

1.设置root密码

```
1 sudo passwd root
```

2.更换清华源

<https://mirrors.tuna.tsinghua.edu.cn/help/ubuntu/>

选择18.04，将内容粘贴到/etc/apt/sources.list

更新

```
1 apt-get upgrade
```

3.安装ssh

```
1 apt-get install openssh-server
```

查看是否安装

```
1 ps -aux | grep sshd
```

启动ssh

```
1 service ssh start
```

给普通账户设置rsa加密

```
1 su xmr
2 ssh-keygen -t rsa
```

全部按回车，设置完后，就用其他电脑ssh 登录对于得地址，使用 ip addr 可以查看地址

4.设置samba

```
1 apt-get install samba
2 vi /etc/samba/smb.conf
3
4 [xmr]
5 path = /home/xmr
6 valid users = xmr
7 browseable = yes
8 public = yes
9 writable = yes
```

创建账号

```
1 smbpasswd -a xmr
```

重启samba 服务

```
1 /etc/init.d/smbd restart
```

5.安装依赖包

```
1 apt-get install gawk wget git-core diffstat unzip texinfo gcc-multilib build-essential
  chrpath socat libstdl1.2-dev
2 apt-get install libstdl1.2-dev xterm sed cvs subversion coreutils texi2html docbook-
  utils python-pysqlite2 help2man make gcc g++ desktop-file-utils libgl1-mesa-dev
  libglu1-mesa-dev mercurial autoconf automake groff curl lzop asciidoc python3-pip
3 apt-get install u-boot-tools libssl-dev
```

6. vim退格问题

```
1 sudo apt-get remove vim-common
2 sudo apt-get install vim
```

7. 安装卸载teamview

下载依赖包

```
1 sudo apt install gdebi-core
```

下载源码

```
1 wget https://download.teamviewer.com/download/linux/teamviewer_amd64.deb
```

安装

```
1 sudo gdebi teamviewer_amd64.deb
```

或者如下命令

```
1 dpkg -i teamviewer_amd64.deb
```

卸载

```
1 sudo apt --purge remove teamviewer
```

8.FTP服务器搭建

(1) 安装vsftp

```
1 sudo apt install vsftpd
```

(2) 启动FTP服务

```
1 sudo service vsftpd start && sudo service vsftpd status
```

(3) 修改配置文件（在修改之前最好备份一下）

```
1 sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.cp
2 sudo vim /etc/vsftpd.conf
```

编辑配置文件如下（直接复制不用改读写权限）：

```
1 # Example config file /etc/vsftpd.conf
2 #
3 # The default compiled in settings are fairly paranoid. This sample file
4 # loosens things up a bit, to make the ftp daemon more usable.
5 # Please see vsftpd.conf.5 for all compiled in defaults.
6 #
7 # READ THIS: This example file is NOT an exhaustive list of vsftpd options.
8 # Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
9 # capabilities.
10 #
11 #
12 # Run standalone? vsftpd can run either from an inetd or as a standalone
13 # daemon started from an initscript.
14 listen=NO
15 #
16 # This directive enables listening on IPv6 sockets. By default, listening
17 # on the IPv6 "any" address (:::) will accept connections from both IPv6
18 # and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
19 # sockets. If you want that (perhaps because you want to listen on specific
20 # addresses) then you must run two copies of vsftpd with two configuration
21 # files.
22 listen_ipv6=YES
23 #
24 # Allow anonymous FTP? (Disabled by default).
25 anonymous_enable=NO
26 #
27 # Uncomment this to allow local users to log in.
28 local_enable=YES
29 #
30 # Uncomment this to enable any form of FTP write command.
```

```
31 write_enable=YES
32 #
33 # Default umask for local users is 077. You may wish to change this to 022,
34 # if your users expect that (022 is used by most other ftpd's)
35 local_umask=022
36 #
37 # Uncomment this to allow the anonymous FTP user to upload files. This only
38 # has an effect if the above global write enable is activated. Also, you will
39 # obviously need to create a directory writable by the FTP user.
40 #anon_upload_enable=YES
41 #
42 # Uncomment this if you want the anonymous FTP user to be able to create
43 # new directories.
44 #anon_mkdir_write_enable=YES
45 #
46 # Activate directory messages - messages given to remote users when they
47 # go into a certain directory.
48 dirmessage_enable=YES
49 #
50 # If enabled, vsftpd will display directory listings with the time
51 # in your local time zone. The default is to display GMT. The
52 # times returned by the MDTM FTP command are also affected by this
53 # option.
54 use_localtime=YES
55 #
56 # Activate logging of uploads/downloads.
57 xferlog_enable=YES
58 #
59 # Make sure PORT transfer connections originate from port 20 (ftp-data).
60 connect_from_port_20=YES
61 #
62 # If you want, you can arrange for uploaded anonymous files to be owned by
63 # a different user. Note! Using "root" for uploaded files is not
64 # recommended!
65 #chown_uploads=YES
66 #chown_username=whoever
67 #
68 # You may override where the log file goes if you like. The default is shown
69 # below.
70 #xferlog_file=/var/log/vsftpd.log
```

```
71 #
72 # If you want, you can have your log file in standard ftpd xferlog format.
73 # Note that the default log file location is /var/log/xferlog in this case.
74 #xferlog_std_format=YES
75 #
76 # You may change the default value for timing out an idle session.
77 #idle_session_timeout=600
78 #
79 # You may change the default value for timing out a data connection.
80 #data_connection_timeout=120
81 #
82 # It is recommended that you define on your system a unique user which the
83 # ftp server can use as a totally isolated and unprivileged user.
84 #nopriv_user=ftpsecure
85 #
86 # Enable this and the server will recognise asynchronous ABOR requests. Not
87 # recommended for security (the code is non-trivial). Not enabling it,
88 # however, may confuse older FTP clients.
89 #async_abor_enable=YES
90 #
91 # By default the server will pretend to allow ASCII mode but in fact ignore
92 # the request. Turn on the below options to have the server actually do ASCII
93 # mangling on files when in ASCII mode.
94 # Beware that on some FTP servers, ASCII support allows a denial of service
95 # attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
96 # predicted this attack and has always been safe, reporting the size of the
97 # raw file.
98 # ASCII mangling is a horrible feature of the protocol.
99 #ascii_upload_enable=YES
100 #ascii_download_enable=YES
101 #
102 # You may fully customise the login banner string:
103 #ftpd_banner=Welcome to blah FTP service.
104 #
105 # You may specify a file of disallowed anonymous e-mail addresses. Apparently
106 # useful for combatting certain DoS attacks.
107 #deny_email_enable=YES
108 # (default follows)
109 #banned_email_file=/etc/vsftpd.banned_emails
```

```
110 #
111 # You may restrict local users to their home directories. See the FAQ for
112 # the possible risks in this before using chroot_local_user or
113 # chroot_list_enable below.
114 #chroot_local_user=YES
115 #
116 # You may specify an explicit list of local users to chroot\(\) to their home
117 # directory. If chroot_local_user is YES, then this list becomes a list of
118 # users to NOT chroot\(\).
119 # (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
120 # the user does not have write access to the top level directory within the
121 # chroot)
122 #chroot_local_user=YES
123 #chroot_list_enable=YES
124 # (default follows)
125 #chroot_list_file=/etc/vsftpd.chroot_list
126 #
127 # You may activate the "-R" option to the builtin ls. This is disabled by
128 # default to avoid remote users being able to cause excessive I/O on large
129 # sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
130 # the presence of the "-R" option, so there is a strong case for enabling it.
131 #ls_recurse_enable=YES
132 #
133 # Customization
134 #
135 # Some of vsftpd's settings don't fit the filesystem layout by
136 # default.
137 #
138 # This option should be the name of a directory which is empty. Also, the
139 # directory should not be writable by the ftp user. This directory is used
140 # as a secure chroot\(\) jail at times vsftpd does not require filesystem
141 # access.
142 secure_chroot_dir=/var/run/vsftpd/empty
143 #
144 # This string is the name of the PAM service vsftpd will use.
145 pam_service_name=vsftpd
146 #
147 # This option specifies the location of the RSA certificate to use for SSL
148 # encrypted connections.
149 rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
```

```
150 rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
151 ssl_enable=NO
152
153 #
154 # Uncomment this to indicate that vsftpd use a utf8 filesystem.
155 #utf8_filesystem=YES
156
```

(4) 重启vsftp服务

```
1 sudo service vsftpd restart
```

9.HTTP服务器搭建

(1) 安装apache2

```
1 $ sudo apt install -y apache2
```

(2) 配置环境

默认是80端口，防止冲突自定义端口：8001

1.修改 /etc/apache2/ports.conf文件监听端口

```
1 Listen 8001 ## 其它行不变
```

2.修改/etc/apache2/sites-enabled/000-default.conf文件端口与访问目录

```
1 <VirtualHost *:8001> ## 其他行不变
2 DocumentRoot /var/www/html ## 浏览器访问目录
```

3.删除html网页文件

```
1 $ sudo rm /var/www/html/index.html
2 ps: 不删除，登录 http://{hostIP}:8001会进入网页
```


4.重启服务

```
1 $ sudo /etc/init.d/apache2 restart
```

(3) 虚拟目录

配置文件路径: /etc/apache2/apache2.conf

参数: Alias [虚拟目录] [物理目录]

虚拟目录的作用是隐藏真实的物理路径, 输入虚拟路径即可访问对应物理路径的内容

```
1 # 对物理路径授权
2 <Directory /var/www/html>
3     AllowOverride None
4     Require all granted
5 </Directory>
```

重启服务

```
1 $ sudo /etc/init.d/apache2 restart
```

(4) 测试

测试访问: 登录 `http://{hostIP}:8001`, 成功访问到/var/www/html/目录下文件2.测试下载, 点击网页上文件, 成功下载

10.NFS环境搭建

(1) 在Ubuntu安装NFS并启动

安装NFS

```
1 sudo apt install nfs-kernel-server
```

创建NFS共享目录

```
1 cd /
2 mkdir nfsShare
```

启动NFS服务

```
1 sudo /etc/init.d/nfs-kernel-server restart
```

(2) 修改配置文件

```
1 sudo vim /etc/exports
```

在配置文件中添加：

```
1 /nfsShare *(rw,sync,no_root_squash)
```

再次重启NFS服务

```
1 sudo /etc/init.d/nfs-kernel-server restart
2 sudo /etc/init.d/nfs-kernel-server status
```

(3) 板端挂载NFS共享目录

在板端根目录创建nfs文件

```
1 cd /root
2 mkdir nfs
```

板端挂载NFS目录

```
1 mount -t nfs 192.168.10.14:/nfsShare /root/nfs -o nolock
```

注意：这里192.168.10.14是指Ubuntu的IP地址

