ftp服务器的配置和管理

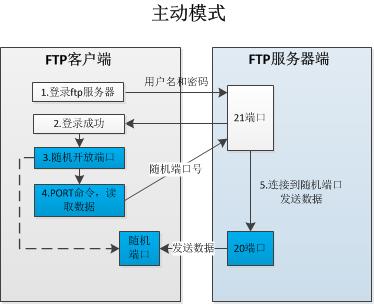
# FTP服务的概述

FTP：filetransfer protocol文件传输协议，基于TCP，是应用层的协议之一。建立FTP的软件很多，通常使用VSFTP（very secureFTP），是一个基于GPL发布的类UNIX系统上的FTP服务器。

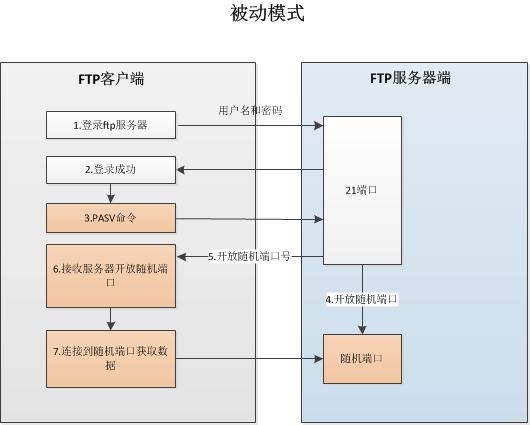
工作原理：一个完整的FTP文件传输需要建立两种类型的连接：一种是用于传递客户端命令和服务器对命令的响应，TCP端口位21,称为控制连接。另一种真正的文件传输称为数据连接，缺省端口为20。FTP控制连接建立后，即可开始进行文件传输。

## 主动模式和被动模式

PORT中文称为主动模式，工作的原理： FTP客户端连接到FTP服务器的21端口，发送用户名和密码登录，登录成功后要list列表或者读取数据时，客户端随机开放一个端口（1024以上），发送 PORT命令到FTP服务器，告诉服务器客户端采用主动模式并开放端口；FTP服务器收到PORT主动模式命令和端口号后，通过服务器的20端口和客户端开放的端口连接，发送数据，原理如下图：

[](http://static.oschina.net/uploads/space/2011/0528/204156_vG81_97118.jpg)

PASV是Passive的缩写，中文成为被动模式，工作原理：FTP客户端连接到FTP服务器的21端口，发送用户名和密码登录，登录成功后要list列表或者读取数据时，发送PASV命令到FTP服务器， 服务器在本地随机开放一个端口（1024以上），然后把开放的端口告诉客户端， 客户端再连接到服务器开放的端口进行数据传输，原理如下图：

[](http://static.oschina.net/uploads/space/2011/0528/204218_G2gD_97118.jpg)

## FTP用户类型

FTP的用户类型：本地用户（本地用户在ftp上拥有一个账号），虚拟用户（并不是一个合法的linux系统用户。通过调用响应的PAM认证模块，和系统的FTP认证文件进行比较。如果通过认证，该账号就会映射成一个Linux下的本地用户。），匿名用户（用户使用特殊的用户anonymous登录ftp服务器，口令为空或者用户的E-mail地址。在linux中，默认登录的目录/var/ftp。

* 匿名用户：anonymous/ftp（密码：只要有@或者空
* 本地用户：linux系统用户和密码（不需要配置）
* 虚拟用户：管理员自定义的模拟用户

# VSFTPD的安装和启动

## 查看是否已经安装vsftpd

rpm -qa | grep vsftpd

## 安装，并设置开机启动

|  |
| --- |
| ip=172.16.130.124  homeDir=/home/3tbetter  v\_user=3tbetter  v\_pass=123456  yum -y install vsftpd db4 db4-utils  chkconfig vsftpd on  #修改vsftpd配置文件  /bin/cp -f /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.bak  cat > /etc/vsftpd/vsftpd.conf <<EOF  anonymous\_enable=NO  local\_enable=YES  write\_enable=YES  local\_umask=022  dirmessage\_enable=YES  xferlog\_enable=YES  connect\_from\_port\_20=YES  xferlog\_std\_format=YES  listen=YES  pam\_service\_name=vsftpd  userlist\_enable=YES  tcp\_wrappers=YES  max\_clients=400  guest\_enable=YES  guest\_username=ftp  user\_config\_dir=/etc/vsftpd/vuser\_conf  port\_enable=YES  pasv\_enable=YES  pasv\_promiscuous=YES  pasv\_min\_port=30001  pasv\_max\_port=61000  dirlist\_enable=YES  # pasv\_address=此选项为一个数字IP地址，作为PASV命令的响应。  pasv\_address=$ip  EOF  #创建虚拟用户，文件的奇数行为虚拟用户名，偶数行是相应的口令  cat > /etc/vsftpd/vuser\_passwd.txt <<EOF  $v\_user  $v\_pass  EOF  #生成虚拟用户数据库文件  db\_load -T -t hash -f /etc/vsftpd/vuser\_passwd.txt /etc/vsftpd/vuser\_passwd.db  #创建PAM认证文件  cat > /etc/pam.d/vsftpd <<EOF  auth required pam\_userdb.so db=/etc/vsftpd/vuser\_passwd  account required pam\_userdb.so db=/etc/vsftpd/vuser\_passwd  EOF  #创建虚拟用户配置文件  mkdir -p /etc/vsftpd/vuser\_conf/  cat > /etc/vsftpd/vuser\_conf/$v\_user <<EOF  local\_root=$homeDir  write\_enable=YES  anon\_umask=022  anon\_world\_readable\_only=NO  anon\_upload\_enable=YES  anon\_mkdir\_write\_enable=YES  anon\_other\_write\_enable=YES  allow\_writeable\_chroot=YES  EOF  #创建虚拟用户根目录  mkdir -p $homeDir  chmod -R 775 $homeDir    service vsftpd restart  service iptables stop |

# VSFTPD的配置文件

vsftpd安装后，与其相关的配置文件如下：

* /etc/logrotate.d/vsftpd(日志轮转备份配置文件)
* /etc/pam.d/vsftpd(基于PAM的vsftpd验证配置文件)
* /etc/rc.d/init.d/vsftpd(启动脚本)
* /etc/vsftpd(vsftpd软件的主目录)
* /etc/vsftpd/ftpusers(默认的vsftpd黑名单,优先级高于user\_list)
* /etc/vsftpd/user\_list(可以通过主配置文件设置该文件为黑名单或者白名单)
* /usr/sbin/vsftpd(vsftpd主程序)
* /usr/share/doc/vsftpd-2.2.2(vsftpd文档资料的路径)
* /var/ftp(默认vsftpd共享目录)

## 全局设置

|  |
| --- |
| ###全局设置  listen=YES #是否监听端口，独立运行守护进程  listen-port=21 #监听入站FTP请求端口  write\_enable=YES #是否允许写操作，全局开关  download\_enable=YES #如果设置为NO,则拒绝所有的下载请求  ascii\_upload\_enable=YES  ascii\_download\_enable=YES #设定支持ASCII模式的上传和下载功能  dirmessage\_enable=YES #用户进入目录是否显示消息  xferlog\_enable=YES #是否开启xferlog日志功能  xferlog\_std\_format=YES #Xferlog日志格式  connect\_from\_port\_20=YES #使用主动模式连接，启用20号端口  pasv\_enable=YES #是否启用被动模式连接，默认是被动模式  pasv\_max\_port=24600 #被动模式连接的最大端口  pasv\_min\_port=24500 #被动模式连接的最小端口  userlist\_enable=YES #是否启用userlist文件中账户访问FTP,一般禁用，没在文件中的用户无法登陆ftp  userlist\_deny=YES #是否禁用userlist文件中账户访问FTP  max\_client=2000 #允许最大同时2000个客户端连接，0表示无限制  max\_per\_ip=0 #每个客户端的最大连接显示，0代表无限制  tcp\_wrappers=YES #是否启用tcp\_wrappers  guest\_enable=YES #如果为YES,则所有的非匿名登录都映射成  #guest\_username指定的账户  guest\_username=ftp #设定来宾账户  user\_config\_dir=/etc/vsftpd/conf #指定目录可以设置用户独立的配置文件和选项  dual\_log\_enable=NO #是否启用双日志功能，生成两个日志文件  pasv\_promiscuous=YES  #可配置为内网地址  pasv\_address= 172.16.128.210 |

注意：pasv\_promiscuous此选项激活时，将关闭PASV模式的安全检查。该检查确保数据连接和控制连接是来自同一个IP地址。小心打开此选项。此选项唯一合理的用法是存在于由安全隧道方案构成的组织中。默认值为NO。

## 匿名账户配置

|  |
| --- |
| ###匿名设置  anonymous\_enable=YES #是否开启匿名访问功能，默认开启  anno\_root=/var/ftp #匿名访问FTP的根路径，默认为/var/ftp  anno\_upload\_enable=YES #是否允许匿名账户上传，默认禁止  anno\_mkdir\_write\_enable=YES #是否允许匿名账号创建目录，默认禁止  anno\_other\_write\_enable=YES #是否允许匿名账户进行其他的写操作  anno\_max\_rate=0 #匿名数据传输率  anno\_umask #匿名上传权限掩码 |

## 本地账户配置

|  |
| --- |
| ###本地账户  local\_enable=YES #是否开启本机账号FTP功能  local\_max\_rate=0 #本地账户数据传输率  local\_mask=077 #本地账户权限掩码  chroot\_local\_user=YES #是否禁锢本地账户根目录，默认为NO  local\_root=/ftp/common #本地用户访问FTP根路径 |

# 配置VSFTPD服务器

## 本地用户配置

|  |
| --- |
| anonymous\_enable=NO  local\_enable=YES  write\_enable=YES  local\_umask=022  dirmessage\_enable=YES  xferlog\_enable=YES  xferlog\_std\_format=YES  chroot\_local\_user=YES  listen=YES  pam\_service\_name=vsftpd  userlist\_enable=YES  tcp\_wrappers=YES |

## 虚拟用户的配置

### 安装Berkeley DB工具

yum install db4 db4-utils -y

### 创建虚拟用户数据库文件/etc/vsftpd/vuser\_passwd.txt

vi /etc/vsftpd/vuser\_passwd.txt

文件的奇数行为虚拟用户名，偶数行是相应的口令。

### 生成虚拟用户数据库文件

db\_load -T -t hash -f /etc/vsftpd/vuser\_passwd.txt /etc/vsftpd/vuser\_passwd.db

### 创建PAM认证文件

#编辑认证文件/etc/pam.d/vsftpd,注释掉以前

|  |
| --- |
| auth required pam\_userdb.so db=/etc/vsftpd/vuser\_passwd  account required pam\_userdb.so db=/etc/vsftpd/vuser\_passwd |

### 创建虚拟用户配置文件

mkdir /etc/vsftpd/vuser\_conf/

#文件名等于vuser\_passwd.txt里面的账户名

vi /etc/vsftpd/vuser\_conf/kobe

|  |
| --- |
| local\_root=/home/kobe  write\_enable=YES  anon\_umask=022  anon\_world\_readable\_only=NO  anon\_upload\_enable=YES  anon\_mkdir\_write\_enable=YES  anon\_other\_write\_enable=YES |

mkdir -p /home/kobe #创建虚拟用户根目录

chmod -R 777 /home/kobe #设置权限

## 设置Selinux

# selinux默认不允许FTP共享家目录

setsebool -P ftp\_home\_dir=1 #设置ftp可以使用home目录

setsebool -P allow\_ftpd\_full\_access=1 #设置ftp用户可以有所有权限

## 设置防火墙

vi /etc/sysconfig/iptables添加：

|  |
| --- |
| -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT  -A INPUT -m state --state NEW -m tcp -p tcp --dport 30001:61000 -j ACCEPT |

注意：这里的端口号为pasv\_min\_port=30001，pasv\_max\_port=61000配置的端口号

## 其他常见设置

#匿名用户不能访问

anonymous\_enable=NO

#开启user\_list，文件默认在/etc/vsftpd/user\_list

userlist\_enable=YES

allow\_writeable\_chroot=YES

注意：默认黑名单的目录在/etc/vsftpd/ftpusers

#启用日志

|  |
| --- |
| xferlog\_enable=YES  xferlog\_std\_format=YES  xferlog\_file=/var/log/xferlog |

#chroot\_local\_user与chroot\_list\_enable详解

|  |
| --- |
| #是否将所有用户限制在主目录,YES为启用 NO禁用(该项默认值是NO)  chroot\_local\_user  #是否启动限制用户的名单 YES为启用 NO禁用(包括注释掉也为禁用)  chroot\_list\_enable  #是否限制在主目录下的用户名单  chroot\_list\_file=/etc/vsftpd/chroot\_list |

|  |  |  |
| --- | --- | --- |
|  | chroot\_local\_user=YES | chroot\_local\_user=NO |
| chroot\_list\_enable=YES | 1.所有用户都被限制在其主目录下  2.使用chroot\_list\_file指定的用户列表，这些用户作为“例外”，不受限制 | 1.所有用户都不被限制其主目录下  2.使用chroot\_list\_file指定的用户列表，  这些用户作为“例外”，受到限制 |
| chroot\_list\_enable=NO | 1.所有用户都被限制在其主目录下  2.不使用chroot\_list\_file指定的用户列表，没有任何“例外”用户 | 1.所有用户都不被限制其主目录下  2.不使用chroot\_list\_file指定的用户列表，  没有任何“例外”用户 |

# ftp命令

安装ftp客服端：

yum install ftp -y

常用命令

* ls 列出远程机的当前目录
* cd 在远程机上改变工作目录
* lcd 在本地机上改变工作目录
* ascii 设置文件传输方式为ASCII模式
* binary 设置文件传输方式为二进制模式
* close终止当前的ftp会话
* hash 每次传输完数据缓冲区中的数据后就显示一个#号
* get（mget） 从远程机传送指定文件到本地机
* put（mput）从本地机传送指定文件到远程机
* passive：打开和关闭被动模式。
* open (ip)连接远程ftp站点
* quit断开与远程机的连接并退出ftp
* ? 显示本地帮助信息
* ! 转到Shell中

# xferlog日志说明

|  |
| --- |
| Thu Nov 10 12:01:11 2016 1 10.25.248.168 144997 /mobile/static/upload/image/certificate/20161131587b876a4-f359-4af1-ad17-e08a7ce090e9-source.jpg b \_ i g 3tftp ftp 0 \* c  Thu Nov 10 12:01:15 2016 1 10.25.248.168 168675 /mobile/static/upload/image/certificate/2016113156122c7fb-68f5-4989-999f-7bf09c4d34bc-source.jpg b \_ i g 3tftp ftp 0 \* c  Thu Nov 10 12:13:47 2016 1 10.25.248.168 152167 /mobile/static/upload/image/certificate/201611315ab7ddbd4-e3c1-4702-a5a0-5d412e2d3e35-source.jpg b \_ i g 3tftp ftp 0 \* c  Thu Nov 10 12:13:51 2016 1 10.25.248.168 121783 /mobile/static/upload/image/certificate/201611315fea766bd-bdf7-4553-87fe-154b3fe9b495-source.jpg b \_ i g 3tftp ftp 0 \* c |
| 记录发生的时间 ： Thu Nov 10 12:01:11 2016  传输该文件使用的时间：1  客户端主机的IP或主机名：10.25.248.168  文件大小(单位：字节)：144997  文件名 ：/mobile/static/upload/image/certificate/20161131587b876a4-f359-4af1-ad17-e08a7ce090e9-source.jpg  文件传输类型(a表示ASCII（文本），b（二进制）)：b  文件特殊处理标记（“\_”表不做任何处理，C表示文件时压缩格式 ,U表示文件是非压缩格式，T表示是tar格式)：\_  文件传输方向(o表示从服务器到客户端，i相反)：i  用户登录方式(a表示匿名登录，g表示虚拟用户登录，r表示真实用户登录) ：g  用户名称(？（匿名用户)：3tftp  服务器名(一般为FTp) ：ftp  认证方式 (0表示无，1表示RFC931认证)：0  认证的用户ID (\*表示无法获得用户ID )：\*  传输完成状态(c表示完成，i表示没完成) ：c |