# Linux ProFTPD文件共享

简介：

ProFTPD是一个安全、配置简单的FTP服务器软件，该软件采用与Apache相似的配置格式，比较容易配置与管理。在该项目开发以前，最流行的FTP软件是wu-ftpd，wu-ftpd具有很高的性能，但缺乏Win32FTP服务器的一些特色功能，而且wu-ftpd的安全问题一直存在。ProFTPD借鉴了wu-ftpd的有点，并且增加了很多wu-ftpd所不具备的功能。

## 安装ProFTPD软件

proftpd网址：<http://www.proftpd.org/>

git仓库下载：<https://github.com/proftpd/proftpd/releases>

ftp镜像下载：<ftp://ftp.proftpd.org/distrib/source/>

[root@centos7 ~]# wget <ftp://ftp.proftpd.org/distrib/source/proftpd-1.3.6.tar.gz>

[root@centos7 ~]# tar -zxvf proftpd-1.3.6.tar.gz -C /usr/src/proftpd

[root@centos7 ~]# cd /usr/src/proftpd

[root@centos7 ~]# ./configure --prefix=/usr/local/proftpd \

> --sysconfdir=/etc/ \

> --enable-nls \

> --enable-openssl \

> --enable-shadow

[root@centos7 ~]# make && make install

configure部分选项说明：

--prefix=PREFIX 指定安装路径

--sysconfdir=DIR 指定FTP服务配置文件路径

--localstatedir=DIR 指定运行状态的文件存放路径（默认/var/proftpd）

--with-modules=mod\_ldap 指定需要加载的功能模块

--enable-memcache 支持缓存功能

--enable-nls 支持多语言环境（如中文），安装完成后在注配置文件

中需要指定字符编码(UseEncoding 、UTF-8 、CP936)

--enable-openssl 支持TLS加密FTP服务

--enable-shadow 支持使用/etc/shadow验证用户密码

安装完成后，ProFTPD主程序目录位于/usr/local/proftpd目录下，服务器主配置文件为/etc/proftpd.conf。

创建proftpd启动账户，并添加环境变量

[root@centos7 ~]# export PATH=$PATH:/usr/local/proftpd/bin #临时生效

[root@centos7 ~]# cp /etc/profile /etc/profile.bak

[root@centos7 ~]# sed -i "/export PATH/i PATH=$PATH:/usr/local/proftpd/bin" \

> /etc/profile #永久生效

[root@centos7 ~]# useradd -M -s /sbin/nologin proftpd

## ProFTPD配置文件解析

ProFTPD主配置文件共分三个部分：全局设置、目录设置和匿名访问设置。

全局设置为全局生效的参数，参数直接使用空格分隔。

目录设置可以指定共享路径以及相关权限，目录设置使用<Directory "路径">开头，以</Directory>结尾，使用Limit设置路径权限。

如果需要开启匿名账户访问，则使用<anonymous "路径"></anonymous>设置匿名访问权限及访问策略。

ServerName "FroFTPD Default Installation"

# 服务器连接后显示的提示字符

ServerType standalone

# proftpd运行的方式,有 standalone和inetd

DeferWelcome off

# 只有在认证用户之后才显示欢迎消息

DefaultServer on

# 作为默认服务器

Prot 21

# 默认监听端口

UseIPv6 off

# 禁用IPv6

Umake 022

# 新文件的权限掩码

MaxInstances 30

# 最大并发连接数为 30

TimeoutLogin 120

# 登陆时允许idel的时间

TimeoutIdel 600

# 登陆后允许idel的时间

TimeoutNoTransfer 900

# 没有数据传输时允许idel的时间

User nobody

# 以nobody用户身份运行程序

Group nogroup

# 以nogroup组身份运行程序

RequireValidShell no

#用户是否拥有shell,关闭安全

AllowRetrieveRestart on

# 允许断点上传

AllowStoreRestart on

# 允许断点下载

UseEncoding on

# 启用UTF-8编码，并不允许客户端改变UTF-8编码。设置no，则禁用所有编码

RootLogin off

# 禁止root用户登陆ftp。on允许

MaxClientPerHost 2

# 每个ip只能由连个连接

MaxClientPerUser 1

# 每个账号只能由一个连接

UseReverseDNS off

# 关闭DNS反向查询，节省连接时间

SystemLog /vat/log/proftpd.log

TransferLog /var/log/proftpd.log

# 数据传输记录文件

LogFormat auth "%v %P %h %t "%r/" %s"

LogFormat write "%h %I %u %t "%r/" %s %b"

# 定义了几种日志格式，可以根据自己的需要定制

# %a ： 客户ip

# %A ： 匿名用户名（就是匿名用户的password）

# %b ： 发送请求的字节数

# %d ： 目录名（绝对路径）

# %D ： 目录名(绝对路径)

# %f ：上传或下载的文件名(绝对路径)

# %F ：上传或下载的文件名(相对路径)

# %h ：客户的域名

# %L ：本服务器ip

# %m ：客户发送的命令

# %p ：本服务器的端口

# %P ：服务进程的id

# %r ：客户发送的整条命令

# %t ：本地时间

# %T ：传送文件所用的时间(秒)

# %u ：客户登陆的用户名

DefaultRoot ~

# ftp的根目录，~限制用户只能访问自己的目录

AllowOverwrite on

# 允许文件可以重写

<Global> #设置一些全局参数

DisplayLogin welcome.msg

#显示~/welcome.msg中的欢迎信息,可以编辑welcome.msg自己制定欢迎信息

# %T 当前的时间

# %F 所在硬盘剩下的空间

# %C 当前所在的目录

# %R:客户的主机名

# %U:客户登陆的帐号

# %M:允许最大连接数

# %N:当前的连接人数

# %E:FTP服务器管理员的email

# %i:本次上传的文件数量

# %o:本次下载的文件数量

AllowOverwrite yes

#允许文件可以重新写

IdentLookups off

#查找客户的远程用户名,关掉节省连接时间

ExtendedLog /var/spool/syslog/proftpd/access.log WRITE,READ write

#以write的日志格式记录READ,WRITE的日志

ExtendedLog /var/spool/syslog/proftpd/auth.log AUTH auth

#以auth的日志格式记录AUTH的日志

</Global>

<Limit SITE\_CHMOD>

DenyAll

</Limit>

<Anonymous ~ftp> # 匿名用户设置

User ftp

Group ftp

UserAlias anonymous ftp

# 匿名用户以ftp用户登陆

MaxClients 10

# 最大客户数

MaxInstances 30

# 连接的间隔时间

RequireValidShell no

# 用户有没shell也可以使用FTP(安全)

DisplayLogin

DisplayChdir

<Limit WRITE>

DenyAll

# 拒绝所有写权限

</Limit>

<Limit LOGIN>

Order deny,allow

Deny from 172.16.0.0/11 #禁止172.16.0.0/11网段访问

Allow from all

</Limit>

<Directory pub>

<Limit READ>

AllowAll #所有人在pub目录有读权限

</Limit>

<Limit WRITE>

AllowUser ftpadmin #ftpadmin用户拥有写权限

DenyAll #其他用户无写权限

</Limit>

RateReadBPS 1024000 #下载最高速1M/s

RateReadFreeBytes 10240000 #下载总速度不超过10M/s

</Directory>

<Directory incoming>

<Limit STOR MKD>

AllowAll #所有人都可以在incoming目录上传文件,新建目录

</Limit>

<Limit WRITE>

AllowUser ftpadmin #允许ftpadmin用户写

DenyAll #其他用户无写权限

</Limit>

RateWriteBPS 1024000 #上传最高速1M/s

RateWriteFreeBytes 10240000 #上传总速度不超过10M/s

</Directory>

</Anonymous>

## ProFTPD权限设置

ProFTPD可以通过在目录属性中添加<Limit>的方式设置访问权限，访问权限设置可以根据自己的实际需求有选择的添加。

以下列出了权限指令以及对应的功能说明

权限指令 含义

CWD 进入该目录

MKD /XMKD 创建目录

RNFR/RNTO 更名

DELE 删除文件

RMD/XRMD 删除目录

READ 可读

WRITE 可写

STOR 可上传

RETR 可下载

DIRS 允许列出目录

LOGIN 允许登陆

ALL 全部

#以上权限结合动作一起使用:

AllowUser 设置允许的账户，多个账户使用逗号隔开

AllowGroup 设置允许的组账户，多个组账户使用逗号隔开

AllowAll 允许所有

DenyAll 拒绝所有

DenyUser 设置拒绝的账户，多个账户使用逗号隔开

DenyGroup 设置拒绝的组账户，多个组账户使用逗号隔开

## ProFtpd常用命令

ftpasswd

描述：创建用户文件、组文件，默认创建的用户文件为ftpd.passwd

语法：ftpasswd 选项.....

选项： --passwd 创建密码文件，即AuthUserFile指定的文件

--group 创建组文件

--name 指定创建的用户名

--uid 指定用户虚拟UID

--gid 指定虚拟GID

--home 指定用户家目录

--shell 指定用户Shell

--file 指定创建的文件名，默认为ftpd.passwd

演示：

[root@centos7 ~]# ftpasswd --passwd --name=tomcat --uid=1001 --gid=1001 \

> --home=/home/nohome --shell=/bin/false

解释：创建一个rpoftpd用户，用户名为tomcat，UID为1001，GID为1001，家目录位于/home/nohome目录，登陆shell为/bin/false。

## ProFTPD常见案例

### 1，虚拟用户应用案例

需求：ABC网站设置公司有商务部，页面设计部，开发部，运维部四个部门，各部门用户访问FTP后可以看到所有的目录，但只可以访问本部门目录，并且只允许上传文件，其余操作不允许，且需要开启FTP日志功能，FTP认证采用基于文件认证的方式，共享目录为/var/ftp。

1. 创建启动账户及目录

[root@centos7 ~]# useradd -M -s /sbin/nologin proftpd

[root@centos7 ~]# mkdir -p /var/proftp/{develop,ops,sales,design}

[root@centos7 ~]# chmod 777 /var/proftp/{develop,ops,sales,design}

1. 修改配置文件

部署服务最主要的步骤就是修改配置文件，部分参数在初始化配置文件中不存在，需要手动输入。

ServerIdent on # 不隐藏服务器版本

ServerName "ProFTPD Default Installation" # 服务器名称

ServerType standalone # 服务器运行类型

DefaultServer on # 默认为FTP服务器

UseEncoding on # 强制UTF-8编码

Port 21 # 监听20端口

AllowRetrieveRestart on # 允许断点下载

AllowStoreRestart on # 允许断点上传，配合下个

AllowOverwrite on # 允许重新写文件

UseIPv6 off # 禁用IPv6

Umask 022 # 上传文件权限掩码

RootLogin off # 禁止root用户登录

MaxInstances 30 # 最大并发连接数

UserReverseDNS off # 禁止反向解析DNS

IdentLookups off # 禁止查找远程客户端名

MaxLoginAttempts 3 # 最大尝试连接次数

MaxClientsPerHost 2 # 每个用户最大线程数

MaxClients 20 # 最大用户数

DeferWelcome on # 用户认证后显示消息

SystemLog /var/log/proftp.log # 日志文件

TransferLog /var/log/proftp.log # 数据传输记录日志文件

User proftp # 运行进程的用户

Group proftp # 运行进程的组

DefaultRoot /var/proftp # 禁锢根目录

#下面的匿名共享部分全部使用#注释，取消匿名访问功能

#<Anonymous ~ftp> # 匿名访问路径，~ftp=/var/ftp

# User ftp # 匿名访问映射用户

# Group ftp # 匿名访问映射用户组

# UserAlias anonymous ftp # 匿名用户以ftp用户登录

# MaxClients 10 # 匿名用户最多同时连接10个

# DisplayLogin welcome.msg # 登录显示文件里的欢迎消息

# DisplayChdir .message # 同上

# <Limit WRITE> # 当前文件夹权限设置

# DenyAll # 拒绝所有写操作

# </Limit>

#</Anonymous>

#用户登录是否需要shell（对虚拟用户很重要）

RequireValidShell off # 登录用户无需用拥有shell

#通过文件认证用户登录，需要使用ftpasswd命令创建该文件

AuthUserFile /usr/local/proftpd/ftpd.passwd # 虚拟用户认证文件

# 对/var/ftp 目录下的所有文件权限设置

<Directory "/var/proftp/\*">

<Limit CWD READ>

AllowAll # 允许所有用户列出目录

</Limit>

</Directory>

# 对/var/proftp/ops 目录的权限设置

<Directory "/var/proftp/ops">

<Limit CWD MAK RNFR READ WRITE STOR RETR>

#拒绝所有人往该目录下执行Limit后的操作指令

DenyAll

</Limit>

<Limit DELE>

#禁止任何人在该目录下删除文件

DenyAll

</Limit>

<Limit CWD MKD RNFR READ WRITE STOR RETR>

#仅允许tomcat用户可以执行Limit后的所有指令

AllowUser tomcat

</Limit>

</Directory>

# 对/var/ftp/develop 目录的权限设置

<Directory "/var/proftp/develop">

<Limit CWD MAK RNFR READ WRITE STOR RETR>

#拒绝所有人往该目录下执行Limit后的操作指令

DenyAll

</Limit>

<Limit DELE>

#禁止任何人在该目录下删除文件

DenyAll

</Limit>

<Limit CWD MKD RNFR READ WRITE STOR RETR>

#仅允许jacob和jack用户可以执行Limit后的所有指令

AllowUser jacob,jack

</Limit>

</Directory>

# 对/var/proftp/sales 目录的权限设置

<Directory "/var/proftp/sales">

<Limit CWD MAK RNFR READ WRITE STOR RETR>

#拒绝所有人往该目录下执行Limit后的操作指令

DenyAll

</Limit>

<Limit DELE>

#禁止任何人在该目录下删除文件

DenyAll

</Limit>

<Limit CWD MKD RNFR READ WRITE STOR RETR>

#仅允许sales1用户可以执行Limit后的所有指令

AllowUser sales1

</Limit>

</Directory>

# 对/var/proftp/design 目录的权限设置

<Directory "/var/proftp/design">

<Limit CWD MAK RNFR READ WRITE STOR RETR>

#拒绝所有人往该目录下执行Limit后的操作指令

DenyAll

</Limit>

<Limit DELE>

#禁止任何人在该目录下删除文件

DenyAll

</Limit>

<Limit CWD MKD RNFR READ WRITE STOR RETR>

#仅允许design1用户可以执行Limit后的所有指令

AllowUser design1

</Limit>

</Directory>

1. 创建虚拟账户

修改完配置文件后，接下来就需要创建访问FTP所需要的账户和密码。

[root@centos7 ~]# cd /usr/local/proftpd/

[root@centos7 ~]# ftpasswd --passwd --name=tomcat --uid=1001 --gid=1001 \

> --home=/home/nohome --shell=/bin/false

[root@centos7 ~]# ftpasswd --passwd --name=jacob --uid=1002 --gid=1002 \

> --home=/home/nohome --shell=/bin/false

[root@centos7 ~]# ftpasswd --passwd --name=jack --uid=1003 --gid=1003 \

> --home=/home/nohome --shell=/bin/false

[root@centos7 ~]# ftpasswd --passwd --name=sales1 --uid=1004 --gid=1004 \

> --home=/home/nohome --shell=/bin/false

[root@centos7 ~]# ftpasswd --passwd --name=design1 --uid=1005 --git=1005 \

> --home=/home/nohome --shell=/bin/false

1. 启动proftpd服务

[root@centos7 ~]# /usr/local/proftpd/sbin/proftpd

### 2，匿名用户应用

需求：开放/var/open 目录,只允许用户列出目录或下载目录，不允许其他操作。限制并发连接数量 和 限制下载速度，记录日志并自定义日志格式。

配置文件如下：

#匿名用户仅下载资源配置

############# 服务器设置 #################

#设置连接上显示的消息

ServerIdent on "Welcome to ftp.linux.cn"

#服务器名称

ServerName "This is a Download FTP Server"

#独立守护进程运行

ServerType standalone

#默认FTP服务器

DefaultServer on

#监听端口

Port 21

#权限掩码

Umask 022

#禁用IPv6

UseIPv6 off

#只允许proftpd用户执行ftp进程

User proftpd

#只允许proftpd用户组执行ftp进程

Group proftpd

#禁锢用户不能离开/var/open目录

DefaultRoot /var/open

#关闭反向解析DNS

UseReverseDNS off

#禁止查询远程客户端主机名

IdentLookups off

############## 客户端限制设置 ################

#允许最大并发连接数

MaxInstances 30

#每个账户最大允许尝试连接次数

MaxLoginAttempts 3

#每个ip只能有两个连接

MaxClientsPerHost 2

#每个帐号只能有两个连接

MaxClientsPerUser 2

#允许客户端最大同时连接数

MaxClients 20

################# 日志设置 ###################

#设置日志格式

#LogFormat auth "IP:%a Name:%u Psaawd:%A %r At:%t"

#LogFormat readwrite "IP:%a Name:%u Passwd:%a %M %f At:%t usedTime:%T"

#以auth的日志格式记录LOGIN的日志

#ExtendedLog /var/log/proftp\_login.log AUTH auth

#以write的日志格式记录READ，WRITE的日志

#ExtendedLog /var/log/proftp\_transfer.log READ,WRITE readwrite

#服务器日志

SystemLog /var/log/open\_ftp.log

#数据传输日志

TransferLog /var/log/open\_ftp.log

################下载/上传设置##################

#允许断点下载

AllowStoreRestart on

#允许断点上传

AllowRetrieveRestart on

#允许覆盖文件

AllowOverwrite on

############ 禁止本地用户登陆 ###############

#<Limit LOGIN>

# DenyAll

#</Limit>

#设置空闲登陆超时时间。登陆认证时间超过10秒，认证失败

TImeoutLogin 10

################ 匿名用户设置 ##################

<Anonymous "/var/open">

#用户验证成功自定义消息

#AccessGrantMsg "自定义消息"

#RequireValidShell on

#允许匿名运行proftpd程序的用户

User ftp

#允许匿名运行proftpd程序的用户组

Group ftp

#把所有匿名登陆的用户映射为ftp用户

UserAlias anonymous ftp

#最大客户端连接数。 会被全局设置覆盖

MaxClients 10 "最大连接10，你等会在来"

#限制每个ip只能有4个连接。会被全局设置覆盖

MaxClientsPerHost 4 "对不起，一个IP只允许4个连接"

#限制下载文件大小

MaxRetrieveFileSize 7 Mb

#限制上传文件大小

MaxStoreFileSize 10 Mb

#限制ftp用户的下载速度

TransferRate RETR 4000 user ftp

#限制ftp用户的上传速度

TransferRate STOR 2000 user ftp

#登陆显示消息

DisplayLogin welcome.msg

#设置空闲连接超时时间。发呆时间超过20秒，则自动退出登陆

#TimeoutIdle 20

#设置当没有数据传输时的超时时间.若20秒内没有数据传输则退出

#TimeoutNoTransfer 20

#设置被阻塞的下载的超时时间.传输数据中断时间超过20秒则停止传输

#TimeoutStalled 20

<Limit MKD RNFR DELE RMD WRITE STOR>

DenyAll

</Limit>

</Anonymous>

### 3，自定义proftpd启动文件

## 常见错误

### 1，如何对匿名账户隐藏一个目录

使用HideGroup或者HideUser指令可以隐藏目录。

语法格式pain段如下：

<Anonymous ~ftp>

...

<Directory test>

HideUser user1,user2,....

</Directory>

</Anonymous>

### 2，如何限制带宽

在新的Proftpd1.2.8版本后，软件加入了TransferRate指令，该指令支持对每个连接限制带宽，限制对上传和下载都有效。

### 3，如何限制上传和下载文件的最大容量

Proftpd1.2.7版本后提供了MaxRetrieveFileSize 和 MaxStoreFileSize，用来控制上传和下载文件的最大容量。

### 4，如何隐藏Proftpd软件的版本信息，防止针对版本漏洞的攻击

在主配置文件中添加ServerIdent off指令，即可对用户隐藏软件的版本信息

### 5，如何确保Proftpd可以开机启动

源码安装的Proftpd软件并不提供开机启动脚本，需要我们自己编写。将Proftpd启动脚本存放在/etc/init.d目录下，使用chkconfig --add proftpd将服务加入开机启动项，最后通过命令chkconfig proftpd on 将该服务设置为2345级别开机启动。

## proftpd配置技巧

### 技巧一、防止proftpd进行DNS反查以及对用户端进行ident确认

在proftpd.conf里面加入两行：

UseReverseDNS off

IdentLookups off

防止proftpd进行DNS反查以及对用户端进行ident确认。

===

### 技巧二、proftpd如何允许以root身份登录

在配置文件中使用下面的配置：

RootLogin on

===

### 技巧三、如何让匿名用户使用proftpd服务器

建立一个用户，用户名为guest，然后在配置文件中使用下面的配置：

AnonRequirePassword off

User private

Group private

RequireValidShell off

DenyAll

===

### 技巧四、如果要支持下载续传，那么必须指定：

AllowRetrieveRestart on

如果要支持上传续传，那么必须指定：

AllowOverwrite on

AllowStoreRestart on

必须同时指定AllowOverwrite和AllowStoreRestart的原因是由于重新上传或者续传也是属于覆盖文件。

同时记得不要同时使用HiddenStor和AllowStoreRestart。

===

### 技巧五、通过ls看见以"."号开头的文件

在配置文件中设置：

ShowDotFiles on

这样就能通过ls看见以"."号开头的文件

好好学习，天天吃饭

===

### 技巧六、proftpd如何实现磁盘限额

首先编译的时候指定--with-modules的时候要包含mod\_quota。

然后在配置文件中使用：

Quotas on

QuotaCalc on

DefaultQuota 8000

QuotaBlockSize 1024

QuotaBlockName kb

就可以实现磁盘限额。其中DefaultQuota说明用户只能用8000个block，而QuotaBlockSize则指明每个block大小是1024byte也就是1k。QuotaBlockName只在提示中出现，告诉用户block的单位。

===

技巧七、proftpd环境下如何将用户限制在自己的home目录下?

修改proftpd.conf，加入

DefaultRoot ~

(将用户限制在自己的目录下)

或者

DefaultRoot ~ group1, !group2,!group3

(将用户限制在自己的目录下，对group1有效，对group2,group3无效)

===

### 技巧八、如何让proftpd只监听在特定IP

如果一台机器有两个或者多个IP，比如192.168.0.1和172.16.0.1，那么缺省情况下ftp到这两个ip都可以连上这个ftp server，有些情况下要求只能ftp到192.168.0.1而不能ftp到172.16.0.1，该如何处理呢?

在proftpd.conf里面设置：

Bind 192.168.0.1

SocketBindTight on

但是这个配置只能在standalone模式下面才能生效。

===

### 技巧九、proftpd中MaxClients和MaxInstances有什么不同

为了有效利用系统资源，防止过多连接，有时候可以在proftpd.conf里面有这样的配置：

MaxClients 100

但是有时候却是看到这样的配置：

MaxInstances 100

这两个有什么区别呢?

MaxInstances设置的是proftpd产生的子进程的个数，而MaxClients限制的是登录用户的个数。而客户端只要产生一个连接，即使不登录，也会导致proftpd产生一个子进程。

如果配置文件中限制MaxClients 100的时候，第101个连上的用户会被提示允许连接的客户端个数已达上限，同时断开连接。而设置MaxInstances 100的时候，第101个连接的用户不会得到任何提示，而服务器拒绝接受任何连接。

====

### 技巧十、Proftpd如何限制某个用户的同时连接数

Proftpd 1.2.7rc1以后提供了一个新参数-MaxClientsPerUser。在配置文件中添加下列参数：

MaxClientsPerUser 5

这样就能限制每个用户只能同时有5个连接，使用例如flashget等下载工具的时候就最多只能分成5块下载。

===

### 技巧十一、如何不用kill proftpd的进程而停止ftp服务

ftpshut命令可以使得管理员不用停止proftpd进程而禁止所有连接，同时送出停止的信息。而且可以做到定时停止、允许当前存在的连接是马上中断还是到用户自己中断。

要重新提供ftp服务只要删除/etc/shutmsg。

===

### 技巧十二、如何查看当前连接到proftpd的用户

使用ftpwho命令，可以查看当前连接的用户相关信息，比如客户端机器名、用户名、连接时间、当前状态、进程号等。比使用ps命令来查看方便多了。

===

### 技巧十三、ftpshut

这个程序的主要功能是生成文件/etc/shutmsg，也就是我们在前面/etc/ftpaccess中设定的shutdown命令，ftpshut的使用格式如下：

ftp <-l min> <-d min> time <说明>

各个参数的说明如下：

-l 这个参数设定在关闭FTP服务器功能前多长时间停止用户的连接;

-d 这个参数设定在关闭FTP服务器功能前多长时间将用户断线;

Time 这个参数指定关闭FTP服务器功能的时间，如想

在8点半关闭机器，这里可以写0830。

===

### 技巧十四、Proftpd如何设置允许非正常shell的用户登录

有时候系统里面有一些只有ftp权限的用户，他们的shell一般被设置成/bin/false来防止他们用telnet登录到系统，但是这样导致他们不能ftp，如何解决呢?

需要注释掉/etc/pam.d/ftp，注释掉下面一行：

auth required /lib/security/pam\_shells.so

同时在proftpd.conf里面加入：

RequireValidShell off

===

### 技巧十五、Proftpd如何限速和设置发呆退出

可以使用:

RateReadBPS RateReadFreeBytes

RateWriteBPS RateWriteFreeBytes

来限制下载和上载速度：

RateReadBPS和RateWriteBPS限制下载和上载的速率

RateReadFreeBytes和RateWriteFreeBytes限制当用户现在这么多数据量以后再进行限速，这样可以实现对于小文件不限速，而大文件限速。

TimeoutIdle -- 设置空闲连接超时时钟

TimeoutLogin -- 设置空闲登陆超时时钟

TimeoutNoTransfer -- 设置当没有数据传输时的超时时钟

TimeoutStalled -- 设置被阻塞的下载的超时时钟

示例：

#############################################################################

ServerName "LittleBoy"

ServerType standalone

DefaultServer on

#隐藏服务器版本信息

ServerIdent off

#FTP使用的端口，21是默认

Port 21

###############################################################################

###################################################################################

RequireValidShell off

AuthPAM off

AuthPAMConfig ftp

###############################################################################

###############################################################################

#续传文件

AllowRetrieveRestart on

AllowStoreRestart on

#超时限制

TimeoutNoTransfer 600

TimeoutStalled 600

TimeoutIdle 1200

#设置最大尝试次数

#MaxLoginAttempts 3

#防止DoS攻击，设置最大子进程数为20.如果你要一次多于这个进程数，增加下面的值

#这个设置只有standalone 时有效，在inetd模式你应设置inetd服务器的每个服务数

#量进程数,例如xinetd

MaxInstances 20

###############################################################################

#掩码 Umask 022可以有效地防止文件被其他用户或同组用户改写

Umask 022

#磁盘配额

#Quotas on

#上传与下载比率

#Ratios on

###############################################################################

# Set the user and group under which the server will run.

User proftpd

Group proftpd

#禁止root登录

#RootLogin off

#DefaultRoot ~

#禁止系统普通用户登录

#<Limit LOGIN>

# DenyAll

#</Limit>

###############################################################################

###############################################################################

#启用日志

LogFormat auth "IP:%a Name:%u PASSWD:%A %r At:%t"

LogFormat readwrite "IP:%a Name:%u PASSWD:%A %m %F At:%t UsedTime:%T"

#以write的日志格式记录READ,WRITE的日志

ExtendedLog /var/log/proftpd/transfer.log WRITE,READ readwrite

#以auth的日志格式记录LOGIN的日志

ExtendedLog /var/log/proftpd/login.log AUTH auth

##根据自己的需要定制:

## %a:客户ip

## %A:匿名用户名

## %b:发送请求的字节数

## %d:目录名(相对路径)

## %D:目录名(绝对路径)

## %f:上传或下载的文件名(绝对路径)

## %F:上传或下载的文件名(相对路径)

## %h:客户的域名

## %L:本服务器ip

## %m:客户发送的命令

## %p:本服务器的端口

## %P:服务进程的id

## %r:客户发送的整条命令

## %t:本地时间

## %T:传送文件所用的时间(秒)

## %u:客户登陆的用户名

###############################################################################

###############################################################################

#一个基本的匿名帐号，带有上传目录

<Anonymous /home/ftp>

RequireValidShell no

User ftp

Group ftp

# 用 "anonymous" 代替 "proftpd" 登录

UserAlias anonymous ftp

AnonRequirePassword off

# Cosmetic changes, all files belongs to ftp user

DirFakeUser on ftp

DirFakeGroup on ftp

# 限制每个匿名帐号连接数

MaxClients 10 "最大连接10达到了，你等会再来"

MaxClientsPerHost 3 "对不起，一个IP只允许3个连接"

#下载与上传速率的设置，单位为KByte/s

TransferRate RETR 4000 user ftp

TransferRate STOR 2000 user ftp

#登录时的欢迎信息

DisplayLogin .welcome.msg

#对这个服务器的根目录下的所有的子目录限制写操作

<Limit WRITE>

DenyAll

</Limit>

#开匿名上传目录，只能上传而不能下载及修改原有文件

<Directory upload>

Umask 022 022

<Limit READ WRITE>

DenyAll

</Limit>

<Limit MKD STOR>

AllowAll

</Limit>

</Directory>

</Anonymous>

## 更多参考

1，配置指示列表: <http://www.proftpd.org/docs/directives/linked/by-name.html>

2，官方网址：<http://www.castaglia.org/proftpd/>

3，博客：<http://blog.csdn.net/neubuffer/article/details/16901151>