第12章 FTP服务器

- FTP：File Transfer Protocol
  - 该协议定义的是一个在远程计算机系统和本地计算机系统之间传输文件的一个标准
- 在FTP会话存在有两个独立的TCP连接
  - 控制连接（control connection）
  - 数据连接（data connection）

FTP的控制连接

- 控制连接主要用来传送在实际通信过程中需要执行的FTP命令以及命令的响应。
- FTP服务器监听端口号21来等待控制连接建立请求 。
- 控制连接建立以后并不立即建立数据连接，而是服务器通过一定的方式来验证客户的身份， 以决定是否可以建立数据传输。
- 数据连接是等到要目录列表、传输文件时才临时建立的，并且每次客户端使用不同的端口号来建立数据连接。 一旦数据传输完毕，就中断这条临时的数据连接。
- 在FTP连接期间，控制连接始终保持通畅的连接状态。 在数据连接存在期间内，控制连接肯定是存在的； 一旦控制连接断开，数据连接会自动关闭。

URL

- ftp://用户名:密码@IP或域名:端口/路径/文件名

- ftp://user:123456@nbut.cn:2003/soft/demo.doc
- ftp://user:123456@nbut.cn
- ftp://nbut.cn
- 匿名账号：Anonymous

传输模式

- （1）ASCII传输方式
- （2）二进制传输模式

- 主动传输模式 （Active FTP）
  - 服务器向客户端发起一个用于数据传输的连接
- 被动传输模式 （Passive FTP）
  - 客户端向服务器发起一个用于数据传输的连接

vsftpd

- CentOS自带了一个高安全性的FTP服务器vsftpd。
- vsftpd的特点
  - 是一个安全、高速、稳定的FTP服务器。
  - 可设定多个基于IP的虚拟FTP server。
  - 匿名FTP服务更是十分容易。
  - 匿名ftp的根目录不需要任何特殊的目录结构，或系统程序或其他系统文件。
  - 不执行任何外部程序，从而减少了安全隐患。
  - 支持虚拟用户，且支持每个虚拟用户具有独立的配置。
  - 可以设置为从inetd启动，或者是独立ftp服务器两种运行方式。
  - 支持PAM 或 xinetd / tcp_wrappers的认证方式。
  - 支持带宽限制等。

FTP服务器的启动与配置

- 查询是否已经安装
  - rpm -qa | grep vsftpd
  - yum list installed | grep vsftpd
- 使用yum安装
  - yum install vsftpd
- 使用rpm安装
  - rpm -ivh vsftpd-2.2.2-24.el6.x86_64.rpm

FTP服务器的启动和停止

- # service vsftpd start
- # service vsftpd stop
- # service vsftpd restart

- 下面的命令是用来检查vsftpd是否被启动：
- # service vsftpd status
- # pstree | grep vsftpd

先连接看看？

vsftpd的配置文件

- vsftpd的主配置文件
  - /etc/vsftpd/vsftpd.conf
- vsftpd的用户访问控制配置文件
  - /etc/vsftpd/ftpusers
    - 禁止使用vsftpd的用户列表
  - /etc/vsftpd/user_list

vsftpd默认的主配置文件

- 允许匿名用户（anonymous）和本地用户登录。
- 匿名用户不能离开匿名服务器目录/var/ftp，且只能下载不能上传。
- 本地用户登录：本地用户名/本地密码。
- 本地用户可以离开该用户目录切换至有权访问的其他目录，并在权限允许的情况下进行上传/下载。
- 写在文件/etc/vsftpd/ftpusers中的本地用户禁止登录。
- 要使用户在下载文件时能够续传文件，必须保证文件对其他用户有读的权限。 否则，当续传时不能读取已传的服务器上的文件。

vsftpd的默认配置文件

```
#是否允许匿名ftp,如否则选择NO
anonymous_enable=YES
# 是否允许本地用户登录
local_enable=YES
# 是否开放本地用户的写权限
write_enable=YES
# 设置本地用户的文件的掩码是022,默认值是077
local_umask=022
#是否允许匿名用户上传文件
#anon_upload_enable=YES
```

vsftpd的默认配置文件（续）

```
# 是否允许匿名用户创建新的文件夹
#anon_mkdir_write_enable=YES

# 是否显示目录说明文件,默认是YES但需要手工创
  建.message文件
dirmessage_enable=YES

# 激活上传下载日志
xferlog_enable=YES

# 启用FTP数据端口的连接请求(ftp-data).
connect_from_port_20=YES
```

vsftpd的默认配置文件（续）

```
# 是否改变上传文件的属主,如果是需要输入一个系统用户
  名,可以把上传的文件都改成root属主
#chown_uploads=YES
#chown_username=whoever

# 传输日志的路径和名字默认是/var/log/vsftpd.log
#xferlog_file=/var/log/vsftpd.log

# 是否使用标准的ftp xferlog模式
xferlog_std_format=YES

#设置默认的断开不活跃session的时间(单位：秒)
#idle_session_timeout=600
```

vsftpd的默认配置文件（续）

```
# 设置数据传输超时时间
#data_connection_timeout=120
#运行vsftpd需要的非特权系统用户默认是nobody
#nopriv_user=ftpsecure
# 是否使用ascii码方式上传和下载文件
#ascii_upload_enable=YES
#ascii_download_enable=YES
# 定制欢迎信息
#ftpd_banner=Welcome to blah FTP service.

# 是否允许禁止匿名用户使用某些邮件地址，如果是，输入禁止的邮件
   地址的路径和文件名
#deny_email_enable=YES
#banned_email_file=/etc/vsftpd.banned_emails
```

vsftpd的默认配置文件（续）

```
#是否将系统用户限止在自己的home目录下,如果选择了yes那么
   chroot_list中列出的是不能chroot的用户的列表
#chroot_local_user=YES
#chroot_list_enable=YES
#chroot_list_file=/etc/vsftpd/chroot_list
#由于默认情况下userlist_deny=YES,所以/etc/vsftpd.user_list文件
   中
#所列出的用户不允许访问vsftpd服务器。
userlist_enable=YES
#使vsftpd处于独立启动模式
listen=YES
#使用tcp_wrappers作为主机的访问控制方式
tcp_wrappers=YES
```

配置基于本地用户的访问控制

- 限制指定的本地用户不能访问，而其他本地用户可访问
  - userlist_enable=YES
  - userlist_deny=YES
  - userlist_file= /etc/vsftpd.user_list
- 限制指定的本地用户可以访问，而其他本地用户不可访问
  - userlist_enable= YES
  - userlist_deny= NO
  - userlist_file= /etc/vsftpd.user_list

chroot

- chroot_local_user
  - 是否将所有用户限制在主目录
  - YES为启用，NO禁用.(默认值=NO)
- chroot_list_enable
  - 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_file=/etc/vsftpd/chroot_list
  - 是否限制在主目录下的用户名单

- chroot_local_user是一个全局性的设定，其为YES时，全部用户被锁定于主目录，其为NO时，全部用户不被锁定于主目录。
- 那么我们势必需要在全局设定下能做出一些“微调”，即，我们总是需要一种“例外机制”，
- 所以当chroot_list_enable=YES时，表示我们“需要例外”。
  - 而”例外“的含义总是有一个上下文的，即，当”全部用户被锁定于主目录“时（即chroot_local_user=YES），”例外”就是：不被锁定的用户是哪些；
  - 当chroot_local_user=NO，”例外”“就是：要被锁定的用户是哪些。

	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

- 关于被动模式的数据连接
  - pasv_enable=Yes
  - pasv_min_port=50000
  - pasv_max_port=60000
- 设置用户类型的访问
  - local_enable=<YES/NO>
  - guest_enable=<YES/NO>
  - anonymous_enable=<YES/NO>

配置速率限制和每客户的连接数限制

- 配置指令
  - local_max_rate=80000 //本地用户最大80 KB/s
  - anon_max_rate=40000 //匿名用户最大40 KB/s
  - max_per_ip
  - max_clients

修改vsftpd的默认配置

- anon_upload_enable=YES
  - //允许匿名用户上传
- anon_mkdir_write_enable=YES
  - //允许匿名用户创建新目录
- anon_other_write_enable=YES
  - 允许匿名用户有更名或删除操作的权限
- write_enable=YES
  - 开放本地用户写的权限必须打开
- chroot_local_user=YES
  - 全部用户被锁定于主目录

- 重新启动vsftpd服务。
  - # service vsftpd restart
- 修改匿名用户上传目录的权限，匿名用户的默认目录是“/var/ftp/pub”。
  - # chmod 777 /var/ftp/pub
- 检查匿名用户是否可以下载、上传
- 增加一个用户，使用该用户登录ftp。

FTP命令及客户端

- ftp命令，如get、put等，可用?或help获得帮助
- Linux下命令行建议使用：lftp
- Windows也有ftp命令，或者图形化客户端，如FlashFXP