**vsftpd配置文件详解**

本项目要用到的配置项：

1）local\_root=/ftpfile(当本地用户登入时，将被更换到定义的目录下，默认值为各用户的家目录)

2）anon\_root=/ftpfile(使用匿名登入时，所登入的目录)

3）use\_localtime=YES(默认是GMT时间，改成使用本机系统时间)

4）anonymous\_enable=NO(不允许匿名用户登录)

5）local\_enable=YES(允许本地用户登录)

6）write\_enable=YES(本地用户可以在自己家目录中进行读写操作)

7）local\_umask=022(本地用户新增档案时的umask值)

8）dirmessage\_enable=YES(如果启动这个选项，那么使用者第一次进入一个目录时，会检查该目录下是否有.message这个档案，如果有，则会出现此档案的内容，通常这个档案会放置欢迎话语，或是对该目录的说明。默认值为开启)

9）xferlog\_enable=YES(是否启用上传/下载日志记录。如果启用，则上传与下载的信息将被完整纪录在xferlog\_file 所定义的档案中。预设为开启。)

10）connect\_from\_port\_20=YES(指定FTP使用20端口进行数据传输，默认值为YES)

11）xferlog\_std\_format=YES(如果启用，则日志文件将会写成xferlog的标准格式)

12）ftpd\_banner=Welcome to mmall FTP Server(这里用来定义欢迎话语的字符串)

13）chroot\_local\_user=NO(用于指定用户列表文件中的用户是否允许切换到上级目录)

14）chroot\_list\_enable=YES(设置是否启用chroot\_list\_file配置项指定的用户列表文件)

15）chroot\_list\_file=/etc/vsftpd/chroot\_list(用于指定用户列表文件)

16）listen=YES(设置vsftpd服务器是否以standalone模式运行，以standalone模式运行是一种较好的方式，此时listen必须设置为YES，此为默认值。建议不要更改，有很多与服务器运行相关的配置命令，需要在此模式下才有效，若设置为NO，则vsftpd不是以独立的服务运行，要受到xinetd服务的管控，功能上会受到限制)

17）pam\_service\_name=vsftpd(虚拟用户使用PAM认证方式，这里是设置PAM使用的名称，默认即可，与/etc/pam.d/vsftpd对应) userlist\_enable=YES(是否启用vsftpd.user\_list文件，黑名单,白名单都可以

18)pasv\_min\_port=61001(被动模式使用端口范围最小值)

19)pasv\_max\_port=62000(被动模式使用端口范围最大值)

20)pasv\_enable=YES(pasv\_enable=YES/NO（YES）

若设置为YES，则使用PASV工作模式；若设置为NO，则使用PORT模式。默认值为YES，即使用PASV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。

一、PORT（主动）方式的连接过程是：客户端向服务器的FTP端口（默认是21）发送连接请求，服务器接受连接，建立一条命令链路。

当需要传送数据时，客户端在命令链路上用 PORT命令告诉服务器：“我打开了\*\*\*\*端口，你过来连接我”。于是服务器从20端口向客户端的\*\*\*\*端口发送连接请求，建立一条数据链路来传送数据。

二、PASV（被动）方式的连接过程是：客户端向服务器的FTP端口（默认是21）发送连接请求，服务器接受连接，建立一条命令链路。

当需要传送数据时，服务器在命令链路上用 PASV命令告诉客户端：“我打开了\*\*\*\*端口，你过来连接我”。于是客户端向服务器的\*\*\*\*端口发送连接请求，建立一条数据链路来传送数据。

从上面可以看出，两种方式的命令链路连接方法是一样的，而数据链路的建立方法就完全不同。而FTP的复杂性就在于此。

**1.默认配置：**

1>允许匿名用户和本地用户登陆。

anonymous\_enable=YES

local\_enable=YES

2>匿名用户使用的登陆名为ftp或anonymous，口令为空；匿名用户不能离开匿名用户家目录/var/ftp,且只能下载不能上传。

3>本地用户的登录名为本地用户名，口令为此本地用户的口令；本地用户可以在自 己家目录中进行读写操作；本地用户可以离开自家目录切换至有权限访问的其他目录，并在权限允许的情况下进行上传/下载。

write\_enable=YES

4>写在文件/etc/vsftpd.ftpusers中的本地用户禁止登陆。

**2.配置文件格式：**

vsftpd.conf 的内容非常单纯，每一行即为一项设定。若是空白行或是开头为#的一行，将会被忽略。内容的格式只有一种，如下所示：

option=value

要注意的是，等号两边不能加空白。

**3.匿名用户（anonymous）设置**

**anonymous\_enable=YES/NO（YES）**

控制是否允许匿名用户登入，YES 为允许匿名登入，NO 为不允许。默认值为YES。

**write\_enable=YES/NO（YES）**

是否允许登陆用户有写权限。属于全局设置，默认值为YES。

**no\_anon\_password=YES/NO（NO）**

若是启动这项功能，则使用匿名登入时，不会询问密码。默认值为NO。

**ftp\_username=ftp**

定义匿名登入的使用者名称。默认值为ftp。

**anon\_root=/var/ftp**

使用匿名登入时，所登入的目录。默认值为/var/ftp。注意ftp目录不能是777的权限属性，即匿名用户的家目录不能有777的权限。

**anon\_upload\_enable=YES/NO（NO）**

如果设为YES，则允许匿名登入者有上传文件（非目录）的权限，只有在write\_enable=YES时，此项才有效。当然，匿名用户必须要有对上层目录的写入权。默认值为NO。

**anon\_world\_readable\_only=YES/NO（YES）**

如果设为YES，则允许匿名登入者下载可阅读的档案（可以下载到本机阅读，不能直接在FTP服务器中打开阅读）。默认值为YES。

**anon\_mkdir\_write\_enable=YES/NO（NO）**

如果设为YES，则允许匿名登入者有新增目录的权限，只有在write\_enable=YES时，此项才有效。当然，匿名用户必须要有对上层目录的写入权。默认值为NO。

**anon\_other\_write\_enable=YES/NO（NO）**

如果设为YES，则允许匿名登入者更多于上传或者建立目录之外的权限，譬如删除或者重命名。（如果anon\_upload\_enable=NO，则匿名用户不能上传文件，但可以删除或者重命名已经存在的文件；如果anon\_mkdir\_write\_enable=NO，则匿名用户不能上传或者新建文件夹，但可以删除或者重命名已经存在的文件夹。）默认值为NO。

**chown\_uploads=YES/NO（NO）**

设置是否改变匿名用户上传文件（非目录）的属主。默认值为NO。

**chown\_username=username**

设置匿名用户上传文件（非目录）的属主名。建议不要设置为root。

**anon\_umask=077**

设置匿名登入者新增或上传档案时的umask 值。默认值为077，则新建档案的对应权限为700。

**deny\_email\_enable=YES/NO（NO）**

若是启动这项功能，则必须提供一个档案/etc/vsftpd/banner\_emails，内容为email address。若是使用匿名登入，则会要求输入email address，若输入的email address 在此档案内，则不允许进入。默认值为NO。

**banned\_email\_file=/etc/vsftpd/banner\_emails**

此文件用来输入email address，只有在deny\_email\_enable=YES时，才会使用到此档案。若是使用匿名登入，则会要求输入email address，若输入的email address 在此档案内，则不允许进入。

**4.本地用户设置**

**local\_enable=YES/NO（YES）**

控制是否允许本地用户登入，YES 为允许本地用户登入，NO为不允许。默认值为YES。

**local\_root=/home/username**

当本地用户登入时，将被更换到定义的目录下。默认值为各用户的家目录。

**write\_enable=YES/NO（YES）**

是否允许登陆用户有写权限。属于全局设置，默认值为YES。

**local\_umask=022**

本地用户新增档案时的umask 值。默认值为077。

**file\_open\_mode=0755**

本地用户上传档案后的档案权限，与chmod 所使用的数值相同。默认值为0666。

**5.欢迎语设置**

**dirmessage\_enable=YES/NO（YES）**

如果启动这个选项，那么使用者第一次进入一个目录时，会检查该目录下是否有.message这个档案，如果有，则会出现此档案的内容，通常这个档案会放置欢迎话语，或是对该目录的说明。默认值为开启。

**message\_file=.message**

设置目录消息文件，可将要显示的信息写入该文件。默认值为.message。

**banner\_file=/etc/vsftpd/banner**

当使用者登入时，会显示此设定所在的档案内容，通常为欢迎话语或是说明。默认值为无。如果欢迎信息较多，则使用该配置项。

**ftpd\_banner=Welcome to BOB's FTP server**

这里用来定义欢迎话语的字符串，banner\_file是档案的形式，而ftpd\_banner 则是字符串的形式。预设为无。

**6.控制用户是否允许切换到上级目录**

在默认配置下，本地用户登入FTP后可以使用cd命令切换到其他目录，这样会对系统带来安全隐患。可以通过以下三条配置文件来控制用户切换目录。

**chroot\_list\_enable=YES/NO（NO）**

设置是否启用chroot\_list\_file配置项指定的用户列表文件。默认值为NO。

**chroot\_list\_file=/etc/vsftpd.chroot\_list**

用于指定用户列表文件，该文件用于控制哪些用户可以切换到用户家目录的上级目录。

**chroot\_local\_user=YES/NO（NO）**

用于指定用户列表文件中的用户是否允许切换到上级目录。默认值为NO。

**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。

**7.数据传输模式设置**

FTP在传输数据时，可以使用二进制方式，也可以使用ASCII模式来上传或下载数据。

**ascii\_upload\_enable=YES/NO（NO）**

设置是否启用ASCII 模式上传数据。默认值为NO。

**ascii\_download\_enable=YES/NO（NO）**

设置是否启用ASCII 模式下载数据。默认值为NO。

**8.访问控制设置**

两种控制方式：一种控制主机访问，另一种控制用户访问。

**①控制主机访问：**

**tcp\_wrappers=YES/NO（YES）**

设置vsftpd是否与tcp wrapper相结合来进行主机的访问控制。默认值为YES。如果启用，则vsftpd服务器会检查/etc/hosts.allow 和/etc/hosts.deny 中的设置，来决定请求连接的主机，是否允许访问该FTP服务器。这两个文件可以起到简易的防火墙功能。

比如：若要仅允许192.168.0.1—192.168.0.254的用户可以连接FTP服务器，则在/etc/hosts.allow文件中添加以下内容：

vsftpd:192.168.0. :allow

all:all :deny

**②控制用户访问：**

对于用户的访问控制可以通过/etc目录下的vsftpd.user\_list和ftpusers文件来实现。

**userlist\_file=/etc/vsftpd.user\_list**

控制用户访问FTP的文件，里面写着用户名称。一个用户名称一行。

**userlist\_enable=YES/NO（NO）**

是否启用vsftpd.user\_list文件。

**userlist\_deny=YES/NO（YES）**

决定vsftpd.user\_list文件中的用户是否能够访问FTP服务器。若设置为YES，则vsftpd.user\_list文件中的用户不允许访问FTP，若设置为NO，则只有vsftpd.user\_list文件中的用户才能访问FTP。

**/etc/vsftpd/ftpusers**文件专门用于定义不允许访问FTP服务器的用户列表（**注意**:如果userlist\_enable=YES,userlist\_deny=NO,此时如果在vsftpd.user\_list和ftpusers中都有某个用户时，那么这个用户是不能够访问FTP的，即ftpusers的优先级要高）。默认情况下vsftpd.user\_list和ftpusers，这两个文件已经预设置了一些不允许访问FTP服务器的系统内部账户。如果系统没有这两个文件，那么新建这两个文件，将用户添加进去即可。

**9.访问速率设置**

**anon\_max\_rate=0**

设置匿名登入者使用的最大传输速度，单位为B/s，0 表示不限制速度。默认值为0。

**local\_max\_rate=0**

本地用户使用的最大传输速度，单位为B/s，0 表示不限制速度。预设值为0。

**10.超时时间设置**

**accept\_timeout=60**

设置建立FTP连接的超时时间，单位为秒。默认值为60。

**connect\_timeout=60**

PORT 方式下建立数据连接的超时时间，单位为秒。默认值为60。

**data\_connection\_timeout=120**

设置建立FTP数据连接的超时时间，单位为秒。默认值为120。

**idle\_session\_timeout=300**

设置多长时间不对FTP服务器进行任何操作，则断开该FTP连接，单位为秒。默认值为300。

**11.日志文件设置**

**xferlog\_enable= YES/NO（YES）**

是否启用上传/下载日志记录。如果启用，则上传与下载的信息将被完整纪录在xferlog\_file 所定义的档案中。预设为开启。

**xferlog\_file=/var/log/vsftpd.log**

设置日志文件名和路径，默认值为/var/log/vsftpd.log。

**xferlog\_std\_format=YES/NO（NO）**

如果启用，则日志文件将会写成xferlog的标准格式，如同wu-ftpd 一般。默认值为关闭。

**log\_ftp\_protocol=YES|NO（NO）**

如果启用此选项，所有的FTP请求和响应都会被记录到日志中，默认日志文件在/var/log/vsftpd.log。启用此选项时，xferlog\_std\_format不能被激活。这个选项有助于调试。默认值为NO。

**12.定义用户配置文件**

在vsftpd中，可以通过定义用户配置文件来实现不同的用户使用不同的配置。

**user\_config\_dir=/etc/vsftpd/userconf**

设置用户配置文件所在的目录。当设置了该配置项后，用户登陆服务器后，系统就会到/etc/vsftpd/userconf目录下，读取与当前用户名相同的文件，并根据文件中的配置命令，对当前用户进行更进一步的配置。

例如：定义user\_config\_dir=/etc/vsftpd/userconf，且主机上有使用者 test1,test2，那么我们就在user\_config\_dir 的目录新增文件名为test1和test2两个文件。若是test1 登入，则会读取user\_config\_dir 下的test1 这个档案内的设定。默认值为无。利用用户配置文件，可以实现对不同用户进行访问速度的控制，在各用户配置文件中定义local\_max\_rate=XX，即可。

**13.FTP的工作方式与端口设置**

FTP有两种工作方式：PORT FTP（主动模式）和PASV FTP（被动模式）

**listen\_port=21**

设置FTP服务器建立连接所监听的端口，默认值为21。

**connect\_from\_port\_20=YES/NO**

指定FTP使用20端口进行数据传输，默认值为YES。

**ftp\_data\_port=20**

设置在PORT方式下，FTP数据连接使用的端口，默认值为20。

**pasv\_enable=YES/NO（YES）**

若设置为YES，则使用PASV工作模式；若设置为NO，则使用PORT模式。默认值为YES，即使用PASV工作模式。

**pasv\_max\_port=0**

在PASV工作模式下，数据连接可以使用的端口范围的最大端口，0 表示任意端口。默认值为0。

**pasv\_min\_port=0**

在PASV工作模式下，数据连接可以使用的端口范围的最小端口，0 表示任意端口。默认值为0。

**14.与连接相关的设置**

**listen=YES/NO（YES）**

设置vsftpd服务器是否以standalone模式运行。以standalone模式运行是一种较好的方式，此时listen必须设置为YES，此为默认值。建议不要更改，有很多与服务器运行相关的配置命令，需要在此模式下才有效。若设置为NO，则vsftpd不是以独立的服务运行，要受到xinetd服务的管控，功能上会受到限制。

**max\_clients=0**

设置vsftpd允许的最大连接数，默认值为0，表示不受限制。若设置为100时，则同时允许有100个连接，超出的将被拒绝。只有在standalone模式运行才有效。

**max\_per\_ip=0**

设置每个IP允许与FTP服务器同时建立连接的数目。默认值为0，表示不受限制。只有在standalone模式运行才有效。

**listen\_address=IP地址**

设置FTP服务器在指定的IP地址上侦听用户的FTP请求。若不设置，则对服务器绑定的所有IP地址进行侦听。只有在standalone模式运行才有效。

**setproctitle\_enable=YES/NO（NO）**

设置每个与FTP服务器的连接，是否以不同的进程表现出来。默认值为NO，此时使用ps aux |grep ftp只会有一个vsftpd的进程。若设置为YES，则每个连接都会有一个vsftpd的进程。

**15.虚拟用户设置**

虚拟用户使用PAM认证方式。

**pam\_service\_name=vsftpd**

设置PAM使用的名称，默认值为/etc/pam.d/vsftpd。

**guest\_enable= YES/NO（NO）**

启用虚拟用户。默认值为NO。

**guest\_username=ftp**

这里用来映射虚拟用户。默认值为ftp。

**virtual\_use\_local\_privs=YES/NO（NO）**

当该参数激活（YES）时，虚拟用户使用与本地用户相同的权限。当此参数关闭（NO）时，虚拟用户使用与匿名用户相同的权限。默认情况下此参数是关闭的（NO）。

**16.其他设置**

**text\_userdb\_names= YES/NO（NO）**

设置在执行ls –la之类的命令时，是显示UID、GID还是显示出具体的用户名和组名。默认值为NO，即以UID和GID方式显示。若希望显示用户名和组名，则设置为YES。

**ls\_recurse\_enable=YES/NO（NO）**

若是启用此功能，则允许登入者使用ls –R（可以查看当前目录下子目录中的文件）这个指令。默认值为NO。

**hide\_ids=YES/NO（NO）**

如果启用此功能，所有档案的拥有者与群组都为ftp，也就是使用者登入使用ls -al之类的指令，所看到的档案拥有者跟群组均为ftp。默认值为关闭。

**download\_enable=YES/NO（YES）**

如果设置为NO，所有的文件都不能下载到本地，文件夹不受影响。默认值为YES。