second)
- 기본값 : 0 (무제한)

```
anon_umask = 077
```

- 익명 FTP에서 익명 사용자들이 파일을 생성하는데 있어서 umask 값 지정 옵션
- 기본값 : 077

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 익명 접속 설정 관련 옵션 (계속)

```
anon_root = 경로
```

- 익명 로그인시 위치할 홈 경로 지정 옵션
- 올바르지 않은 경로 지정시 옵션 무시

```
ftp_username = ftp
```

- 익명 FTP에 사용될 사용자명 지정 옵션
- 기본값 : ftp

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 실명 로그인 및 시스템 설정 옵션

```
local_enable = NO
```

- 로컬 호스트상에 있는 사용자의 로그인 허용 여부 설정 옵션
- /etc/passwd 파일에 존재하는 사용자의 로그인 허용 여부 설정
- 실명 접속시 YES
- 기본값 : NO

```
write_enable = NO
```

- 파일을 변경하는 FTP 명령을 사용할 수 있도록 할 것인지 여부 설정 옵션
- 기본값 : NO
- 익명 서버에서는 클라이언트가 파일을 업로드하지 않아도 되므로 NO 값을 설정하지만, 실명 접속 서버에서는 사용자들이 자신의 계정에 데이터를 업로드 할 수 있도록 YES로 지정

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 실명 로그인 및 시스템 설정 옵션 (계속)

```
local_mask = 077
```

- 파일이 생성될 때 파일 퍼미션(허가권)에 적용될 umask 값 지정 옵션
- 기본값 : 077

```
dirlist_enable = YES
```

- LIST 명령 허용할 것인지 여부 설정 옵션
- NO로 설정하면 FTP 클라이언트 접속시 퍼미션 오류와 함께 디렉토리 목록이 나타나지 않음
- 기본값 : YES

```
dirmessage_enable = NO
```

- 사용자가 새로운 디렉토리로 이동할 경우 그 디렉토리에 있는 메시지 파일을 보여줄 것인지를 설정해 주는 옵션
- 디렉토리 내의 메시지 파일은 message_file 옵션에서 지정
- 기본값 : NO

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 실명 로그인 및 시스템 설정 옵션 (계속)

```
message_file = .message
```

- 디렉토리 이동시 보여줄 메시지를 담고 있는 파일명을 지정해 주는 옵션
- dirmessage_enable 옵션이 활성화 되었을 때 적용되는 옵션
- 기본값 : .message

```
download_enable = YES
```

- 다운로드 허용 여부 설정 옵션
- 기본값 : YES

```
force_dot_files = NO
```

- 점(.)으로 시작되는 파일과 디렉토리 출력 여부 설정 옵션
- 기본값 : NO

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 실명 로그인 및 시스템 설정 옵션 (계속)

```
guest_enable = NO
```

- 실제 계정에는 존재하지 않는 가상 사용자 계정 로그인 여부 설정 옵션
- 가상 사용자의 계정과 패스워드가 들어있는 데이터베이스 포맷으로 된 파일(/etc/vsftpd/vsftpd_login.db)과 가상 사용자의 인증을 위해 PAM 파일이 있어야 함
- guest_username 옵션과 함께 작동
- 기본값 : NO

```
guest_username = ftp
```

- guest_enable 옵션이 활성화 되었을 때 가상 사용잘르 맵핑시킬 실제 사용자 지정 옵션
- 기본값 : ftp

LINUX 서버 구축

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 실명 로그인 및 시스템 설정 옵션 (계속)

```
text_userdb_names = NO
```

- 디렉토리 및 파일 목록에서 사용자와 그룹의 ID가 숫자 대신에 텍스트 이름으로 보여지도록 할 것인지를 지정하는 옵션
- 시스템 안전을 위해 이 옵션 비활성화
- 기본값 : NO

```
userlist_enable = NO
```

- userlist_file 옵션으로 명시된 파일안에 있는 계정들만 로그인을 허용할 것인지를 설정하는 옵션
- 기본값 : NO

```
userlist_deny = YES
```

- userlist_enable 옵션과는 반대로 userlist_file로 명시된 파일에 있는 계정들의 로그인을 거부하고자 할 경우 사용되는 옵션
- 기본값 : YES

YD 예담직업전문학교

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 실명 로그인 및 시스템 설정 옵션 (계속)

```
userlist_file = /etc/vsftpd/user_list
```

- userlist_enable 옵션이 적용될 때 로그인 가능한 유저를 담고 있는 파일을 지정하는 옵션
- 기본값 : /etc/vsftpd/user_list

```
file_open_mode = 0666
```

- 파일이 업로드되었을 때의 퍼미션을 지정해 주는 옵션
- umask 옵션은 이 옵션보다 선행
- 기본값 : 0666

```
listen = NO
```

- vsftpd 데몬을 독립 모드로 동작되도록 할 때 지정하는 옵션
- inetd 모드로 vsftpd 데몬을 돌릴 때는 이 옵션 사용하면 안됨

LINUX 서버 구축

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 실명 로그인 및 시스템 설정 옵션 (계속)

```
listen_port = 21
```

- vsftpd 데몬이 독립모드로 작동할 때 vsftpd 데몬이 외부의 접속 요청에 경청할 ftp 포트 설정 옵션
- 기본값 : 21

```
user_config_dir = /etc/vsftpd/vsftpd_user_conf
```

- 가상 유저마다 각기 다른 vsftpd.conf 설정이 적용되도록 사용자의 vsftpd.conf 파일을 지정해 주는 옵션

```
virtual_use_local_privs = NO
```

- 가상 사용자 접속 설정에서 사용되는 옵션으로 익명 접속 사용자와 동일한 권한을 가진 가상 사용자의 권한을 로컬 사용자와 같은 권한을 가지도록 설정하는 옵션

YD 예담직업전문학교

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 실명 로그인 및 시스템 설정 옵션 (계속)

```
deny_file = {*.exe, *.pif}
```

- 업로드 및 다운로드를 금지할 파일 형태를 지정하는 옵션

```
hide_file = {*.iso, *.conf}
```

- FTP 접속시 디렉토리나 파일 목록에서 보여지지 않는 파일 지정 옵션
- 클라이언트가 파일 위치와 파일명을 알고 있을 경우 직접 다운로드 가능
- 웹링크시 유용

LINUX 서버 구축

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 접속 제어 관련 설정

```
one_process_model = NO
```

- 클라이언트 접속마다 하나의 프로세스가 작동되도록 할 것인지를 지정하는 옵션
- 오직 익명 접속에만 적용되는 옵션
- 기본값 : NO

```
max_clients = 100
```

- vsftpd 서버에 접속할 수 있는 클라이언트 최대 수 지정 옵션

```
max_per_ip = 0
```

- 호스트당 접속할 때 최대 접속수 지정 옵션
- 기본값 : 0 (무제한)

YD 예담직업전문학교

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 접속 제어 관련 설정 (계속)

```
local_max_rate = 0
```

- 로컬 사용자가 파일을 전송할 수 있는 최대 속도 지정 옵션
- 기본값 : 0 (무제한)

```
idle_session_timeout = 30
```

- FTP 명령을 실행한 후 일정 시간 동안 다른 명령을 입력하지 않으면 접속 세션을 끊어지도록 지정하는 옵션
- 기본값 : 300 (초)

```
ftpd_banner = Welcome to SKJ
```

- 사용자가 FTP 서버에 접속할 때 보여주는 배너 메시지 지정 옵션

```
accept_timeout = 60
```

- 수동 모드로 클라이언트가 서버의 데이터 포트에 연결될 때 타임아웃 기간 설정 옵션
- 기본값 : 60 (초)

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 보안 관련 설정

```
chroot_local_user = NO
```

- 로컬 시스템에 존재하는 사용자들이 자신의 디렉토리에 대해서 chroot(상위 디렉토리 접근)를 가질 것인지를 지정하는 옵션
- 기본값 : NO

```
chroot_list_enable = NO
```

- 사용자가 로그인시 자신의 디렉토리에 대해서 chroot를 갖도록 할 것인지를 설정하는 옵션
- 활성화 될 경우 chroot_list_file 옵션에 지정된 파일에 있는 사용자는 자신의 디렉토리 이외의 상위 디렉토리로는 접근 불가능
- 기본값 : NO

3.2 /etc/vsftpd/vsftpd.conf (계속)

보안 관련 설정 (계속)

```
chroot_list_file = /etc/vsftpd/chroot-list
```

- 사용자 홈 디렉토리에 대해서 chroot를 적용하고자 하는 사용자 계정을 담고 있는 파일명을 지정하는 옵션
- chroot_list_enable 옵션이 활성화되고 chroot_local_user 옵션은 비활성화되어 있어야 적용 됨
- 기본값 : /etc/vsftpd/chroot-list

```
chown_uploads = NO
```

- 익명으로 업로드된 파일에 대해서 chown_username 옵션으로 명시된 사용자의 소유권으로 변경되도록 할 것인지를 지정하는 옵션
- 기본값 : NO

```
chown_username = root
```

- 익명의 업로드 파일에 대한 소유권을 갖는 사용자 계정을 가진 파일 지정 옵션
- chown_uploads 옵션과 함께 적용되는 옵션
- 기본값 : root

LINUX 서버 구축

3.2 /etc/vsftpd/vsftpd.conf (계속)

보안 관련 설정 (계속)

```
nopriv_user = nobody
```

- vsftpd 데몬을 루트 권한이 아닌 시스템에 존재하는 일반 사용자의 비특권 권한으로 작동되도록 하고자 할 경우 지정하는 옵션
- 기본값 : nobody

```
ascii_download_enable = NO
ascii_upload_enable = NO
```

- 파일 전송을 아스키 모드(ASCII)로 작동하게 할 것인지를 지정하는 옵션
- 기본값 : NO

```
ls_recurse_enable = NO
```

- ls -R (현재 디렉토리 및 하위 디렉토리) 명령을 허용할 것인지를 지정하는 옵션
- 기본값 : NO

YD 예담직업전문학교

3.2 /etc/vsftpd/vsftpd.conf (계속)

보안 관련 설정 (계속)

```
hide_ids = NO
```

- 디렉토리 목록에서 사용자의 ID와 그룹의 ID를 보여주지 않고 모두 ftp로 표시할 것인지를 지정하는 옵션
- 기본값 : NO

```
pam_service_name = ftp
```

- PAM(장착식 모듈)을 이용하여 사용자 인증을 하고자 할 경우 인증 파일을 지정하는 옵션
- 기본값 : ftp

```
check_shell = YES
```

- 사용자 로그인시 사용자의 유효 쉘을 /etc/shell 파일에서 체크할 것인지를 설정하는 옵션
- PAM 모듈이 작동하지 않는 vsftpd 서버에서 효과적

LINUX 서버 구축

3.2 /etc/vsftpd/vsftpd.conf (계속)

데이터 연결 관련 설정

```
pasv_enable = YES
```

- 수동 데이터 연결 모드(passive mode)로 지원할 것인지를 지정하는 옵션
- 기본값 : YES

```
pasv_promiscuous = YES
```

- 제어 연결에서 사용된 동일한 아이피 주소에서 이뤄지는 데이터 연결을 보장해 주는 수동 보안 체크 기능을 사용할 것인지를 지정하는 옵션
- 기본값 : YES (수동 보안 기능 비활성화)

```
pasv_max_port / pasv_min_port
```

- 수동 모드로 데이터 연결시 할당될 최대 및 최소 포트를 지정하는 옵션
- 수동 모드로 연결될 때의 포트는 일반적으로 5000~6000
- 기본값 : 0 (포트 제한없음)

YD 예담직업전문학교

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 데이터 연결 관련 설정 (계속)

```
ftp_data_port = 20
```

- 포트 형식의 데이터 연결시 사용할 포트를 지정하는 옵션
- 기본값 : 20

```
data_connection_timeout = 300
```

- FTP 서버로부터 데이터를 다운로드하거나 업로드한 후에 다시 파일을 전송하지 않으면 끊어질 시간을 지정하는 옵션
- 기본값 : 300 (초)

```
port_enable = YES
```

- PORT 명령으로 서버와 클라이언트간의 데이터 포트 연결되는 방식을 허용할 것인지 아닌지를 지정하는 옵션
- 기본값 : YES

LINUX 서버 구축

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 데이터 연결 관련 설정 (계속)

```
connect_timeout = 60
```

- 클라이언트가 서버의 제어 포트에 연결되었을 경우 타임아웃 시간을 설정하는 옵션
- 기본값 : 60 (초)

YD 예담직업전문학교

3.2 /etc/vsftpd/vsftpd.conf (계속)

로그 관련 설정

```
xferlog_enable = NO
```

- 파일 송수신 결과를 xferlog_file 옵션으로 지정된 로그 파일에 저장할 것인지를 지정하는 옵션
- 기본값 : NO

```
xferlog_file = /var/log/vsftpd.log
```

- xferlog_enable 옵션이 활성화 되었을 경우 파일 송수신 과정을 기록할 로그 파일을 지정하는 옵션
- 기본값 : /var/log/vsftpd.log

```
xferlog_std_format = NO
```

- 파일 송수신 로그를 표준 xferlog 포맷으로 저장되도록 할 것인지를 지정하는 옵션
- 기본값 : NO

3.2 /etc/vsftpd/vsftpd.conf (계속)

로그 관련 설정 (계속)

```
log_tp_protocol = NO
```

- xferlog_std_format 옵션이 선택되지 않을 경우 모든 FTP 요청 및 응답에 관련된 메시지를 기록할 것인지를 지정하는 옵션
- 오류 분석시 유용
- 기본값 : NO

```
syslog_enable = NO
```

- FTP에 관련된 로그가 /var/log/vsftpd.log에 저장되지 않는 대신 시스템 로그 파일 (/var/log/syslog)에 저장되도록 할 것인지를 지정하는 옵션
- FTP 데몬의 메시지 종류에 따라 로그 기록
- 기본값 : NO

```
dual_log_enable = NO
```

- /var/log/xferlog 파일과 /var/log/vsftpd.log 파일 모두에 FTP 전송 기록이 저장되도록 하는 옵션
- 기본값 : NO

3.2 /etc/vsftpd/vsftpd.conf (계속)

- 로그 관련 설정 (계속)

```
vsftpd_log_file = /var/log/vsftpd.log
```

  - vsftpd 데몬에 의한 로그 메시지를 기록할 파일명을 지정하는 옵션
  - 로그가 기록되도록 하기 위해서는 xferlog_enable 옵션이 활성화되고, xferlog_std_format 옵션이 비활성화
  - 기본값 : /var/log/vsftpd.log

3.3 /etc/vsftpd/ftpusers

- vsftpd 서버에서 로그인할 수 없는 사용자 목록을 담고 있는 파일
- 소스 설치시 생성되지 않으므로 만들어서 사용
- /etc/pam.d/vsftpd PAM 모듈에 의해서 이 파일에 열거된 사용자들의 로그인을 거부하게 됨
- 로그인을 제한하고자 하는 사용자가 있다면 그 계정을 이 파일에 한줄 씩 넣어주면 됨

```
[root@seokj vsftpd]# cat /etc/vsftpd/ftpusers
# Users that are not allowed to login via ftp
root
bin
daemon
adm
lp
sync
shutdown
halt
```

3.4 /etc/pam.d/vsftpd

- PAM(Pluggable Authentication Modules, 장착식 인증 모듈)에 의해서 사용자의 로그인을 제어하고자 할 경우 사용되는 모듈 파일
- vsftpd.conf 파일에 pam_service_name = vsftpd 옵션을 추가해 주어야 실명 접속시 모듈에 의해서 사용자의 로그인에 대해서 인증 기능 사용 가능

```
[root@seokj vsftpd]# cat /etc/pam.d/vsftpd
#%PAM-1.0
auth       required     pam_listfile.so item=user sense=deny file=/
etc/vsftpd/ftpusers onerr=succeed
auth       required     pam_shells.so
session    required     pam_loginuid.so
```


3.5 /etc/vsftpd/user_list

- vsftpd.conf 파일에서
  - userlist_deny = NO : 이 파일안에 있는 사용자들은 로그인 가능
  - userlist_deny = YES : 이 파일안에 있는 사용자들은 로그인 불가능

```
[root@seokj vsftpd]# cat /etc/vsftpd/user_list
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, a
nd
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/f
tpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
```