链滴

1-FTP 文件传输协议

作者：Carey

原文链接：https://ld246.com/article/1615547559242

来源网站：链滴

1 FTP 文件传输协议

1.1 FTP工作原理介绍

文件传输协议：File Transfer Protocol 早期的三个应用级协议之一，基于C/S结构

数据传输格式：二进制（默认）和文本

双通道协议：命令和数据连接

两种模式：从服务器角度

- 主动(PORT style)：服务器主动连接
  - 命令（控制）：客户端：随机port ---> 服务器：21/tcp
  - 数据：客户端：随机port <---服务器：20/tcp
- 被动(PASV style)：客户端主动连接
  - 命令（控制）：客户端：随机port ---> 服务器：21/tcp
  - 数据：客户端：随机port ---> 服务器：随机port /tcp

范例：服务器被动模式数据端口

227 Entering Passive Mode (172,16,0,1,224,59)
服务器数据端口为：224*256+59

范例: windows 连接FTP服务器默认使用主动模式

C:\Users\zhangzhuo>ftp 192.168.10.81

```
连接到 192.168.10.81。
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
用户(192.168.10.81:(none)): ftp
331 Please specify the password.
密码:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
pub
226 Directory send OK.
ftp: 收到 8 字节，用时 0.00秒 8000.00千字节/秒。
ftp> literal pasv
227 Entering Passive Mode (192,168,10,81,188,81)
```

FTP服务状态码：

```
1XX：信息        125：数据连接打开
2XX：成功类状态   200：命令OK    230：登录成功
3XX：补充类      331：用户名OK
4XX：客户端错误   425：不能打开数据连接
5XX：服务器错误   530：不能登录
```

用户认证：

- 匿名用户：ftp,anonymous,对应Linux用户ftp
- 系统用户：Linux用户,用户/etc/passwd,密码/etc/shadow
- 虚拟用户：特定服务的专用用户，独立的用户/密码文件

1.2 常见 FTP 相关软件

FTP服务器端软件

- Wu-ftpd,Proftpd,Pureftpd,Filezilla Server,Serv-U,Wing FTP Server,IIS
- vsftpd：Very Secure FTP Daemon，CentOS 默认FTP服务器
  - 高速，稳定，下载速度是WU-FTP的两倍
  - ftp.redhat.com数据:单机最多可支持15000个并发
  - vsftpd官网： https://security.appspot.com/vsftpd.html

客户端软件：

```
ftp，lftp，lftpget，wget，curl
ftp -A ftpserver port -A 主动模式 -p 被动模式
lftp -u username ftpserver
lftp username@ftpserver
lftpget ftp://ftpserver/pub/file
gftp：GUI centos5 最新版2.0.19 (11/30/2008)，官网：https://www.gftp.org/
filezilla，FTP Rush，CuteFtp，FlashFXP，LeapFtp
IE ftp://username:password@ftpserver
```

1.3 vsftpd 软件介绍

由 vsftpd 包提供，不再由xinetd管理

用户认证配置文件：/etc/pam.d/vsftpd

启动服务相关文件：

/usr/lib/systemd/system/vsftpd.service
/etc/rc.d/init.d/vsftpd

配置文件：

/etc/vsftpd/vsftpd.conf

帮助：man 5 vsftpd.conf

配置文件格式：

option=value

注意：= 前后不要有空格

用户和其共享目录

- 匿名用户（映射为系统用户ftp ）共享文件位置：/var/ftp
- 系统用户共享文件位置：用户家目录
- 虚拟用户共享文件位置：为其映射的系统用户的家目录

1.4 vsftpd服务常见配置

1.4.1 命令端口

listen_port=2121 默认值为21

范例：

[09:38:55 root@ftp ~]#ftp 192.168.10.81 2121

1.4.2 主动模式端口

connect_from_port_20=YES 主动模式端口为20
ftp_data_port=20 （默认） 指定主动模式的端口

1.4.3 被动模式端口范围

linux ftp 客户端默认使用被动模式
windows ftp 客户端默认使用主动模式
pasv_min_port=6000 0为随机分配，端口范围会影响客户端的并发数
pasv_max_port=6010

1.4.4 使用当地时间

use_localtime=YES 使用当地时间（默认为NO，使用GMT）

1.4.5 匿名用户登录

anonymous_enable=YES 支持匿名用户，CentOS8 默认不允许匿名
no_anon_password=YES 匿名用户略过口令检查，默认NO

1.4.6 匿名用户上传

anon_upload_enable=YES 匿名上传，注意:文件系统权限
anon_mkdir_write_enable=YES 匿名建目录

setfacl -m u:ftp:rwx /var/ftp/pub

注意：还需要开启文件系统访问的权限，不能给FTP根目录写权限，只能级子目录写权限

anon_world_readable_only=NO 只能下载全部读的文件, 默认YES
anon_umask=0333 指定匿名上传文件的umask，默认077，注意：0333中的0不能省略
anon_other_write_enable=YES 可删除和修改上传的文件，默认NO

1.4.7 指定匿名用户的上传文件的默认的所有者和权限

chown_uploads=YES　　#默认NO
chown_username=wang
chown_upload_mode=0644

1.4.8 Linux系统用户

local_enable=YES 是否允许linux用户登录
write_enable=YES 允许linux用户上传文件
local_umask=022 指定系统用户上传文件的默认权限对应umask

1.4.9 将所有系统用户映射为指定的guest用户

guest_enable=YES 所有系统用户都映射成guest用户
guest_username=ftp　配合上面选项才生效，指定guest用户
local_root=/ftproot 指定guest用户登录所在目录,但不影响匿名用户的登录目录
user_config_dir=/etc/vsftpd/conf.d/ 每个用户独立的配置文件目录

范例: 让所有的系统用户映射指定guest用户,并且每个用户目录的不同的

[10:07:44 root@ftp ~]#useradd ftpuser
[10:15:00 root@ftp ~]#vim /etc/vsftpd/vsftpd.conf
guest_enable=YES
guest_username=ftpuser
user_config_dir=/etc/vsftpd/conf.d/　　#每个用户独立的配置文件目录
[10:20:41 root@ftp ~]#systemctl restart vsftpd.service
[10:21:03 root@ftp ~]#mkdir /etc/vsftpd/conf.d
[10:21:24 root@ftp ~]#vim /etc/vsftpd/conf.d/zhangzhuo

local_root=/ftproot_zhangzhuo
[10:24:58 root@ftp ~]#vim /etc/vsftpd/conf.d/ftpuser
local_root=/ftproot_ftpuser
[10:22:22 root@ftp ~]#mkdir /ftproot_zhangzhu
[10:24:42 root@ftp ~]#mkdir /ftproot_ftpuser

1.4.10 禁锢系统用户

禁锢所有系统用户在家目录中

chroot_local_user=YES #禁锢系统用户，默认NO，即不禁锢

如果启用chroot,必须保证ftp根目录不可写,这样对于ftp根直接为网站根目录的用户不方便，不修改会错

```
500 OOPS: vsftpd: refusing to run with writable root inside chroot(
Login failed.
```

禁锢或不禁锢特定的系统用户在家目录中，与上面设置功能相反

chroot_list_enable=YES #默认是NO
chroot_list_file=/etc/vsftpd/chroot_list #默认值

当chroot_local_user=YES和chroot_list_enable=YES时，则chroot_list中用户不禁锢，即白名单
当chroot_local_user=NO和chroot_list_enable=YES时， 则chroot_list中用户禁锢，即黑名单

1.4.11 日志

#wu-ftp 日志：默认启用
xferlog_enable=YES 启用记录上传下载日志，此为默认值
xferlog_std_format=YES 使用wu-ftp日志格式，此为默认值
xferlog_file=/var/log/xferlog 可自动生成， 此为默认值

#vsftpd日志：默认不启用
dual_log_enable=YES 使用vsftpd日志格式，默认不启用
vsftpd_log_file=/var/log/vsftpd.log 可自动生成， 此为默认值

1.4.12 提示信息

登录前提示信息

ftpd_banner="welcome to mage ftp server" #配置文件直接定义
banner_file=/etc/vsftpd/ftpbanner.txt #在文件中定义

目录访问提示信息

dirmessage_enable=YES #开启此为默认值
message_file=.message #信息存放在指定目录下.message ，此为默认值,只支持单行说明

1.4.13 PAM模块实现用户访问控制

pam_service_name=vsftpd
#pam配置文件:/etc/pam.d/vsftpd
/etc/vsftpd/ftpusers 默认文件中用户拒绝登录，默认是黑名单，但也可以是白名单

范例：

```
[11:00:56 root@ftp ~]#ldd /usr/sbin/vsftpd | grep pam
libpam.so.0 => /lib64/libpam.so.0 (0x00007fbe30904000)
[11:07:33 root@ftp ~]#cat /etc/pam.d/vsftpd
#%PAM-1.0
session    optional     pam_keyinit.so    force revoke
#将sense=deny 修改为 sense=allow    #修改黑名单为白名单
auth       required     pam_listfile.so item=user sense=allow file=/etc/vsftpd/ftpusers onerr=succeed
auth       required     pam_shells.so
auth       include     password-auth
account    include     password-auth
session    required     pam_loginuid.so
session    include     password-auth
```

1.4.14 是否启用控制用户登录的列表文件

```
userlist_enable=YES   此为默认值
userlist_deny=YES     (默认值) 黑名单,不提示口令，NO为白名单
userlist_file=/etc/vsftpd/user_list 此为默认值
```

1.4.15 vsftpd服务指定用户身份运行

```
nopriv_user=nobody   此为默认值
```

范例：

```
[11:19:04 root@ftp ~]#ps auxf
root       4140  0.0  0.0  27032   420 ?        Ss   11:18   0:00 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
nobody     4143  0.0  0.4  62340  4548 ?        Ss   11:18   0:00  \_ /usr/sbin/vsftpd /etc/vsftpd/vftpd.conf
ls         4145  0.0  0.4  75440  4672 ?        S    11:18   0:00      \_ /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
```

1.4.16 连接数限制

```
max_clients=0 #最大并发连接数
```

如果超出连接，会报如下提示

```
[root@centos6 ~]#ftp 10.0.0.8
Connected to 10.0.0.8 (10.0.0.8).
421 There are too many connected users, please try later.
ftp>
```

```
max_per_ip=0 #每个IP同时发起的最大连接数
```

如果超出连接，会报如下提示

```
[root@centos6 ~]#ftp 10.0.0.8
Connected to 10.0.0.8 (10.0.0.8).
421 There are too many connections from your internet address.
ftp>
```

1.4.17 传输速率，单位：字节/秒

anon_max_rate=0 匿名用户的最大传输速率,以字节为单位,比如:1024000表示1MB/s
local_max_rate=0 本地用户的最大传输速率

范例：

```
#限速
[11:23:58 root@ftp ~]#vim /etc/vsftpd/vsftpd.conf
anon_max_rate=1024000
local_max_rate=10240000
#生成测试文件
[11:29:16 root@ftp ~]#dd if=/dev/zero of=/home/ls/1.test bs=1G count=2
[11:29:16 root@ftp ~]#dd if=/dev/zero of=/var/ftp/pub/1.test bs=1G count=2
#测试匿名下载速度
[11:30:50 root@centos8 ~]#wget ftp://192.168.10.81:2121/pub/1.test
1.test              1%[                    ]  29.38M  1000KB/s    eta 34m 27s
#测试本地用户下载速度
[11:31:29 root@centos8 ~]#wget ftp://ls:123456@192.168.10.81:2121/1.test
1.test.1            4%[                    ]  83.57M  9.76MB/s    eta 3m 22s
```

1.4.18 连接时间：秒为单位

connect_timeout=60 主动模式数据连接超时时长
accept_timeout=60 被动模式数据连接超时时长
data_connection_timeout=300 数据连接无数据输超时时长
idle_session_timeout=60 无命令操作超时时长

1.4.19 以文本方式传输

以文本方式传输文件时,会自动对文件进行格式转换,比如转换成windows的文本格式

```
#启用此选项可使服务器在ASCII模式下实际对文件进行ASCII处理。
#默认是禁用,禁用后，服务器将假装允许ASCII模式，但实际上会忽略激活它的请求
ascii_upload_enable=YES
ascii_download_enable=YES
```

说明：不建议使用文本方式，因为可能导致二进制文件内容被破坏

1.5 vsftpd 虚拟用户

虚拟用户：给特定服务使用的用户帐号

- 所有虚拟用户会统一映射为一个指定的系统帐号：访问共享位置，即为此系统帐号的家目录
- 各虚拟用户可被赋予不同的访问权限，通过匿名用户的权限控制参数进行指定

虚拟用户帐号的存储方式：

- 文件：创建文本文件，奇数行为用户名，偶数行为密码,再被编码为hash 格式Berkeley DBdatabas文件

```
db_load -T -t hash -f vusers.txt vusers.db
```

- 关系型数据库中的表中：实时查询数据库完成用户认证
  - vsftpd 支持mysql库：pam要依赖于pam-mysql

```
/lib64/security/pam_mysql.so
/usr/share/doc/pam_mysql-0.7/README
```

1.5.1 实现基于文件验证的vsftpd虚拟用户

1.5.1.1 创建用户数据库文件

```
[18:38:44 root@ftp ~]#rpm -qf `which db_load`
libdb-utils-5.3.28-39.el8.x86_64
[18:38:48 root@ftp ~]#vim /etc/vsftpd/vusers.txt
[18:39:49 root@ftp ~]#cat /etc/vsftpd/vusers.txt
ftp_zhang
123456
ftp_cheng
123456
[18:40:37 root@ftp ~]#db_load -T -t hash -f /etc/vsftpd/vusers.txt /etc/vsftpd/vusers.db
[18:40:57 root@ftp ~]#chmod 600 /etc/vsftpd/vusers.db
```

1.5.1.2 创建用户和访问FTP目录

```
[18:41:11 root@ftp ~]#useradd -d /data/ftproot -s /sbin/nologin -r vuser
[18:42:35 root@ftp ~]#mkdir /data/ftproot/upload -p
[18:42:52 root@ftp ~]#setfacl -m u:vuser:rwx /data/ftproot/upload
#chmod a=rx /data/ftproot/ 如果自动创建家目录，需修改权限,ftproot目录不允许有写权限
```

1.5.1.3 创建pam配置文件

```
[18:43:17 root@ftp ~]#vim /etc/pam.d/vsftpd.db
auth required pam_userdb.so db=/etc/vsftpd/vusers
account required pam_userdb.so db=/etc/vsftpd/vusers
```

1.5.1.4 指定pam配置文件

```
[18:46:33 root@ftp ~]#vim /etc/vsftpd/vsftpd.conf
pam_service_name=vsftpd.db
guest_enable=YES
guest_username=vuser
```

1.5.1.5 虚拟用户建立独立的配置文件

#指定各个用户配置文件存放的路径
[18:48:17 root@ftp ~]#vim /etc/vsftpd/vsftpd.conf
user_config_dir=/etc/vsftpd/conf.d/
#创建各个用户配置文件存放的路径
[18:49:24 root@ftp ~]#mkdir /etc/vsftpd/conf.d
#创建各用户自已的配置文件,允许zhang用户可读写，其它用户只读
[18:50:04 root@ftp ~]#vim /etc/vsftpd/conf.d/ftp_zhang
anon_upload_enable=YES
anon_mkdir_write_enable=YES
anon_mkdir_write_enable=YES
#创建各用户自已的配置文件
[18:51:51 root@ftp ~]#vim /etc/vsftpd/conf.d/ftp_cheng
#登录目录改变至指定的目录
local_root=/data/ftproot2
#针对ftp_mage用户建立对应的数据目录
[18:53:02 root@ftp ~]#mkdir /data/ftproot2

1.5.2 实现基于MYSQL验证的vsftpd虚拟用户

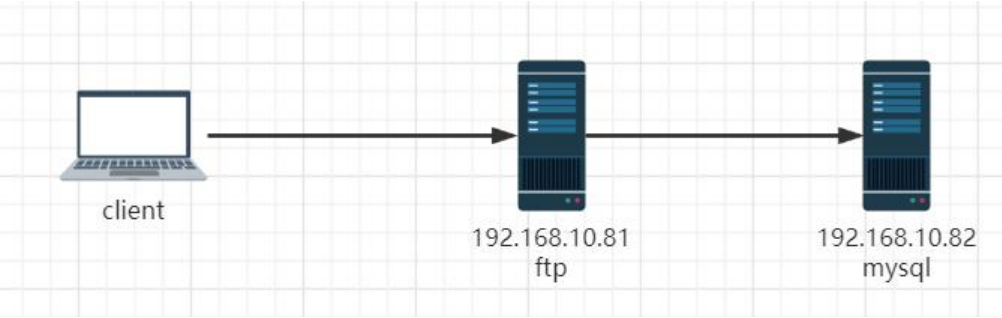
利用 pam_mysql 模块可以实现基于MySQL的FTP虚拟用户功能

项目网站:

http://pam-mysql.sourceforge.net/
https://sourceforge.net/projects/pam-mysql/
http://sf.net/projects/pam-mysql

注意:因为此项目年代久远不再更新，当前只支持CentOS 6,7，不支持CentOS 8

环境准备



本实验在两台主机上实现
一台做为FTP服务器CentOS 7
一台做 Mariadb 数据库服务器

1.5.2.1 在数据库服务器上安装mysql数据库

#注意：MySQL8.0由于取消了PASSWORD()函数不支持,因此选择Mariadb
[19:50:14 root@mysql ~]#yum install -y mariadb-server
[19:54:02 root@mysql ~]#systemctl enable --now mariadb

1.5.2.2 在数据库服务上配置数据库支持vsftpd服务

```
#建立存储虚拟用户数据库和表
MariaDB [(none)]> create database vsftpd;
MariaDB [(none)]> use vsftpd
MariaDB [(none)]>create table users( id int auto_increment not null primary key, name char(5
) binary not null, password char(48) binary not null);

#添加虚拟用户，为了安全应该使用PASSWORD函数加密其密码后存储
MariaDB [vsftpd]> insert into users(name,password) values('ftp_zhang',password('123456'));
MariaDB [vsftpd]> insert into users(name,password) values('ftp_cheng',password('123456'));
#创建连接的数据库用户
MariaDB [vsftpd]> create user 'vsftpd'@'192.168.10.%' identified by '123456';
MariaDB [vsftpd]> grant all on vsftpd.* to 'vsftpd'@'192.168.10.%';
```

1.5.2.3 在FTP服务器上安装vsftpd 和 pam_mysql包

```
[19:52:50 root@ftp ~]#yum install -y vsftpd
```

1.5.2.4 在FTP服务器上安装 pam_mysql

对于 centos 6：pam_mysql由EPEL的源中提供

```
[root@centos6 ~]#yum install pam_mysql
```

对于 centos7 和 8：无对应rpm包，需手动编译安装

注意: 当前版本的源码不支持 CentOS 8,使用中会提示下面错误

```
[root@centos8 ~]#tail -f /var/log/secure
Jan  2 10:20:31 centos8 vsftpd[15519]: PAM unable to
dlopen(/usr/lib64/security/pam_mysql.so): /usr/lib64/security/pam_mysql.so:
undefined symbol: make_scrambled_password
```

pam-mysql 源码进行编译

```
[20:03:01 root@ftp ~]#yum -y install vsftpd gcc gcc-c++ make mariadb-devel pam-devel
[20:03:16 root@ftp ~]#tar xvf pam_mysql-0.7RC1.tar.gz
[20:03:16 root@ftp ~]#cd pam_mysql-0.7RC1/
[20:03:43 root@ftp pam_mysql-0.7RC1]#./configure --with-pam-mods-dir=/lib64/security
[20:04:24 root@ftp pam_mysql-0.7RC1]#make
[20:04:24 root@ftp pam_mysql-0.7RC1]#make install
[20:04:59 root@ftp pam_mysql-0.7RC1]#ll /lib64/security/pam_mysql.*
-rwxr-xr-x 1 root root    882 Mar 10 20:04 /lib64/security/pam_mysql.la
-rwxr-xr-x 1 root root 141712 Mar 10 20:04 /lib64/security/pam_mysql.so
```

1.5.2.5 在FTP服务器上建立pam认证所需文件

```
[19:29:27 root@ftp ~]#cat /etc/pam.d/vsftpd.mysql
auth required pam_mysql.so user=vsftpd passwd=123456 host=192.168.10.82 db=vsftpd tab
e=users usercolumn=name passwdcolumn=password crypt=9
account required pam_mysql.so user=vsftpd passwd=123456 host=192.168.10.82 db=vsftpd
able=users usercolumn=name passwdcolumn=password crypt=9
```

注意：以上参考 README文档

crypt 加密方式：

- 0表示不加密
- 1表示crypt(3)加密
- 2表示使用mysql password()函数加密
- 3表示md5加密
- 4表示sha1加密

配置字段说明

- auth 表示认证
- account 验证账号密码正常使用
- required 表示认证要通过
- pam_mysql.so模块是默认的相对路径，是相对/lib64/security/路径而言，也可以写绝对路径；后为给此模块传递的参数
- user=vsftpd为登录mysql的用户
- passwd=magedu 登录mysql的的密码
- host=mysqlserver mysql服务器的主机名或ip地址
- db=vsftpd 指定连接msyql的数据库名称
- table=users 指定连接数据库中的表名
- usercolumn=name 当做用户名的字段
- passwdcolumn=password 当做用户名字段的密码
- crypt=2 密码的加密方式为mysql password()函数加密

1.5.2.6 建立相应用户和修改vsftpd配置文件

```
[20:07:46 root@ftp ~]#useradd -s /sbin/nologin -d /data/ftproot -r vuser
[20:08:13 root@ftp ~]#mkdir -pv /data/ftproot/upload
[20:08:43 root@ftp ~]#setfacl -m u:vuser:rwx /data/ftproot/upload
[20:09:03 root@ftp ~]#vim /etc/vsftpd/vsftpd.conf
pam_service_name=vsftpd.mysql
guest_enable=YES
guest_username=vuser
[20:10:13 root@ftp ~]#systemctl enable --now vsftpd
```

1.5.2.7 在FTP服务器上配置虚拟用户具有不同的访问权限

```
#配置vsftpd为虚拟用户使用配置文件目录
[root@centos7 ~]#vim /etc/vsftpd/vsftpd.conf
#添加如下选项
user_config_dir=/etc/vsftpd/conf.d/
#创建所需要目录，并为虚拟用户提供配置文件
[root@centos7 ~]#mkdir /etc/vsftpd/conf.d/
#配置虚拟用户的访问权限
#虚拟用户对vsftpd服务的访问权限是通过匿名用户的相关指令进行的。如要让用户wang具有上传文的权
```

限，可修改/etc/vsftpd/vusers.d/wang文件，在里面添加如下选项并设置为YES即可,只读则设为NO
#注意：需确保对应的映射用户对于文件系统有写权限
[root@centos7 ~]#vim /etc/vsftpd/conf.d/ftp_wang
anon_upload_enable={YES|NO}
anon_mkdir_write_enable={YES|NO}
anon_other_write_enable={YES|NO}
#登录目录改变至指定的目录
local_root=/data/ftproot2