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

（3）重启服务：sudo service vsftpd restart

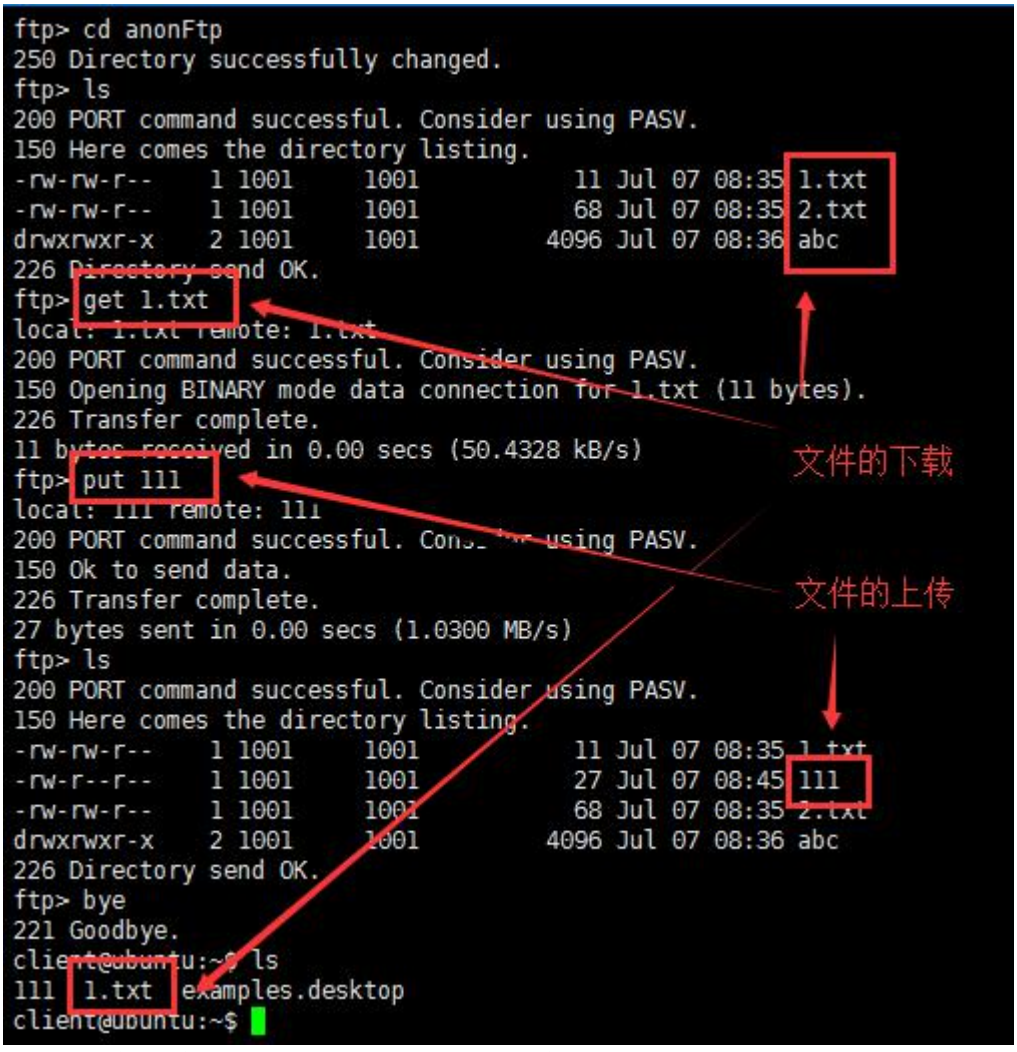
2）客户端：

（1）实名用户登陆：ftp + 服务器 IP → 输入服务器的用户名和密码

文件的上传：put file

文件的下载：get file

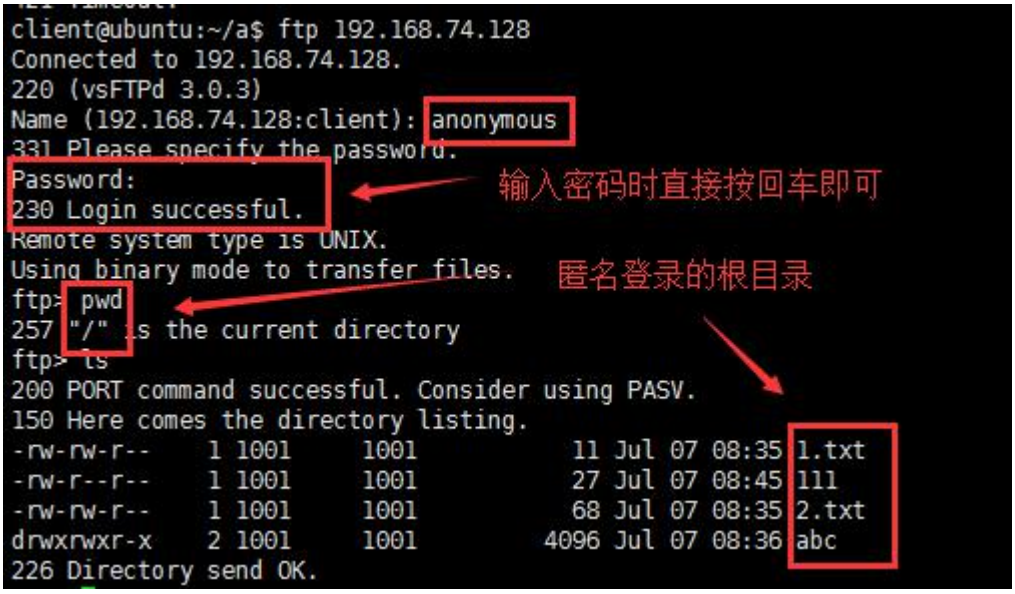
退出命令：bye/exit/quit



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



文件的上传：put file

文件的下载：get file

不允许匿名用户在任意目录中切换，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。

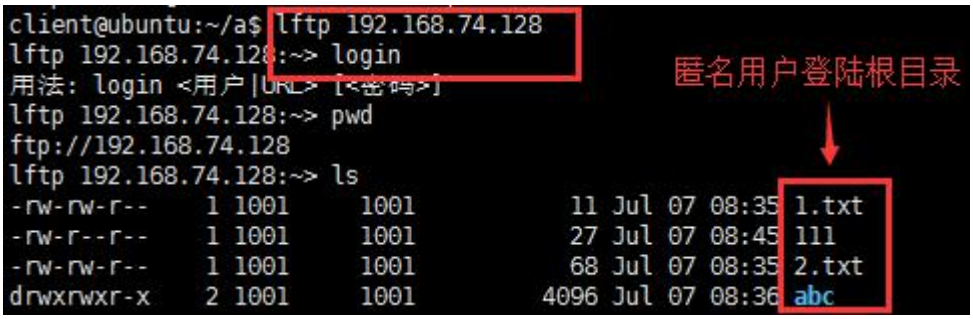
（3）使用 lftp 客户端访问 ftp 服务器

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

匿名登录：lftp + 服务器 IP → 输入 login



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)
~
~
~
~
~
```

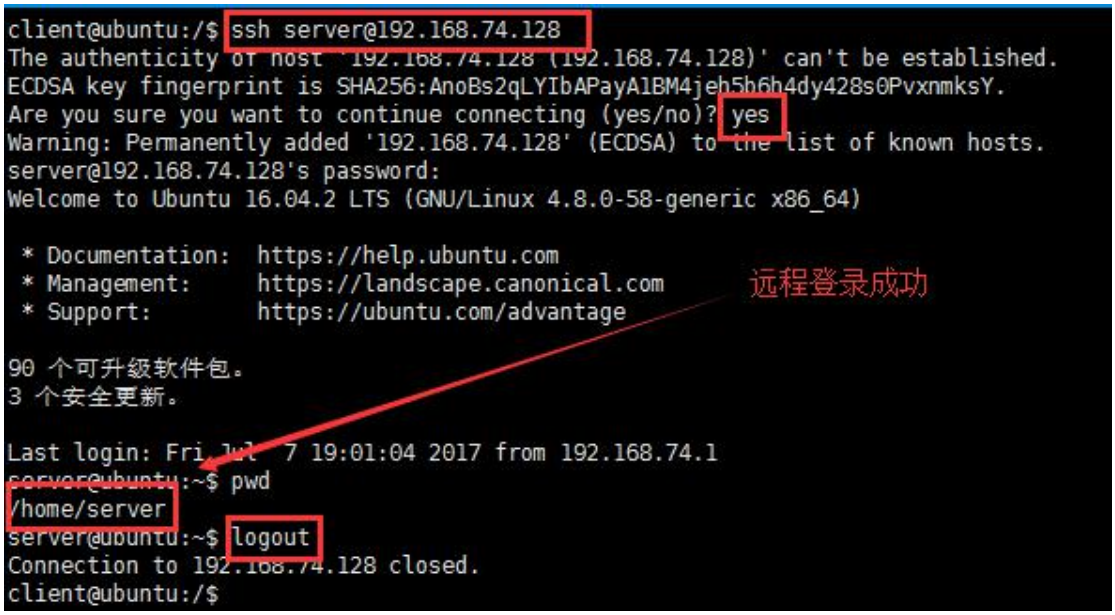
共享目录　　共享网段

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:AnoBs2qLYIbAPayA1BM4jeh5b6h4dy428s0PvxnmksY.
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