FTP服务的简介和配置详解

**FTP服务的简介和配置详解**

**(1)anonymous(\***\*匿名帐号)\*\*

使用anonymous是应用广泛的一种FTP服务器.如果用户在FTP服务器上没有帐号,那么用户可以以anonymous为用户名,以自己的电子邮件地址为密码进行登录.当匿名用户登录FTP服务器后,其登录目录为匿名FTP服务器的根目录/var/ftp.为了减轻FTP服务器的负载,一般情况下,应关闭匿名帐号的上传功能.

**(2)real(\***\*真实帐号)\*\*

real也称为本地帐号,就是以真实的用户名和密码进行登录,但前提条件是用户在FTP服务器上拥有自己的帐号.用真实帐号登录后,其登录的目录为用户自己的目录,该目录在系统建立帐号时系统就自动创建.

**(3)guest(\***\*虚拟帐号)\*\*

如果用户在FTP服务器上拥有帐号,但此帐号只能用于文件传输服务,那么该帐号就是guest,guest是真实帐号的一种形式,它们的不同之处在于,geust登录FTP服务器后,不能访问除宿主目录以外的内容.

1．登录和对匿名用户的设置 write\_enable=YES //是否对登录用户开启写权限。属全局性设置。默认NO local\_enable=YES //是否允许本地用户登录FTP服务器。默认为NO anonymous\_enable=YES //设置是否允许匿名用户登录FTP服务器。默认为YES ftp\_username=ftp //定义匿名用户的账户名称，默认值为ftp。 no\_anon\_password=YES //匿名用户登录时是否询问口令。设置为YES，则不询问。默 认NO anon\_world\_readable\_only=YES //匿名用户是否允许下载可阅读的文档，默认为YES。 anon\_upload\_enable=YES //是否允许匿名用户上传文件。只有在write\_enable设置

local\_root=/var/ftp // 设置本地用户登录后所在的目录。默认配置文件中没有设置该项，此时用户登录FTP服务器后，所在的目录为该用户的主目录，对于root用户，则为/root目录。 anon\_root=/var/ftp //设置匿名用户登录后所在的目录。若未指定，则默认为/var/ftp目录。

　　通过搭配能实现以下几种效果： 　　　　①当chroot\_list\_enable=YES，chroot\_local\_user=YES时，在/etc/vsftpd.chroot\_list文件中列出的用户，可以切换到其他目录；未在文件中列出的用户，不能切换到其他目录。 　　　　②当chroot\_list\_enable=YES，chroot\_local\_user=NO时，在/etc/vsftpd.chroot\_list文件中列出的用户，不能切换到其他目录；未在文件中列出的用户，可以切换到其他目录。 　　　　③当chroot\_list\_enable=NO，chroot\_local\_user=YES时，所有的用户均不能切换到其他目录。 　　　　④当chroot\_list\_enable=NO，chroot\_local\_user=NO时，所有的用户均可以切换到其他目录。

**注意：配置FTP服务时，最好关闭防火墙和selinux**

**1、FTP服务简介**

FTP 是File Transfer Protocol（[文件传输协议](https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE)）的英文简称，而中文简称为“文件传输协议”。用于Internet上的[控制文件](https://baike.baidu.com/item/%E6%8E%A7%E5%88%B6%E6%96%87%E4%BB%B6)的双向传输。同时，它也是一个[应用程序](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E7%A8%8B%E5%BA%8F)（Application）。基于不同的操作系统有不同的FTP应用程序，而所有这些应用程序都遵守同一种协议以传输文件。在FTP的使用当中，用户经常遇到两个概念："下载"（Download）和"上传"（Upload）。"下载"文件就是从远程主机拷贝文件至自己的计算机上；"上传"文件就是将文件从自己的计算机中拷贝至远程主机上。用Internet语言来说，用户可通过客户机程序向（从）远程主机上传（下载）文件，由于FTP的文件传输是明文方式，具有一定危险性，所以就诞生了一种更加安全的传输方式vsftp，下面主要介绍vsftp的特性及相关配置。

**2、VSFTP特点**

VSFTP是一个比FTP更安全的软件具有以下特点：

（1）vsftp一般以普通用户运行，降低了进程的权限，提高了安全性

（2）任何需要执行较高权限的指令都需要上层程序的许可

（3）ftp的命令都被整合到了vsftp中，不需要系统额外提供命令

（4）用于chroot功能，可以改变用户的根目录，限制用户只能在自己的家目录

（5）vsftpd 是一个基于GPL发布的FTP服务器软件。其中的vs是“ Very Secure”的缩写，由此名称缩写可以看出，本服务器的初衷就是服务的安全性。

（6）vsftpd是RedHat Linux默认使用的ftp服务端软件。

（7）vsftpd不再依赖于xinetd服务

（8）vsftpd可同时允许匿名（ anonymous ）与本地用户(local)访问,还可以支持虚拟用户。

**3、VSFTP连接类型**

控制连接：TCP 21，用于发送FTP命令信息

数据连接：TCP 20，用于上传、下载数据

**4、Vsftp工作模式**

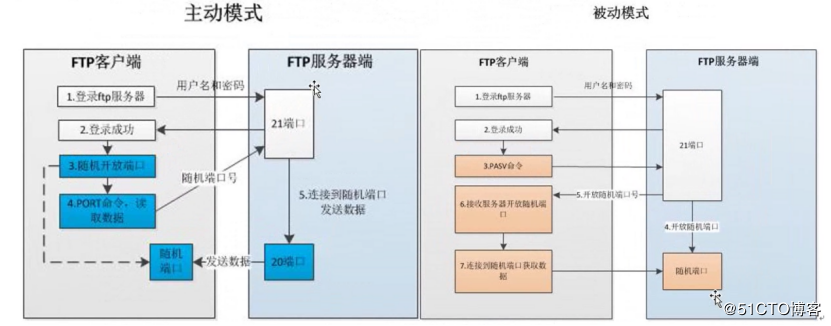
**FTP协议有两种工作方式：PORT方式和PASV方式,中文意思为主动式和[被动式](http://baike.so.com/doc/586709-621078.html)**

主动模式：服务端从20端口主动向客户端发起连接

被动模式：服务端在指定范围内某个端口被动等待客户端连接

主动模式端口分配：控制端口 21  传输数据端口 20

被动模式端口分配：控制端口 21  传输数据端口 随机



**5、VSFTP传输模式**

（1）文本模式：ASCII模式，以文本序列传输数据

（2）二进制模式：Binary模式，以二进制序列传输数据

**6、FTP用户的类型**

（1）匿名用户：anonymous或ftp

（2）本地用户：帐号名称、密码等信息保存在passwd/shadow文件中

（3）虚拟用户：使用独立的帐号/密码数据文件

**7、VSFTP配置文件介绍**

|  |  |
| --- | --- |
| 配置文件作用 | 配置文件路径 |
| vsftpd的可执行文件（主程序） | /usr/sbin/vsftpd |
| vsftpd启动脚本 | /etc/rc.d/init.d/vsftpd |
| vsftpd主配置文件 | /etc/vsftpd/vsftpd.conf |
| vsftpd的PAM认证文件 | /etc/pam.d/vsftpd |
| 禁止使用vsftpd的用户列表文件 | /etc/vsftpd/ftpusers |
| 禁止或允许使用vsftpd的用户列表文件 | /etc/vsftpd/user\_list |
| 匿名用户主目录 | /var/ftp |

**8、vsftpd.conf文件常用的配置参数说明**

**（1）常用的全局配置**

listen\_address=192.168.4.1         **设置监听的IP地址**

listen=YES                        **是否以独立运行的方式监听服务**

listen\_port=21                    **设置监听FTP服务的端口号**

write\_enable=YES                **是否启用写入权限**

download\_enable＝YES             **是否允许下载文件**

max\_clients=0                    **限制并发客户端连接数**

max\_per\_ip=0                   **限制同一IP地址的并发连接数**

pasv\_enable=yes                  **设置最小的被动端口号**

pasv\_min\_port=9981              **设置最小的被动端口号**

pasv\_max\_port=9981              **设置最大的被动端口号**

dirmessage\_enable=yes           **是否显示目录说明文件**

xferlog\_enable=yes                 **是否记录ftp传输过程**

xferlog\_file=/var/log/vsftpd.log      **日志的路径和名字**

xferlog\_std\_format=yes             **是否使用标准的ftp xferlog**

chown\_username=username  **是否改变上传文件的属主，如果是则需要输入一个系统用户名**

idle\_session\_timeout=600          **设置默认不活跃session时间**

date\_connection\_timeout=120       **设置数据传输超时时间**

ftpd\_banner=welcome to ftp server    **定制欢迎信息**

**（2）本地用户访问限制**

userlist\_enable=YES        **是否启用user\_list列表文件**

userlist\_deny=YES         **是否禁用user\_list中的用户**

**（3）本地用户权限控制**

local\_enable=YES           **是否启用本地系统用户**

local\_umask=022           **本地用户所上传文件的权限掩码**

local\_root=/var/ftp         **设置本地用户的FTP根目录**

chroot\_local\_user=YES       **是否将用户禁锢在主目录**

local\_max\_rate=0           **限制最大传输速率（字节/秒）**

chroot\_list\_enable=YES     **配合下面的文件使用**

chroot\_list\_file=/etc/vsftpd/chroot\_list   **配合使用，列表中的用户将被禁锢在目录中**

**说明：本地用户的权限除了使用以上的参数控制以外，还可以使用系统的权限进行控制。ftp的权限和系统的权限都允许时才会放行，只要有一方权限不足使用FTP就会出现权限不足。**

**（4）匿名权限控制**

anonymous\_enable=YES        **启用匿名访问**

anon\_umask=022            **匿名用户所上传文件的权限掩码**

anon\_root=/var/ftp            **匿名用户的FTP根目录**

anon\_word\_readable\_only=YES  **允许匿名下载**

anon\_upload\_enable=YES      **允许上传文件anon\_mkdir\_write\_enable=YES：允许创建目录**

anon\_other\_write\_enable=YES   **开放其他写入权**

anon\_max\_rate=0             **限制最大传输速率（字节/秒）**

**说明：匿名用户账号名称默认为ftp或anonymous，不需要登录密码，默认只能下载无法上传。**

**9、配置拥有所有权限的匿名用户**

**说明：这里为了展示匿名用户的所有功能才这样配置，实际中不能这样配置。**

**（1）安装vsftp软件，并按照下面配置修改配置文件**

[root@localhost ~]# yum -y install vsftpd

[root@localhost ~]# chown ftp /var/ftp/pub/

[root@localhost ~]# cp -a /etc/vsftpd/vsftpd.conf  /etc/vsftpd/vsftpd.conf.back

[root@localhost ~]# vim /etc/vsftpd/vsftpd.conf

anonymous\_enable=YES     **启用匿名访问**

anon\_upload\_enable=YES    **允许匿名用户可上传文件**

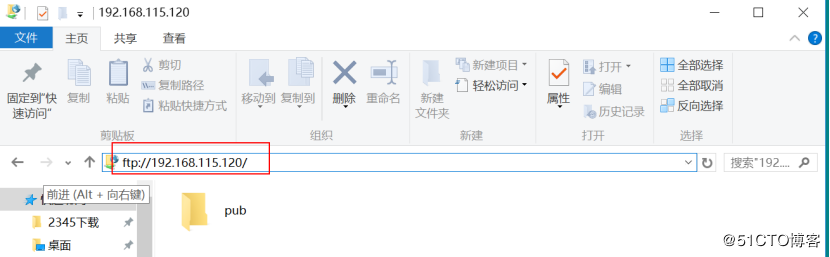
anon\_mkdir\_write\_enable=YES   **允许匿名用户可创建目录**

anon\_other\_write\_enable=YES   **开放其他写入权比如改名，需要手动添加**

[root@localhost ~]# systemctl restart vsftpd

**（2）在windows上或者Linux上测试即可**

a、在Windows上文件里面的地址栏输入ftp://192.168.115.120/，如下所示：



输入地址以后，进入pub目录测试能否上传文件、删除文件、创建目录、给文件改名等功能。

**b、在Linux中匿名登陆FTP服务器需要先yum install ftp软件，然后输入ftp 192.168.115.120，之后输入用户ftp或者anonymous，密码为空回车即可登陆。**

**10、配置ftp本地用户的访问控制**

**（1）把之前的虚拟机还原，重新安装vsftpd软件并创建本地用户**

[root@localhost ~]# yum -y install vsftpd

[root@localhost ~]# chown ftp /var/ftp/pub/

[root@localhost ~]# cp -a /etc/vsftpd/vsftpd.conf  /etc/vsftpd/vsftpd.conf.back

[root@localhost ~]# useradd user1

[root@localhost ~]# useradd user2

[root@localhost ~]# useradd user3

[root@localhost ~]# echo '123456' | passwd --stdin user1

[root@localhost ~]# echo '123456' | passwd --stdin user2

[root@localhost ~]# echo '123456' | passwd --stdin user3

**（2）修改配置文件设置本地用户的访问控制**

[root@localhost ~]# vim /etc/vsftpd/vsftpd.conf

local\_enable=YES     **启用本地系统用户**

local\_umask=000      **修改权限掩码为000，用系统的setfacl权限限制即可**

chroot\_local\_user=YES   **是否将用户禁锢在local\_root设置的目录**

local\_root=/var/ftp    **设置本地用户的FTP根目录**

chroot\_list\_enable=YES   **是否启用列表控制，启用后和chroot\_list\_file配合使用**

chroot\_list\_file=/etc/vsftpd/chroot\_list  **该文件要自己创建，列表中的用户将被禁锢在目录中**

userlist\_enable=YES      **是否开启用户列表访问控制**

userlist\_deny=YES        **拒绝访问FTP用户列表是否启用**

[root@localhost ~]# systemctl restart vsftpd

**说明：**userlist\_enable=YES对应/etc/vsftpd/user\_list文件灵活控制用户访问

（a） userlist\_enable=YES

userlist\_deny=YES

满足这两个条件时，出现在user\_list文件里的用户会被拒绝访问FTP服务器

（b） userlist\_enable=YES

userlist\_deny=NO

满足这两个条件时，只允许出现在user\_list文件里的用户登录FTP服务器

（c）只要出现在/etc/vsftpd/ftpusers文件里的用户都禁止登陆FTP服务器，优先级要高于上面的user\_list文件

**（3）在Windows或Linux中测试上面的配置是否生效**

（a）在Windows测试输入：[ftp://192.168.115.106](ftp://192.168.115.106/)之后输入对应的本地用户名和密码登录测试。

（b）在Linux测试之前先yum安装ftp软件，然后输入[ftp 192.168.115.106回车然](ftp://ftp%20192.168.115.xn--106-7g6ei81j131b/)后输入对应的本地用户名回车然后输入密码回车即可进行登录测试 。

（c）如果需要不同用户给予不同的访问权限，可以使用系统的setfacl进行设置。

**11、修改vsftpd服务的监听地址、端口**

[root@localhost ~]# vim /etc/vsftpd/vsftpd.conf

listen=YES    **是否开启监听地址和端口**

listen\_address=192.168.115.120     **监听的IP地址，写FTP服务器的地址**

listen\_port=2100     **监听的端口，默认为21，建议不修改**

**注意：上面最后两行的参数需要手动写入。**

**12、开启使用FTP服务器的被动模式**

[root@localhost ~]# vim /etc/vsftpd/vsftpd.conf

pasv\_enable=YES       **是否开启被动模式**

pasv\_min\_port=24500    **传输数据时随机端口最小值**

pasv\_max\_port=24600    **传输数据时随机端口最大值**

**注意：上面三行的参数需要手动写入。**