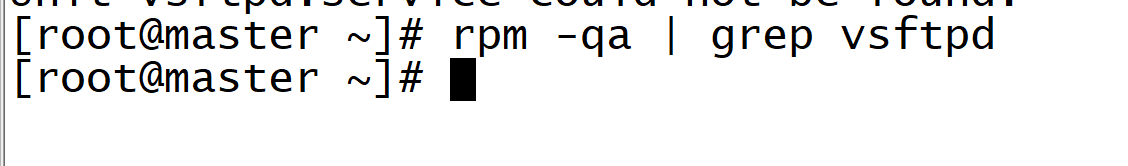
# 检查环境

检查机器是否安装 vsftpd 服务：

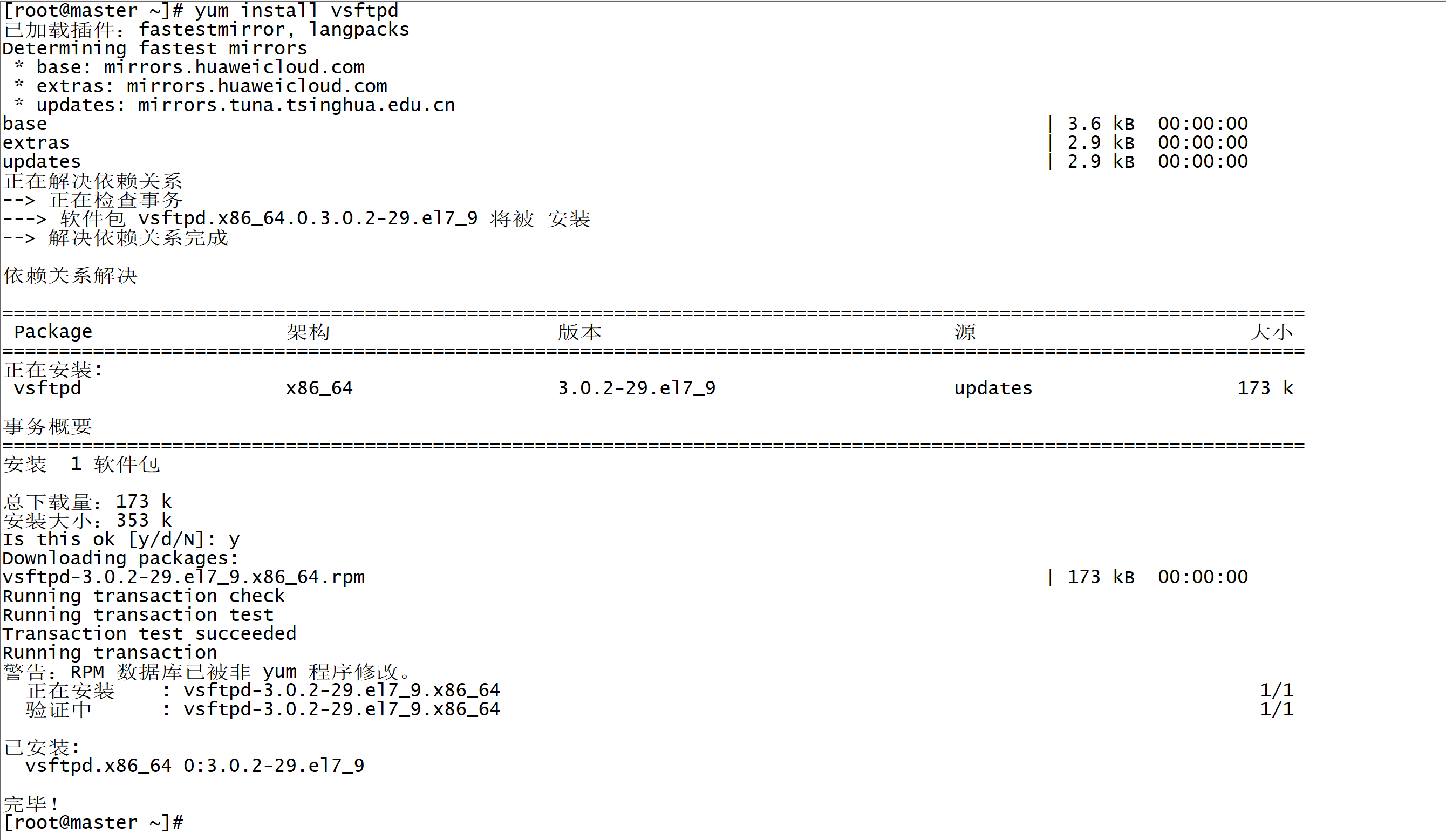
|  |
| --- |
| $ rpm -qa | grep vsftpd |



# 安装vsftpd服务

若未安装，执行如下命令进行安装：

|  |
| --- |
| $ yum install vsftpd |

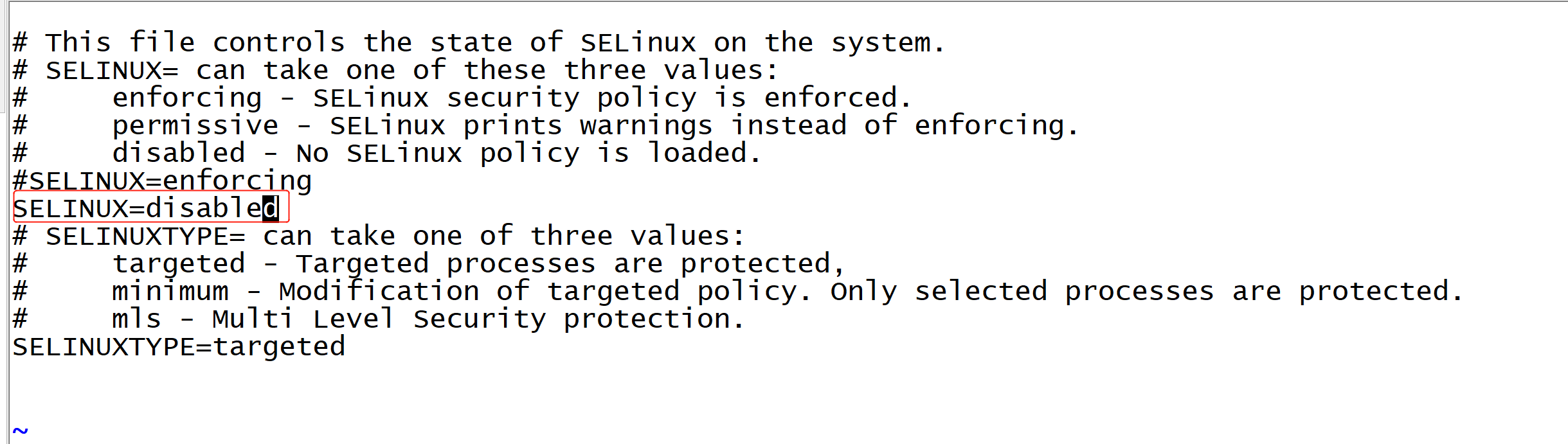


# 启动服务

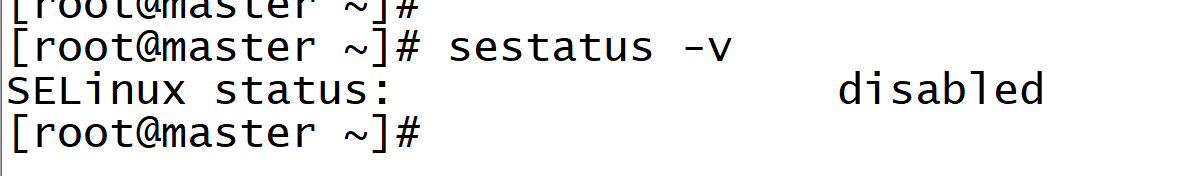
### 禁用 selinux

启动服务前需要禁用 selinux

|  |
| --- |
| $ vi /etc/selinux/config |
| # 将 SELINUX 设置为 disabled |



重启系统后生效：

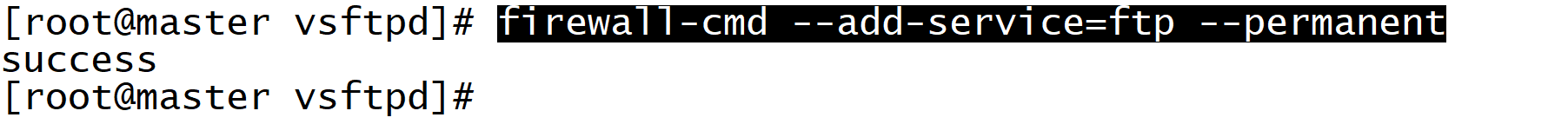


### 开通防火墙

两种方式： 直接开通服务或者开通服务的端口

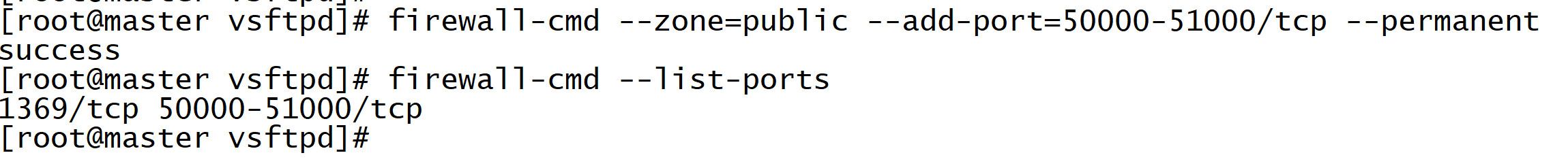
1. 直接开通防火墙的ftp服务

|  |
| --- |
| $ firewall-cmd --add-service=ftp --permanent |



1. 开放ftp服务的端口

|  |
| --- |
| $ firewall-cmd --zone=public --add-port=50000-51000/tcp --permanent |



CentOS 7 ：

|  |
| --- |
| $ systemctl start vsftpd.service |

CentOS 6 等早期版本使用如下命令：

|  |
| --- |
| $ service vsftpd start |

查看服务状态：

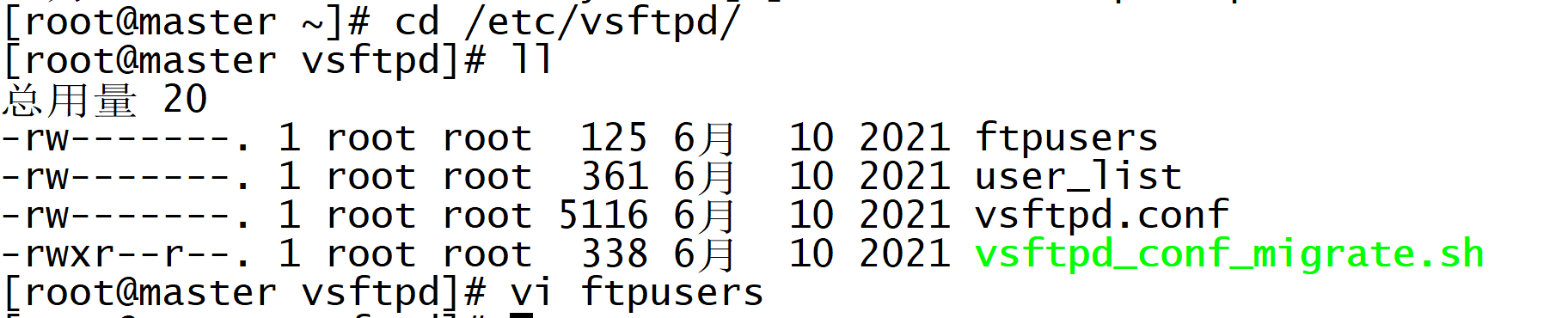
|  |
| --- |
| $ systemctl status vsftpd.service |



# vsftpd服务配置

## 配置文件

主要配置文件都位于 /etc/vsftpd/ 目录下



* ftpusers

用来指定不能通过ftp进行登录的用户(黑名单，不受任何参数限制)

* user\_list

既可以用作白名单，也可用作黑名单，由vsftpd.conf 文件中的配置参数 userlist\_enable 和 userlist\_deny 决定

黑名单(在user\_list文件中的用户都不能通过ftp进行登录)：

|  |
| --- |
| userlist\_enable=YES  userlist\_deny=YES |

白名单(除user\_list文件中的用户，都不能通过ftp进行登录)：

|  |
| --- |
| userlist\_enable=YES  userlist\_deny=NO |

若userlist\_enable参数配置为 NO，则不管 userlist\_deny配置如何，user\_list配置文件都将失效

* vsftpd.conf

vsftpd服务的主要配置文件

## vsftpd.conf 详解

vsftpd.conf 的配置项特别多，若要查看所有配置项，可以参考 vsftpd.conf.5 帮助手册

|  |
| --- |
| $ man vsftpd.conf |

这里列举一些常用的配置项进行说明：

|  |
| --- |
| anonymous\_enable=NO  local\_enable=YES  write\_enable=YES  local\_umask=022  dirmessage\_enable=YES  xferlog\_enable=YES  xferlog\_std\_format=YES  # chroot\_list 文件中指定的用户具有切换目录的权限  chroot\_local\_user=YES  chroot\_list\_enable=YES  chroot\_list\_file=/etc/vsftpd/chroot\_list  # 以 standalone 模式运行 vsftpd 服务  listen=YES  # 修改ftp连接的端口为 1369  listen\_port=1369  # 关闭主动模式  port\_enable=NO  # 开启被动模式  pasv\_enable=YES  # 被动模式数据传输端口最小值  pasv\_min\_port=50000  # 被动模式数据传输端口最大值  pasv\_max\_port=51000  pasv\_address=10.0.110.10  # 启用 user\_list， user\_list 文件中的用户将被拒绝连接  userlist\_enable=YES  tcp\_wrappers=YES  # 启用虚拟用户  guest\_enable=YES  pam\_service\_name=/etc/pam.d/vsftpd  # 虚拟用户名称  guest\_username=vsftpd  # 虚拟用户权限与本地用户一样  virtual\_use\_local\_privs=YES  # 用户配置目录  user\_config\_dir=/etc/vsftpd/ftplogin  # 最好配置上，否则当目录具有写权限的时候，进入目录会报错  allow\_writeable\_chroot=YES |

# ftp传输模式

## 主动模式

21端口

接收ftp命令

ftp服务端

发送ftp命令

ftp客户端

20端口

传输数据

传输数据

在主动模式下，ftp客户端会给服务端的21端口发送ftp命令，告诉服务端我已打开自己的20端口，请向我的20端口发起TCP连接来传输文件，服务端接收到命令后，会主动向客户端的20端口发起连接，连接成功后开始传输文件。

**注意：主动模式下，ftp请求是由客户端发起的，传输数据的时候TCP连接是由服务端发起的。**

## 被动模式

ftp客户端

发送ftp命令

传输数据

ftp服务端

接收ftp命令

传输数据

21端口

高位端口

**在被动模式下，不管是ftp命令还是数据传输，都是由客户端向服务端发起TCP连接，服务端在接收到ftp命令后会打开一个空闲的高位端口。**

**在共享网络环境下，只能使用被动模式**。因为主动模式需要服务端向客户端发起请求，而共享网络的客户端和服务端中间隔了个公网网关，服务端只能向公网地址的20端口发送请求，共享网络中设备的内部地址是无法收到这个请求的。