第5章 chapter 5

FTP服务器搭建与应用

教学目标与要求

文件传输协议(File Transfer Protocol,FTP)服务是Internet上最早提供的服务之一,应用非常广泛,至今它仍是最基本的应用之一。FTP提供了在计算机网络上任意两台计算机之间相互传输文件的机制。由于FTP操作性好,开放性强,在Internet上进行信息传递与共享非常方便,所以目前越来越多的FTP服务器已连入Internet,实现了资源共享。

本章将介绍FTP的基本概念、VSFTP服务器的搭建及访问FTP服务器的方法等。通过本章的学习,读者应该做到:

- 了解FTP的基本原理。
- 掌握安装和启动默认的VSFTP服务。
- 掌握修改配置文件的方法。
- 了解VSFTP两种运行模式的区别。
- 熟练掌握各种FTP服务器的配置方法。

教学重点与难点

配置不同安全级别的FTP服务器。

5.1 FTP简介

FTP能够使用户不需要了解远程主机操作系统的操作方法,就可直接完成主机之间可靠的文件传输。同时,FTP允许用户使用一组标准的命令集,在远程主机访问文件,从而使不同操作系统的客户都可与文件服务器进行通信,降低了用户工作的复杂度,保证了操作的通用性。

FTP是TCP/IP应用层上的具体应用,即它工作在OSI模型或TCP/IP模型的应用层。FTP使用传输层的TCP,建立连接可靠的链路。使用FTP可以高效地从FTP服务器下载大信息量的数据文件,将远程主机上的文件复制到自己的计算机上,达到资源共享

和传递信息的目的。

5.1.1 FTP的工作原理

1. 工作原理

FTP服务与大多数Internet服务类似，也是基于客户端/服务器(C/S)模式的。客户端通过支持FTP的程序连接到主机上的FTP服务器；用户通过客户端程序向服务器程序发出命令；服务器程序执行用户发出的命令，然后将执行结果返回给客户端。

客户端与服务器建立TCP连接时必须各自使用一个端口。FTP有两个连接：一个是控制连接；另一个是数据传输。因此，FTP需要两个端口，其中一个端口作为控制连接端口，即21端口，用于发送指令给服务器以及等待服务器响应；另外一个端口作为数据传输端口，即20端口(仅用PORT模式)，用于建立数据传输通道，主要实现在客户端从服务器获得文件，从客户端向服务器发送文件，从服务器向客户端发送文件或目录列表。

在FTP连接过程中，控制连线始终保持连接状态；而数据连线是需要时才建立的，即有传输文件时才建立连接；若文件传输完毕，则中断此连接。结束FTP操作时，控制连线也相应结束。FTP的工作流程如图5.1所示。

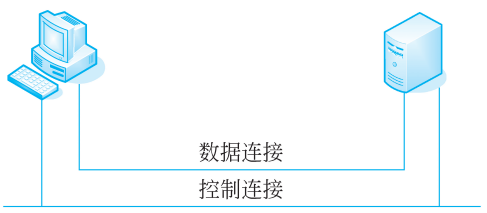

图5.1 FTP的工作流程

2. 登录流程

FTP的通信过程由多个步骤构成。从建立连接、传输文件到断开连接，这些不同的动作通过FTP的指令完成。当客户端与FTP通信时，首先要进行身份验证，如图5.2所示。

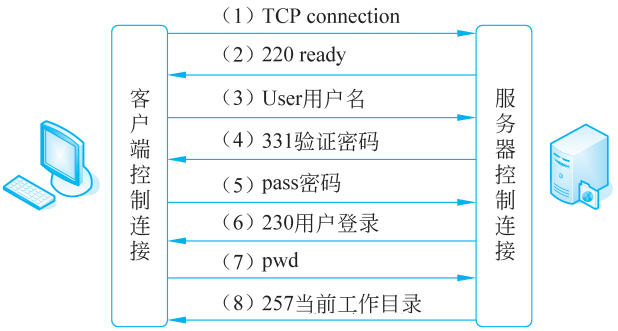

图5.2 FTP身份验证

(1) 客户端向服务器发送建立TCP连接的请求。

(2) 服务器响应220代码，表明21号端口工作正常，处于监听状态。

(3) 客户端以User指令发送用户名。

(4) 服务器响应331代码，通知客户端发送密码。

(5) 客户端使用pass指令发送密码。

(6) 服务器验证客户端的用户名和密码匹配关系。如果成功,则响应230代码,通知客户端身份验证通过。

(7) 客户端提交pwd指令,请求显示当前路径。

(8) 服务器响应257代码,显示当前工作目录。

5.1.2 FTP传输模式

FTP的任务是把文件从一台计算机传送到另一台计算机。FTP的传输有两种方式:ASCII码传输模式和二进制传输模式。

1. ASCII码传输模式

ASCII码传输模式即文本传输模式。假设用户正在复制的文件是包含简单ASCII码的文本文件,如果客户端和服务器上运行的操作系统不相同,那么对文件格式的处理也会有所不同。FTP在文件传输时会自动调整文件内容,并把文件转换成另一台主机存储文本文件的格式。但必须注意的是,不是所有文件都可以转换,很多情况下,要传输的文件不是文本文件,而可能是可执行文件、压缩文件或图片文件等。复制这些非文本文件时就不要用ASCII码传输模式了,此时必须使用二进制传输模式。

2. 二进制传输模式

二进制传输模式是指在文件的传输过程中保存文件的位序一致,并且原始文件和副本一一对应。如果两台操作系统不同的主机用二进制传输模式来传输文件,则对于保存文件的位序是没意义的。若传送可执行文件、压缩文件和图片文件,就必须使用二进制模式。如果用ASCII码模式传输,则会显示一堆乱码。如果传送的这两台机器类型相同,则二进制模式对文本文件和数据文件都是可以有效完成的。

5.1.3 FTP连接模式

FTP主要支持两种连接模式:一种是主动传输模式(PORT模式);另一种是被动传输模式(PASV模式)。主动传输模式FTP的客户端发送PORT命令到FTP服务器。被动传输模式FTP的客户端发送PASV命令到FTP服务器。

1. 主动传输模式

主动传输模式是指FTP客户端随机开启一个端口(通常是1024号以上端口)向FTP服务器的TCP 21端口发起控制连接请求,在FTP的控制连接成功建立后,如果客户端再提出目录列表、传输文件请求时,那么客户端会在这个控制通道上发送PORT命令,此命令通常包含客户端用哪个端口接收数据。当FTP服务器接收到客户端发送的PORT命令时,与其进行协商确定,然后FTP服务器使用TCP 20号端口作为服务器端的数据连接端口与客户端建立起数据连接。20号端口没有监听进程来监听客户请求,它只用于连接源地址是服务器端的情况,如图5.3所示。在主动传输模式下,FTP的数据连接与控制连接方向相反,控制连接是由客户端主动发起的,而数据传输的连接是由服务器向客户端发起的。客户端的连接端口由服务器端和客户端通过协商确定。

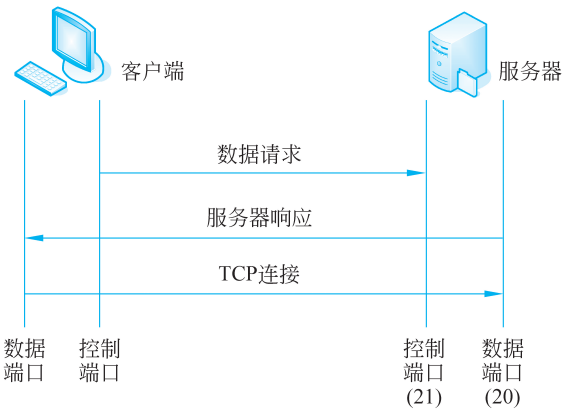

图 5.3　FTP 主动模式

2. 被动传输模式

被动传输模式在建立控制通道的时候与主动传输模式类似，不同的是，被动传输模式使用 PASV 命令，而不是 PORT 命令。在 FTP 的控制连接成功建立后，客户端在提出目录列表及传输文件请求时，客户端会在这个控制通道上发送 PASV 命令。当 FTP 服务器接收到 PASV 命令后，就处于被动传输模式。也就是说，FTP 服务器等待客户与其联系。此时，FTP 服务器在非 20 号端口（通常是 1024 号以上端口）上监听客户端的请求。FTP 服务器将使用该端口进行数据的传送，此时 FTP 服务器已经不再需要建立一个新的和客户端之间的连接，如图 5.4 所示。在被动传输模式下，FTP 的数据连接与控制连接方向一样，控制连接和数据传输的连接都是由客户端向服务器发起的。

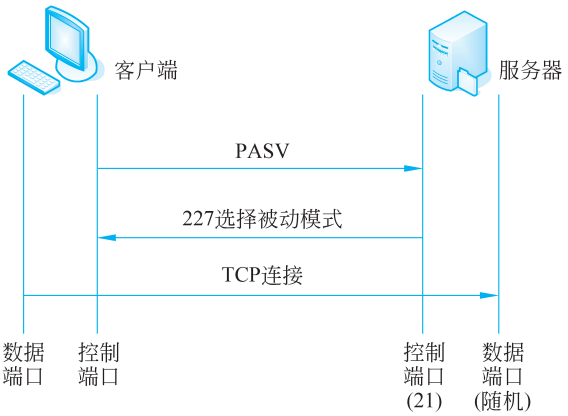

图 5.4　FTP 被动模式

说明：

(1) 被动传输模式受到很多防火墙的限制，通常防火墙都不允许接受外部发起的连接，而主动传输模式下也有许多内网的客户端因为防火墙的限制不能用 PORT 模式登录 FTP 服务器，从而使得服务器的 TCP 20 号端口不能与客户端建立数据连接。这也是可能造成无法工作的原因。

(2) FTP服务器被动模式需要使用大于1024号的端口,所以在配置服务器端的防火墙时,请开启1024号以上的端口,并适当限制范围;否则,客户端将无法使用被动模式连接FTP服务器。

其实,除上述两种模式外,还有一种单端口模式。在该模式的数据连接请求由FTP服务器发起。使用该传输模式时,客户端的控制连接端口和数据连接端口是一样的。由于这种模式无法在短时间连续输入数据、传输命令,所以该模式不常用。

5.1.4 FTP用户分类

1. 匿名用户

客户端访问FTP资源时,可以在没有服务器账户及密码的情况下,使用匿名(anonymous)身份获取公共资源,但权限有限。

2. 实体用户

实体用户(real user)是指FTP服务器的本地账户,使用/etc/passwd中的用户名为认证方式。

3. 虚拟用户

区别于实体用户,FTP支持建立专有用户,将账号及密码保存在数据库中,采用非系统账户访问服务器资源。相对于FTP的实体用户而言,虚拟用户只能访问FTP共享资源,增强了系统安全性。并且,客户端使用虚拟用户登录,需要提交账号和密码,管理员可以根据这些账号进行策略设置,从而增加了对用户和下载的可管理性。考虑到FTP服务器的安全性以及管理因素,选择虚拟用户登录是一个非常可靠的方案。

5.2 安装FTP服务器

Linux下的FTP服务器软件有很多,其中比较知名的有WU-FTP(Washington University-FTP)和VSFTP。WU-FTP是一个很不错的FTP服务器软件,其功能非常强大,并且能够很好地运行于多种UNIX类型的操作系统。不过,作为后起之秀的VSFTP现在也越来越流行了。VSFTP中VS的意思是Very Secure。从名称可以看出,VSFTP设计的出发点就是安全性,下面以VSFTP配置FTP服务器。

安装VSFTP服务之前,首先安装VSFTP软件包。

```
vsftpd-2.0.5-10.el5.i386
```

5.2.1 安装VSFTP

如果在安装Linux系统时没有选择安装VSFTP服务,此时就要进行安装。如果无法确认是否安装了该软件,或者不知道安装了哪个版本,可以输入以下命令查看。

```
[root@zhou~]#rpm -qa | grep vsftpd
```

查看结果如下，表明系统已经安装了 vsftpd-2.0.5-10.el5。

```
vsftpd-2.0.5-10.el5
```

如果没有安装 VSFTP 服务程序的 RPM 安装包文件，则可以通过 Red Hat Enterprise Linux 5 的安装盘(DVD 版第一张)进行安装。加载光驱后在光盘的 Server 目录下找到 vsftpd-2.0.5-10.el5.ppc.rpm 安装包文件进行安装，如图 5.5 所示。

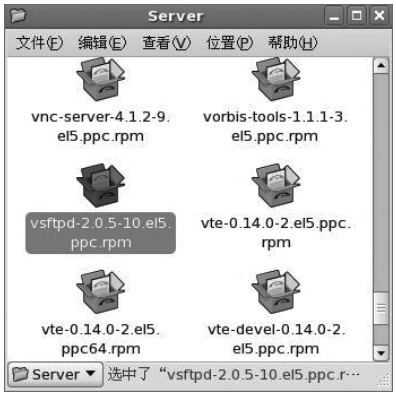

图 5.5 VSFTP 安装包

5.2.2 启动与停止 VSFTP

1. 启动 VSFTP

```
service vsftpd start 或 /etc/rc.d/init.d/vsftpd start
```

2. 关闭 VSFTP

```
service vsftpd stop 或 /etc/rc.d/init.d/vsftpd stop
```

3. 重新启动 VSFTP

```
service vsftpd restart 或 /etc/rc.d/init.d/vsftpd restart
```

4. 重新加载 VSFTP

```
service vsftpd reload 或 /etc/rc.d/init.d/vsftpd reload
```

5. 自动加载

```
Chkconfig -level 3 vsftpd on        #运行级别 3 自动加载
Chkconfig -level 3 vsftpd of        #运行级别 3 不自动加载
```

或用 ntsysv 命令，利用图形界面对 VSFTP 自动加载进行配置。

5.3 FTP 常规服务器配置

要深入掌握 VSFTP 的配置，首先要了解其文件目录结构，如表 5.1 所示，可见其目录文件结构非常简洁。

表 5.1 VSFTP 的文件目录结构

目 录	说 明
/usr/sbin/vsftpd	VSFTPD 的主程序
/etc/rc.d/init.d/vsftpd	启动 VSFTPD 的脚本
/etc/vsftpd/vsftpd.conf	主配置文件
/etc/pam.d/vsftpd	PAM 认证文件
/var/ftp	匿名用户的主目录
/var/ftp/pub	匿名用户的下载目录
/etc/vsftpd/ftpusers	禁止使用 VSFTPD 的用户列表文件
/etc/vsftpd/user_list	禁止或允许使用 VSFTPD 的用户列表文件

其中 VSFTP 文件主要有以下三个。

1. vsftpd.conf

vsftpd.conf 是 vsftpd 的核心配置文件，位于/etc/vsftpd/目录下。

2. /etc/vsftpd.user_list

/etc/vsftpd.user_list 为禁止或允许使用 vsftpd 的用户列表文件。

3. /var/ftp

/var/ftp 为默认情况下匿名用户的根目录。

5.3.1 主配置文件 vsftpd.conf

VSFTP 与 Samba 有很多类似的地方。它们相似的地方主要就是配置文件的格式。整个配置文件都由很多字段组合而成，其格式如下：

```
定段= 设定值
```

这与 Samba 几乎一样。需要特别说明的是，“=”两边没有空格，与 Samba 不同。安装 vsftpd 的主程序后，主配置文件就自动建立好了，其中以“#”开头的表示注释。整个配置文件一共有 117 行。打开 vsftpd.conf 可查看其内容(部分)。

```
[root@zhou ~]#vi /etc/vsftpd/vsftpd.conf
#Allow anonymous FTP?(Beware-allowed by default if you comment this out).
anonymous_enable=NO
#
#Uncomment this to allow local users to log in.
local_enable=YES
#
#Uncomment this to enable any form of FTP write command.
write_enable=YES
```

下面先对配置文件中的常用命令进行介绍。

1. 进程选项

```
Listen(YES|NO)
```

作用：Listen 字段表示是否使用 stand-alone 模式启动 VSFTPD，而不是使用超级进程（xinetd）控制它（VSFTPD 推荐使用 stand-alone 方式）。

YES：使用 standalone 启动 VSFTPD。

NO：不使用 standalone 启动 VSFTPD。

【例 5.1】 采用独立进程来控制 VSFTPD。

```
listen=YES
```

2. 登录和访问控制选项

1）anonymous_enable（YES|NO）

作用：anonymous_enable 字段用于控制是否允许匿名用户登录。

YES：表示允许；NO：表示不允许。

2）local_enable（YES|NO）

作用：local_enable 字段用于控制是否允许本地用户登录。

YES：表示允许；NO：表示不允许。

【例 5.2】 允许本地用户登录 FTP。

```
Local_enable=YES
```

3）pam_service_name

作用：用于设置在使用 PAM 模块进行验证时所使用的 PAM 配置文件名。

该字段默认值为 vsftpd，而默认的 PAM 配置文件为/etc/pam.d/vsftpd。

4）userlist_enable（YES|NO）

作用：userlist_enable 字段表示是否使用控制用户登录的用户列表。用户列表由 userlist_file 字段所指定。如果用户出现在列表中，则在登录 FTP 服务器时被 vsftpd 禁止登录。

YES：表示允许；

NO：表示不允许。

【例 5.3】 设置一个禁止登录的用户列表文件/etc/vsftpd/user_list，并让该文件可以正常工作。

```
userlist_enable=YES
userlist_file=/etc/vsftpd/user_list
```

5）tcp_wrappers（YES|NO）

作用：是否在 VSFTPD 中使用 tcp_wrappers 远程访问控制机制。

YES：表示使用；

NO：表示不使用。

3. 匿名用户选项

匿名用户访问服务器相关设置，使用以下这些字段的时候，必须设置 anonymous_

enable＝YES。

```
anou_root
```

作用：设置匿名用户的根目录，也就是匿名用户登录所在的目录。

【例 5.4】 设置匿名用户的根目录为/var/ftp/temp。

```
anou_root=/var/ftp/temp
```

4. 本地用户选项

本地用户访问服务器的相关设置，使用以下这些字段时，必须将 local_enable 设置为 YES。

```
local_umask
```

作用：local_umask 字段用于设置本地用户新建文件的 umask 数值。大多数 FTP 服务器都在使用 022，也可以根据需要自行修改。

5. 目录选项

影响目录设置的相关字段有

```
dirmessage_enable(YES|NO)
```

作用：dirmessage_enable 字段用于设置是否开启目录提示功能。

YES：表示开启；

NO：表示不开启。

说明：如果开启了目录提示功能，则当用户进入某一目录时，会检查该目录下是否有 message_file 字段所指定的文件。如果有，则会将文件内容显示在屏幕上。

6. 文件传输选项

文件传输的字段有

```
write_enable(YES|NO)
```

作用：write_enable 字段用于设置使用者是否有写权限。

YES：表示可以删除和修改文件；

NO：表示不可以删除或修改文件。

7. 日志选项

有关日志行为的字段有以下两个。

1）xferlog_enable(YES|NO)

作用：xferlog_enable 字段表示是否设置用于记录下载和上传的日志文件。

YES：表示启用；

NO：表示不启用。

说明：日志文件的名称和位置需要由 xferlog_file 字段来设置。

【例 5.5】 设置记录下载和上传的日志文件/var/log/vsftp.log。

```
xferlog_enable=YES
xferlog_file=/var/log/vsftp.log
```

2）xferlog_std_format(YES|NO)

作用：xferlog_std_format 字段用于设置日志的格式是否采用标准格式。

YES：表示使用标准格式；

NO：表示不使用标准格式。

8. 网络选项

与网络设置相关的字段有以下两个。

1）connect_from_port_20

作用：设置以 port 模式进行数据传输时使用 20 端口。

YES：表示使用；

NO：表示不使用。

2）connect_timeou

作用：设置客户端尝试连接 vsftpd 命令通道的超时时间，以秒为单位。

说明：如果客户端在尝试连接 vsftpd 的命令通道时超时，则强制断开。

5.3.2 匿名账号 FTP 服务器

匿名账号 FTP 服务器面向的用户很不固定。为了方便管理，需使匿名用户可以访问 FTP 服务。根据不同的应用环境，可以对匿名账号 FTP 服务器进行不同的设置。

1. 与匿名相关的常用字段

要使匿名用户能访问服务器，必须把 anonymous_enable 字段设置为 YES。在主配置文件中，和匿名用户相关的常用字段还有如下 5 个。

1）anon_mkdir_write_enable(YES|NO)

作用：控制是否允许匿名用户创建目录。

YES：表示允许；

NO：表示不允许。

2）anon_root(YES|NO)

作用：用于设置匿名用户的根目录。

YES：表示允许；

NO：表示不允许。

3）anon_upload_enable(YES|NO)

作用：控制是否允许匿名用户上传文件。

YES：表示允许；

NO：表示不允许。

4）anon_world_readable_only(YES|NO)