服务器知识手册

（八）

狄登峰 主编

需要全本请访问 www.ertongbook.com

目　　录

FTP 服务器 1
用 Linux 架设 FTP 服务器 1
小组开发环境搭建 24
国人自己的专业 FTP 服务器软件 34
FTP 非交互方式文件传输 38
基于 Linux 的校园网计费系统 40
构造公司内部 Web、FTP 服务器 44
如何以 Solaris 架设 FTP 虚拟系统 48
FTP 服务器如何实现安全性 52
基于 UNIX 平台 FTP 服务器的建立 55
NT 中如何实现用户只能进入自己的 FTP 目录 59
ProFtpd 快速指南 60
Serv-U3.0 的 User 和 Group 设置 69
Serv-U3.0 的 Domain 设置 73
Serv-U3.0 的 Server 设置 79
Serv-U:快速构建功能强大 FTP 服务器 83
Leapftp 的安全问题 98
FTP 命令详解 101
文件共享服务器 103
如何组建高速又安全的文件服务器 103
强化 Win2003 文件服务器 109
轻松搭建 Excel 服务器 118
用 2003 架设共享服务器 123

FTP 服务器

用 Linux 架设 FTP 服务器

概述

使用文件传输协议（FTP）来通过网络在计算机之间传输文件是很普遍的一种方法。几乎在所有的平台上面都有 FTP 的客户端和服务端的软件，因此用 FTP 来传送文件也是很方便的一个方法。

有很多配置 FTP 服务器的不同方法。其中一种是把 FTP 配置成只对系统中的用户开放的私有服务器，这也是 FTP 的默认配置。一个私有的 FTP 服务器只运行系统中的用户访问，而且可以对用户进行访问控制，这样可以给予或拒绝特定用户的访问权限。

另一种是把 FTP 服务器配置成匿名服务器。匿名 FTP 服务器允许任何人（不管有没有帐号）访问服务器并传输文件。因为可能存在潜在的安全问题，必须小心配置使得只允许访问系统中特定的目录。在这一节里，我们把 FTP 配置成“chrooted”的方式，这种配置运行用户访问，例如：Web 站点的目录，但是不允许他们访问更高一层的目录。

注意事项

下面所有的命令都是 Unix 兼容的命令。

源路径都为“/var/tmp”（当然在实际情况中也可以用其它路径）。

安装在 RedHatLinux6.1 下测试通过。

要用“root”用户进行安装。

wu-ftp 的版本号是 2.6.0。

编译和安装

把软件包（tar.gz）解压缩：

[root@deep]#cpwu-ftpd-version.tar.gz/var/tmp

[root@deep]#cd/var/tmp

[root@deep]#tarxzpfwu-ftpd-version.tar.gz

编译和优化

转到 wu-ftpd 的新目录下，运行下面的命令：

编辑“ftpcount.c”文件（vi+241src/ftpcount.c），改变下面这一行：

#ifdefined(LINUX)

改为：

#ifdefined(LINUX_BUT_NOT_REDHAT_6_0)

编辑“pathnames.h.in”文件（vi+42src/pathnames.h.in），改变下面这一行：

#define_PATH_EXECPATH"/bin/ftp-exec"

改为：

#define_PATH_EXECPATH"/usr/bin/ftp-exec"

我们把“ftp-exec”从“/bin”目录改到“/usr/bin”目录下。

先设置编译器的编译参数：

CC="egcs"

CFLAGS="-O9-funroll-loops-ffast-math-malign-double-mcpu=pentiumpro-march=pentiumpro-fomit-frame-pointer-fno-exceptions"

./configure

--prefix=/usr

--sysconfdir=/etc

--localstatedir=/var

--disable-dnsretry

--enable-quota

--enable-pam

--disable-daemon

--disable-newlines

--disable-virtual

--disable-plsm

--disable-pasvip

--disable-anonymous

--enable-ls

--enable-numericuid

这些编译参数告诉编译器如何编译 wu-ftpd：

不要用失败的 DNS 查询

加入对定额（QUOTA）的支持（如果 OS 支持）

加入对 PAM 的支持

不允许作为单独的 daemon 运行

删除过多的空行

不支持虚拟服务器

禁止 PID 加锁睡眠消息（用于繁忙的站点）

被动连接的时候不要求用同样的 IP

不允许匿名 ftp 访问

使用内部的“ls”命令（试验性的）

内部的“ls”命令显示 UID 而不显示用户名（为了提高速度）

用下面的命令编译和安装软件：

需要全本请访问 www.ertongbook.com

make

makeinstall

install-m755util/xferstats/usr/sbin

touch/var/log/xferlog

chmod600/var/log/xferlog

cd/usr/sbin

ln-sfin.ftpd/usr/sbin/wu.ftpd

ln-sfin.ftpd/usr/sbin/in.wuftpd

strip/usr/bin/ftpcount

strip/usr/bin/ftpwho

strip/usr/sbin/in.ftpd

strip/usr/sbin/ftpshut

strip/usr/sbin/ckconfig

strip/usr/sbin/ftprestart

上面的“make”**和**“makeinstall”**可以配置软件以保证系统中有编译所需要的函数库，然后把所有的源文件都编译成可执行的二进制文件，最后把二进制文件和配置文件安装到相应的目录里**。

“install–m”**安装**“xferstats”**程序，用于统计传输了多少文件**。“touch”**命令为** xferstats **在**“/var/log”**目录下创建日志文件**。“chomod”**把**“xferlog”**的权限改为只对超级用户**“root”**可读和可写**。**接着，我们为**“in.ftpd”**二进制文件创建符号链接**。**最后，用**“strip”**命令减小所有二进制文件的大小以提高** wu-ftpd **的性能**。

清除不必要的文件

[root@deep]#cd/var/tmp

[root@deep]#rm-rfwu-ftpd-version/wu-ftpd-version.tar.gz

“rm”命令删除所有编译和安装 wu-ftpd 所需要的源程序，并且把 wu-ftpd 软件的压缩包删除掉。

为 FTP 站点的用户建立没有 shell 的帐号

首先，创建一个新的用户，这个用户被允许连接到 ftp 服务器上。因为要有“chroot”的环境，这个帐号不同于正常的用户帐号，不能受访问限制。“chroot”使用户产生这样的感觉好像自己已经在文件系统的最顶层了。

第一步

用下面的命令在“/etc/passwd”文件中创建用户。对于每个允许访问 ftp 服务器的新用户都要重复这个步骤。

[root@deep]#mkdir/home/ftp

[root@deep]#useradd-d/home/ftp/ftpadmin/-s/dev/nul lftpadmin＞/dev/null2＞&1

[root@deep]#passwdftpadmin

Changingpasswordforuserftpadmin

NewUNIXpassword:

RetypenewUNIXpassword:

passwd:allauthenticationtokensupdatedsuccessfully

第二步

编辑“/etc/shells”文件并加入一个空 shell，如：null。这个假的 shell 可以限制用户对 ftp 服务器的访问。

[root@deep]#vi/etc/shells

/bin/bash

/bin/sh

/bin/ash

/bin/bsh

/bin/tcsh

/bin/csh

/dev/null?Thisisouraddednoexistentshell

第三步

现在编辑“/etc/passwd”**文件，手工加上**“/./”**把**“/home/ftp”**目录和**“/ftpadmin”**目录分开，用户**“ftpadmin”**会自动转到**（chdir）“/ftpadming”**目录下。在**“passwd”**文件中每添加一个** ftp **用户都要重复这个步骤。**

编辑“passwd”**文件**（vi/etc/passwd），**把下面这一行改为：**

ftpadmin:x:502:502::/home/ftp/ftpadmin/:/dev/null

改为：

ftpadmin:x:502:502::/home/ftp/./ftpadmin/:/dev/null

帐号为“ftpadmin”，**这这个帐号的家目录有一些奇怪。第一部分**“/home/ftp/”**表示**“chroot”**时作为根目录的目录。被点号分开的**“/ftpadmin”**表示当登录** ftp **服务器的时候会自动转到这个目录。**“/dev/null”**这个空** shell **不允许**“ftpadmin”**像正常用户那样登录。经过这些改变，**“ftpadmin”**用户用的不是真正的** shell **而是伪** shell，**这样访问** ftp **服务器就受到限制。创建一个**“chroot”**用户环境**

先要创建一个简单的根文件系统（rootfilesystem），**包含有足够的文件，如果二进制程序、口令文件，等等。当用户登录的时候，**Unix **就可以改变根文件系统**（chroot）。**注意一下，如果编译的时候象上面那样加上**“--enable-ls”**参数，**“/home/ftp/bin”**和**“/home/ftp/lib”**两个目录就可以不要了，因为** WU-FTP **会用自己带的**“ls”。**不过我们还是介绍一下旧的方法，也就是把**“/bin/ls”**拷贝到**“/home/ftp/bin”（chroot **之后就是**“/bin”）**目录下，然后把相关的运行库拷贝到**“/home/ftp/lib”**目录下。**

第一步

创建改变根文件系统（chrooted）**环境所需要的所有的目录**：

[root@deep]#mkdir/home/ftp/dev

[root@deep]#mkdir/home/ftp/etc

[root@deep]#mkdir/home/ftp/bin(requireonlyifyouarenotusingthe“--enable-ls”option)

[root@deep]#mkdir/home/ftp/lib(requireonlyifyouarenotusingthe“--enable-ls”option)

第二步

把新目录的权限设成 0511：

[root@deep]#chmod0511/home/ftp/dev

[root@deep]#chmod0511/home/ftp/etc

[root@deep]#chmod0511/home/ftp/bin(requireonlyifyouarenotusingthe“--enable-ls”option)

[root@deep]#chmod0511/home/ftp/lib(requireonlyifyouarenotusingthe“--enable-ls”option)

上面这些“chmod”**命令把** chrooted **之后的**“dev”、“etc”、“bin”**和**“lib”**目录设置成超级用户**“root”**可读、可执行，用户组和所有用户可执行**。

第三步

把“/bin/ls”**文件拷贝到**“/home/ftp/bin”**目录下，并把**“ls”**的权限改为** 0111（**不运行用户改变这个文件**）。

[root@deep]#cp/bin/ls/home/ftp/bin(requireonlyifyouarenotusingthe“--enable-ls”option)

[root@deep]#chmod0111/bin/ls/home/ftp/bin/ls(requireonlyifyouarenotusingthe“--enable-ls”option)

第四步

找到“ls”**程序所需的共享库**：

[root@deep]#ldd/bin/ls(requireonlyifyouarenotusingthe“--enable-ls”option)

libc.so.6=＞/lib/libc.so.6(0x00125000)

/lib/ld-linux.so.2=＞/lib/ld-linux.so.2(0x00110000)

把共享库拷贝到“/home/ftp/lib”**目录下：**

[root@deep]#cp/lib/libc.so.6/home/ftp/lib/(requireonlyifyouarenotusingthe“--enable-ls”option)

[root@deep]#cp/lib/ld-linux.so.2/home/ftp/lib/(requireonlyifyouarenotusingthe“--enable-ls”option)

注意：如果想用 Linux **的**“ls”**程序而不是用** WU-ftpd **自带的**“ls”（**编译时加上**“--enable-ls”**参数**），**才需要第三和第四步**。

第五步

创建“/home/ftp/dev/null”**文件：**

[root@deep]#mknod/home/ftp/dev/nullc13

[root@deep]#chmod666/home/ftp/dev/null

第六步

把“group”**和**“passwd”**文件拷贝到**“/home/ftp/etc”**目录下，然后再改变这两个文件**。

[root@deep]#cp/etc/passwd/home/ftp/etc/

[root@deep]#cp/etc/group/home/ftp/etc/

编辑“passwd”**文件**（vi/home/ftp/etc/passwd）**把除了**“root”**和允许使用** ftp **的用户之外的所有其它项删掉。这对于改变根文件系统的环境很重要，改变之后的**“passwd”**文件会是象下面这样的：**

root:x:0:0:root:/:/dev/null

ftpadmin:x:502:502::/ftpadmin/:/dev/null

编辑“group”**文件**（vi/home/ftp/etc/group），**把除了**“r

oot”和允许使用 ftp 的用户之外的所有其它项删掉。改变之后的“group”文件会是象下面这样的：

root:x:0:root

ftpadmin:x:502:

配置

可以到这去下载“floppy.tgz”文件：http://pages.infinit.net/lotus1/doc/opti/floppy.tgz。把“floppy.tgz”文件解开之后，可以在相应的目录下发现我们在这本书中介绍的所有软件的配置文件。这样就没有必要手工重新生成这些文件，或者用拷贝粘贴的方法把它们粘贴到配置文件中去。不管是打算自己动手生成配置文件还是拷贝现成的，你都要学会自己修改配置文件并且把配置文件拷贝到正确的目录下。下面将具体说明。

为了运行 FTP 服务器，必须创建或者把下面的文件拷贝到相应的目录下：

把“ftpaccess”文件拷贝到“/etc”目录下

把“ftpusers”文件拷贝到“/etc”目录下

把“ftphosts”文件拷贝到“/etc”目录下

把“ftpgroups”文件拷贝到“/etc”目录下

把“ftpconversion”文件拷贝到“/etc”目录下

把“ftp”文件拷贝到“/etc/pam.d”目录下

把“ftpd”文件拷贝到“/etc/logrotate.d”目录下

可以把“floppy.tgz”解压之后，找到上面列出来的文件，并拷贝到相应的目录下，或者用拷贝粘贴的方法从本书中直接粘贴出。

配置“/etc/ftpaccess”文件

“/etc/ftpaccess”文件是用来配置“ftpd”的。这个文件主要是设置允许哪个用户、多少用户访问 ftp 服务器，

需要全本请访问 www.ertongbook.com

以及一些安全方面的问题。配置文件的每一行或者定义一个属性或者设定一个属性值，。对于非匿名的“chroot”访问，必须创建一些“guestgroup”，每一个都要对应“/home/ftp/etc/group”文件中的项。

创建 ftpaccess 文件（touch/etc/ftpaccess），在文件中加入：

classopenarchguest208.164.186.*

limitopenarch20MoTuWeTh,Fr0000-1800/home/ftp/.too_many.msg

emailadmin@openarch.com

loginfails3

readmeREADME*login

readmeREADME*cwd=*

message/home/ftp/.welcome.msglogin

message.messagecwd=*

compressyesall

taryesall

chmodyesguest

deleteyesguest

overwriteyesguest

renameyesguest

logcommandsreal,guest

logtransfersreal,guestinbound,outbound

guestgroupftpadmin

guestgroupwebmaster

#Wedon‘twantusersbeingabletouploadintotheseareas.

upload/home/ftp/*/no

upload/home/ftp/*/etcno

upload/home/ftp/*/devno

#We‘llpreventdownloadswithnoretrieve.

noretrieve/home/ftp/etc

noretrieve/home/ftp/dev

logsecurityreal,guest

guest-root/home/ftpftpadminwebmaster

restricted-uidftpadminwebmaster

restricted-gidftpadminwebmaster

greetingterse

Keepaliveyes

noretrieve.notar

现在把文件的权限设成 600：

[root@deep]#chmod600/etc/ftpaccess

下面解释配置文件中的设置：

class

“class”**用来定义一个允许访问** ftp **服务器的用户类别。可以定义任意多的类别**（class）。**每一个**“class”**行的格式如下：**

class＜classname＞＜typelist＞＜addrglob＞

＜classname＞**是** class **的名字，**＜typelist＞**是允许加到类别**（class）**中的用户类型，**＜addrglob＞**是这个** class **允许的** IP **地址范围。**

＜typelist＞**中的项是用逗号隔开的，每一个项有三种可能的取值：**anonymous、guest **或** real。anonymous **用户是用** anonymous **或** ftp **帐号访问** ftp **服务器而且只需要访问公用文件的那些用户。**guest **用户有一些特殊因为他们在系统中没有帐号，但是却又是** guest **组的成员。**real **用户必须在** FTP **服务器上有帐号，而且需要经过服**

务器的安全验证。

＜addrglob＞可以用通配符，例如："*"表示所有的站点。下面这一行：

classopenarchguest208.164.186.*

表示只有在系统中有自己帐号的 guest 用户而且 IP 地址为"208.164.186.*"才能访问 ftp 服务器。

limit

"limit"根据 class 和时间范围来限制登录 ftp 服务器的用户数。"limit"的格式是：

limit＜class＞＜n＞＜times＞＜message_file＞

其中＜class＞是受限制的类别（class），＜n＞表示在这个类别中受到限制的最多用户数，＜times＞表示"limit"有效的时间段，＜message_file＞是当达到最大的用户数目的时候，别的用户还想登录时显示的信息。

＜times＞中的字符串用逗号隔开，每一个字串表示一天。星期一到星期日分别用 Mo、Tu、We、Th、Fr、Sa 和 Su 表示，周末也可以用 Wk 表示。表示时间的小时和分钟之间不要用冒号隔开。"-"用来表示范围。

例如，限制"openarch"这个类别，最多可以有 20 个用户，访问时间是星期一道星期四全天，星期五从半夜到下午六点。用下面这一行来表示：limitopenarch20MoTuWeTh,Fr0000-1800/home/ftp/.too_many.msg

如果一旦达到最大的用户数，还有别的用户想连接 ftp 服务器，就会把"/home/ftp/.too_mang.msg"中的信息传给用户。

loginfails

"loginfails"设置最多允许的登录失败的次数。可以用下面这一行来表示：

loginfails＜n＞

＜n＞表示最多允许的登录失败的次数。例如，只允许失败两次可以这样表示：

loginfails3

readme

“readme”设置在什么条件下，一旦当前目录中的文件发生了变化需要提醒用户。

这个命令的格式为：

readme＜path＞＜when＞

＜path＞是用来提醒用户的文件的名字（例如：README），＜when＞设置出现这个提示信息的条件。

＜when＞可以为下面两种形式：LOGIN 或 CWD=＜dir＞。如果为 LOGIN，当用户成功登录的时候就会出现提示信息。如果为 CWD=＜dir＞，当用户进入＜dir＞目录的时候就会有提示信息。

请记住当给匿名（anonymous）用户设置提示信息的路径的时候，这个路径必须是相对于匿名 ftp 目录。

message

“message”设置当用户登录或转到一个目录的时候会收到什么消息。可以设定多个消息。命令的格式为：

message＜path＞＜when＞

＜path＞表示需要显示的文件的完整路径名，＜when＞和“readme”中的＜when＞意思一样。

还需要注意的是消息文件的路径名也是相对于匿名 ftp 目录的。

例如：

message/home/ftp/.welcome.msgLOGIN

compress、tar、chmod、delete、overwrite、rename

如果这些都不设置，那么就使用默认值，也就是对所有人都是“yes”。下面例子中的设置的意思是给 guest 组 chmod、delete、overwrite 和 rename 文件的权力，所有人都可以使用 compress 和 tar。

例如：

compressyesall

taryesall

chmodyesguest

deleteyesguest

overwriteyesguest

renameyesguest

logcommands

因为安全上的原因需要记录用户使用的每一个命令。“logcommands”的格式是：

logcommands＜typelist＞

＜typelist＞是用逗号隔开的字串，表示哪些用户的命令需要记录下来，字串的取值可以是：anonymous、guest 或 real。

例如：要记录 real 和 guest 用户的每一个命令，可以这么表示：

logcommandsreal,guest

这些记录都保存在“/var/log/message”文件中。

logtransfers

因为安全文件需要把文件的传输都记录下来。“logtransfers”的格式是：

logtransfers＜typelist＞＜directions＞

＜typelist＞是用逗号隔开的字串，表示哪些用户的命令需要记录下来，字串的取值可以是：anonymous、g

uest 或 real。＜direction＞也是用逗号隔开的字串，设置需要记录的文件传输的方向，可以选择的两个传输方向是“inbound”（向内）和“outbound”（向外）。

例如，用下面表示记录所有 real 和 guest 用户的“inbound”和“outbound”方向的文件传输：

logtransfersreal,guestinbound,outbound

这些记录保存在“/var/log/xferlog”文件中。

guestgroup

这个命令用来设置 guest 组，每一行只能有一个成员。

例如：

guestgroupftpadmin

guestgroupwebmaster

logsecurity

用来设置记录 real、guest 或 anonymous 用户违反安全规则的行为。

logsecurity＜typelist＞

＜typelist＞是用逗号隔开的字串，字串的取值可以是：anonymous、guest 或 real。“real”表示真正在 ftp 服务器上有帐号的用户，“anonymous”表示匿名用户，“guest”表示 guest 用户。

例如：

logsecurityreal,guest

restricted-uid、restricted-gid、guest-root

这些用来设置是否允许 real 和 guest 用户访问家目录之外的目录。格式为：

guest-root＜root-dir＞

restricted-uid＜uid-range＞

需要全本请访问 www.ertongbook.com