vsftpd 配置文件详解

（一） 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。

（二） 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。

（三） 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。

（四） 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。

（五） 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。

（六） 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。

（七） 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。

（八） 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。

（九） 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。

（十） 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 。

（十一） 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。

（十二） 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。

（十三） 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。

（十四） 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。

（十五） 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）。

（十六） 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。

（十七） 响应代码解释说明：

110 新文件指示器上的重启标记

120 服务器准备就绪的时间（分钟数）

125 打开数据连接，开始传输
150 打开连接
200 成功
202 命令没有执行
211 系统状态回复
212 目录状态回复
213 文件状态回复
214 帮助信息回复
215 系统类型回复
220 服务就绪
221 退出网络
225 打开数据连接
226 结束数据连接
227 进入被动模式（IP 地址、ID 端口）
230 登录因特网
250 文件行为完成
257 路径名建立
331 要求密码
332 要求帐号
350 文件行为暂停
421 服务关闭
425 无法打开数据连接
426 结束连接
450 文件不可用
451 遇到本地错误
452 磁盘空间不足
500 无效命令
501 错误参数
502 命令没有执行
503 错误指令序列
504 无效命令参数
530 未登录网络
532 存储文件需要帐号
550 文件不可用
551 不知道的页类型
552 超过存储分配
553 文件名不允许