

ftp、nfs、ssh 服务器的搭建

—— 介绍三个常用的服务器软件，演示中以 server 用户作为服务器端，以 client 用户作为客户端。

1、ftp 服务器的搭建 —— vsftpd（自带服务器端和客户端）

功能：文件的上传和下载

注意：在使用 vsftpd 的客户端登录时，一定要分清服务器端和客户端的当前目录，客户端在那个目录登陆的，那么这个目录就是客户端的当前目录，而登陆成功后可以随时切换服务器端的当前目录。

1) 服务器端：

(1) 安装 vsftpd 软件：sudo apt-get install vsftpd

(2) 修改配置文件 —— /etc/vsftpd.conf

```
# daemon started from an initscript.
listen=YES ← 开启监听
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disbled by default).
anonymous_enable=YES ← 允许匿名登录，并设置匿名登录的根目录
anon_root=/home/server/anonFtp/
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES ← 实名登录可上传文件
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022 ← 设置本地掩码，决定实名登录上传文件的默认权限
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES ← 允许匿名用户上传文件
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories
anon_mkdir_write_enable=YES ← 允许匿名用户创建目录
#
```

(3) 重启服务：sudo service vsftpd restart

2) 客户端：

(1) 实名用户登陆：ftp + 服务器 IP → 输入服务器的用户名和密码

```

client@ubuntu:~$ ftp 192.168.74.128
Connected to 192.168.74.128.
220 (vsFTPd 3.0.3)
Name (192.168.74.128:client): server
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/server" is the current directory

```

实名登录首先进入服务器用户的主目录

文件的上传: put file

文件的下载: get file

退出命令: bye/exit/quit

```

ftp> cd anonFtp
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1001 1001 11 Jul 07 08:35 1.txt
-rw-rw-r-- 1 1001 1001 68 Jul 07 08:35 2.txt
drwxrwxr-x 2 1001 1001 4096 Jul 07 08:36 abc
226 Directory send OK.
ftp> get 1.txt
local: 1.txt remote: 1.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for 1.txt (11 bytes).
226 Transfer complete.
11 bytes received in 0.00 secs (50.4328 kB/s)
ftp> put 111
local: 111 remote: 111
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
27 bytes sent in 0.00 secs (1.0300 MB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1001 1001 11 Jul 07 08:35 1.txt
-rw-r--r-- 1 1001 1001 27 Jul 07 08:45 111
-rw-rw-r-- 1 1001 1001 68 Jul 07 08:35 2.txt
drwxrwxr-x 2 1001 1001 4096 Jul 07 08:36 abc
226 Directory send OK.
ftp> bye
221 Goodbye.
client@ubuntu:~$ ls
111 1.txt examples.desktop
client@ubuntu:~$

```

文件的下载

文件的上传

不允许直接操作目录，可以先打包再进行操作。

缺点：暴露服务器用户的密码；可以对服务器任意目录进行操作，不安全。

(2) 匿名用户登陆: ftp + 服务器 IP → 输入用户名 anonymous，无需密码

```
client@ubuntu:~/a$ ftp 192.168.74.128
Connected to 192.168.74.128.
220 (vsFTPD 3.0.3)
Name (192.168.74.128:client): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1001 1001 11 Jul 07 08:35 1.txt
-rw-r--r-- 1 1001 1001 27 Jul 07 08:45 111
-rw-rw-r-- 1 1001 1001 68 Jul 07 08:35 2.txt
drwxrwxr-x 2 1001 1001 4096 Jul 07 08:36 abc
226 Directory send OK.
```

文件的上传: put file

文件的下载: get file

不允许匿名用户在任何目录中切换,只能在指定的目录范围中进行操作。在配置文件中写入 anon_root=xxx (目录的绝对路径) 指定匿名用户登陆的根目录。

(3) 使用 lftp 客户端访问 ftp 服务器

使用 vsftpd 自带的客户端登陆成功后不能再对客户端进行操纵,而使用 lftp 客户端登陆成功后,只要在命令前加 l 就是对客户端进行操纵。

安装: sudo apt-get install lftp

实名登录: lftp + 服务器用户名@服务器 IP → 输入服务器密码

```
client@ubuntu:~/a$ lftp server@192.168.74.128
口令:
lftp server@192.168.74.128:~> pwd
ftp://server@192.168.74.128
lftp server@192.168.74.128:~> lpwd
/home/client/a
lftp server@192.168.74.128:~> lcd ..
lcd 成功, 本地目录=/home/client
lftp server@192.168.74.128:~>
```

匿名登录: lftp + 服务器 IP → 输入 login

```
client@ubuntu:~/a$ lftp 192.168.74.128
lftp 192.168.74.128:~> login
用法: login <用户> [<URL> [<密码>]]
lftp 192.168.74.128:~> pwd
ftp://192.168.74.128
lftp 192.168.74.128:~> ls
-rw-rw-r-- 1 1001 1001 11 Jul 07 08:35 1.txt
-rw-r--r-- 1 1001 1001 27 Jul 07 08:45 111
-rw-rw-r-- 1 1001 1001 68 Jul 07 08:35 2.txt
drwxrwxr-x 2 1001 1001 4096 Jul 07 08:36 abc
```

操作:

put/get —— 上传/下载文件

mput/mget —— 上传/下载多个文件

mirror —— 下载整个目录及其子目录
mirror -R —— 上传整个目录及其子目录

2、nfs 服务器的搭建 —— nfs-kernel-server

功能：共享文件夹

1) 服务器端：

- (1) 安装 nfs-kernel-server 软件：sudo apt-get install nfs-kernel-server
- (2) 创建共享目录
- (3) 修改配置文件 —— /etc/exports

```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/home/server/shareNfs *(rw,sync)
~
~
~
~
```

共享目录 共享网段

rw —— 可读可写
ro —— 只读
sync —— 实时更新到磁盘

- (4) 重启服务：sudo service nfs-kernel-server restart

2) 客户端（和挂载 U 盘的操作类似）：

- (1) 挂载服务器共享目录：sudo mount + 服务器 IP:共享目录 + 挂载点
- (2) 取消挂载：sudo umount + 挂载点

```
client@ubuntu:/$ sudo mount 192.168.74.128:/home/server/shareNfs/ /mnt/
client@ubuntu:/$ cd /mnt/
client@ubuntu:/mnt$ ls
1.txt 2.txt abc
client@ubuntu:/mnt$ cd ..
client@ubuntu:/$ sudo umount /mnt
```

3、ssh 服务器的搭建 —— openssh-server

功能：远程登录

1) 服务器端：

- (1) 安装 openssh-server 软件：sudo apt-get install openssh-server

2) 客户端：

- (1) 远程登录：ssh + 服务器用户名@服务器 IP → 输入服务器用户密码
- (2) 退出登录：logout

```
client@ubuntu:/$ ssh server@192.168.74.128
The authenticity of host '192.168.74.128 (192.168.74.128)' can't be established.
ECDSA key fingerprint is SHA256:AnoBs2qLYIbAPayAlBM4jeh5b6h4dy428s0PvxnmsY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.74.128' (ECDSA) to the list of known hosts.
server@192.168.74.128's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

90 个可升级软件包。
3 个安全更新。

Last login: Fri Jul 7 19:01:04 2017 from 192.168.74.1
server@ubuntu:~$ pwd
/home/server
server@ubuntu:~$ logout
Connection to 192.168.74.128 closed.
client@ubuntu:/$
```

远程登录成功