FTP—vsftpd 服务安装和配置

--------陈功磊 2009-6-1

http://chgl7.blog.51cto.com/

说明：系统镜像：[红帽企业.Linux.5].rhel-5.2-server-i386-dvd.iso

1、vsftpd 安装

```
[root@linux01 ~]# mkdir /media/cdrom
[root@linux01 ~]# mount -t iso9660 /dev/cdrom /media/cdrom   # 挂载镜像
mount: block device /dev/cdrom is write-protected, mounting read-only
[root@linux01 ~]# cd /media/cdrom/Server   # 进入软件包目录
[root@linux01 Server]#
[root@linux01 Server]# rpm -qa | grep ^vsftpd   # 查询相关已经安装的软件包
[root@linux01 Server]# ls | grep vsftpd*    # 查询当前路径下安装包
vsftpd-2.0.5-12.el5.i386.rpm
[root@linux01 Server]# rpm -ivh vsftpd-2.0.5-12.el5.i386.rpm   # 安装软件包 i 安装 v 输出详细信息 h 进度
warning: vsftpd-2.0.5-12.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID 37017186
Preparing...                ########################################### [100%]
   1:vsftpd                 ########################################### [100%]
 [root@linux01 Server]# rpm -qa | grep ^vsftpd   # 再次查询相关已经安装的软件包
vsftpd-2.0.5-12.el5
[root@linux01 Server]#cd
[root@linux01 ~]# rpm -ql vsftpd | grep etc    # 查询 etc 中与 vsftpd 相关的文件
/etc/logrotate.d/vsftpd.log
/etc/pam.d/vsftpd
/etc/rc.d/init.d/vsftpd
/etc/vsftpd
/etc/vsftpd/ftpusers
/etc/vsftpd/user_list
/etc/vsftpd/vsftpd.conf
/etc/vsftpd/vsftpd_conf_migrate.sh
[root@linux01 ~]#
```

2、、/etc/vsftpd/vsftpd.conf 文件配置

```
[root@linux01 Server]# cat /etc/vsftp/vsftpd.conf   # 读取原文，默认配置
cat: /etc/vsftp/vsftpd.conf: No such file or directory
[root@linux01 Server]# cat /etc/vsftpd/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
```

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES     # 允许匿名登录
#
# Uncomment this to allow local users to log in.
local_enable=YES       # 允许本地帐户登录
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES     # 开放对本地用户的写权限
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022       # 本地用户的文件生成掩码
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES       # 显示目录下的.message
#
# Activate logging of uploads/downloads.
xferlog_enable=YES       # 启用上传和下载日志
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES    # 启用 FTP 数据端口
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format
xferlog_std_format=YES     # 使用标准的 ftpd xferlog 日志格式
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
```

```
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
```

# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES　　# FTP 服务器处于独立启动模式（相对于受 xinnetd 管理的启动模式）
#
This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
sockets, you must run two copies of vsftpd whith two configuration files.
Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd　　# PAM 认证服务的配置文件名称，/etc/pam.d/vsftpd
userlist_enable=YES　　# FTP 将检查 userlist_file(/etc/vsftpd/user_list)中用户是否可以访问 FTP 服务器
tcp_wrappers=YES　# 使用 tcp_wrappers 作为主机访问控制方式，/etc/host.allow 和/etc/hosts.deny。
[root@linux01 Server]#

3、/etc/vsftpd.user_list 文件配置

[root@linux01 ~]# cd /etc/vsftpd
root@linux01 vsftpd]# ls
ftpusers　user_list　vsftpd.conf　vsftpd_conf_migrate.sh
[root@linux01 vsftpd]# cat user_list
vsftpd userlist
If userlist_deny=NO, only allow users in this file
If userlist_deny=YES (default), never allow users in this file, and
do not even prompt for a password.
Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
[root@linux01 vsftpd]#
(当 vsftp.conf 配置文件中包括以下配置时，user_list 中用户帐号禁止登录配置：
userlist_enable=YES　　# 注意大小写
userlist_deny=YES
当 vsftp.conf 配置文件中包括以下配置时，只有 user_list 中用户帐号允许登录配置：注意考虑 ftpusers 文件用户
userlist_enable=YES　　# 注意大小写
userlist_deny=NO

)

```
[root@linux01 vsftpd]# cat ftpusers
# Users that are not allowed to login via ftp
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
[root@linux01 vsftpd]#
```

4、匿名用户登录目录

匿名用户将进入/var/ftp 目录

5、vsftpd 服务启动与关闭

```
root@linux01 vsftpd]# ls -l /etc/init.d/vsftpd      # vsftpd 启动脚本文件
-rwxr-xr-x 1 root root 1778 Dec 13    2007 /etc/init.d/vsftpd
[root@linux01 vsftpd]#
[root@linux01 vsftpd]# chkconfig --list vsftpd    #  查看
vsftpd                  0:off      1:off      2:off      3:off      4:off      5:off      6:off
[root@linux01 vsftpd]# chkconfig --level 35 vsftpd on    #  设置在 35 模式下随机启动
[root@linux01 vsftpd]# chkconfig --list vsftpd    #  检查查看
vsftpd                  0:off      1:off      2:off      3:on       4:off      5:on       6:off
[root@linux01 vsftpd]#
[root@linux01 vsftpd]# service vsftpd start    #  启用服务
Starting vsftpd for vsftpd: [    OK    ]
[root@linux01 vsftpd]# service vsftpd stop    #  停止服务
Shutting down vsftpd: [    OK    ]
[root@linux01 vsftpd]# service vsftpd restart    #  重启服务
Shutting down vsftpd: [FAILED]
Starting vsftpd for vsftpd: [    OK    ]
[root@linux01 vsftpd]# service vsftpd status    #  查看服务状态
vsftpd (pid 13071) is running...
[root@linux01 vsftpd]#
```

6、测试帐号登录

```
[root@redhatCLI ~]# ftp 192.168.7.2
ftp: connect: No route to host      #  防火墙阻止登录
ftp>bye      #  退出 ftp
[root@linux01 vsftpd]# service iptables stop    #  在服务器上关闭防火墙，在客户端上也要关闭防火墙
Flushing firewall rules: [    OK    ]
Setting chains to policy ACCEPT: nat filter [    OK    ]
Unloading iptables modules: [    OK    ]
```

[root@linux01 vsftpd]#
匿名帐号登录（可以登录）
[root@redhatCLI ~]# ftp 192.168.7.2 #在客户端上登录ftp服务器
Connected to 192.168.7.2.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.7.2:root): anonymous # 使用匿名帐号登录
331 Please specify the password.
Password: # 密码为空
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
227 Entering Passive Mode (192,168,7,2,159,53)
150 Here comes the directory listing.
drwxr-xr-x 2 0 0 4096 Dec 13 2007 pub
226 Directory send OK.
ftp> pwd
257 "/"
ftp> bye
221 Goodbye.
[root@redhatCLI ~]#
服务器本地帐号登录（默认不能登录）
[root@redhatCLI ~]# ftp 192.168.7.2
Connected to 192.168.7.2.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.7.2:root): test01
331 Please specify the password.
Password:
500 OOPS: cannot change directory:/home/test01 # 其他帐号同样不能登录，与 user_list、vsftdpd.conf 等无关
Login failed.
ftp> bye
服务器本地帐号不能登录的修复处理
root@linux01 vsftpd]# setsebool ftpd_disable_trans 1 # 服务器本地帐号不能登录的修复处理，
                                                      # disable SELinux protection of the ftp daemon
                                                      # 有什么不会的后果就不知了。
[root@linux01 vsftpd]# service vsftpd restart # 重启服务
Shutting down vsftpd: [OK]
Starting vsftpd for vsftpd: [OK]
[root@linux01 vsftpd]#

[root@redhatCLI ~]# ftp 192.168.7.2 # 服务器本地帐号登录

```
Connected to 192.168.7.2.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.7.2:root): test01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
227 Entering Passive Mode (192,168,7,2,43,10)
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
257 "/home/test01"
ftp> cd /    # 进入根目录
250 Directory successfully changed.
ftp> pwd
257 "/"      # 不安全啊
ftp> cd /home    # 可以进入/home 目录
250 Directory successfully changed.
ftp> pwd
257 "/home
ftp> mkdir 123
550 Create directory operation failed.
ftp> bye
221 Goodbye.
[root@redhatCLI ~]#
```

7、禁锢登录用只在宿主目录中

```
[root@linux01 vsftpd]# vi vsftpd.conf

# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
                    ……..
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
chroot_local_user=YES    # 添加此行，来禁锢登录用只在宿主目录中
"vsftpd.conf" 117L, 4419C written
[root@linux01 vsftpd]# service vsftpd restart    # 重启服务
Shutting down vsftpd: [    OK    ]
```

Starting vsftpd for vsftpd: [OK]
[root@linux01 vsftpd]#
测试
[root@redhatCLI ~]# ftp 192.168.7.2
Connected to 192.168.7.2.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.7.2:root): test01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> cd /home # 不能使用 cd 进入非根目录了
550 Failed to change directory.
ftp> bye
221 Goodbye.
[root@redhatCLI ~]#

8、配置 FTP 服务器的虚拟用户（虚拟帐号对系统更安全）

（1）建立虚拟用户口令库文件
[root@linux01 ~]# touch /etc/vsftpd/logins.txt
[root@linux01 ~]# vi /etc/vsftpd/logins.txt

mike # 奇数行为用户名
pwabc # 偶数行为密码
john
pw1234
~
~
"/etc/vsftpd/logins.txt" 4L, 23C written
[root@linux01 ~]# cat /etc/vsftpd/logins.txt
mike
pwabc
john
pw1234
[root@linux01 ~]#
（2）生成 vsftpd 的认证文件
root@linux01 Server]# db # db + 两次空格键
dbconverter-2 dbus-cleanup-sockets dbus-launch dbus-send
dbus-binding-tool dbus-daemon dbus-monitor dbus-uuidgen
[root@linux01 Server] # 可以看出没有 db_load 命令，默认系统没有安装时，要手工安装了
[root@linux01 Server]# ls | grep ^db # 挂载好光驱后，进入到 rpm 包文件目录，查看 db 有关软件包

db4-4.3.29-9.fc6.i386.rpm
db4-devel-4.3.29-9.fc6.i386.rpm
db4-java-4.3.29-9.fc6.i386.rpm
db4-tcl-4.3.29-9.fc6.i386.rpm
db4-utils-4.3.29-9.fc6.i386.rpm
dbus-1.0.0-7.el5.i386.rpm
dbus-devel-1.0.0-7.el5.i386.rpm
dbus-glib-0.70-5.i386.rpm
dbus-glib-devel-0.70-5.i386.rpm
dbus-python-0.70-7.el5.i386.rpm
dbus-x11-1.0.0-7.el5.i386.rpm
[root@linux01 Server]#
[root@linux01 Server]# rpm -ivh db4-4.3.29-9.fc6.i386.rpm
[root@linux01 Server]# rpm -ivh db4-devel-4.3.29-9.fc6.i386.rpm
[root@linux01 Server]# rpm -ivh db4-java-4.3.29-9.fc6.i386.rpm
[root@linux01 Server]# rpm -ivh db4-tcl-4.3.29-9.fc6.i386.rpm
[root@linux01 Server]# rpm -ivh db4-utils-4.3.29-9.fc6.i386.rpm # 之后实验好像装他就可以了
[root@linux01 Server]# rpm -ivh dbus-1.0.0-7.el5.i386.rpm # 不知 db_load 是 db4 的哪个软件包，所以都安装了。
[root@linux01 Server]# db # db + 两次空格键。嗨，有了，出来了吧。
db_archive db_dump185 db_upgrade dbus-monitor
db_checkpoint db_load dbus-binding-tool dbus-send
dbconverter-2 db_printlog dbus-cleanup-sockets dbus-uuidgen
db_deadlock db_recover dbus-daemon db_verify
db_dump db_stat dbus-launch
[root@linux01 Server]# cd
root@linux01 ~]# db_load -T -t hash -f /etc/vsftpd/logins.txt /etc/vsftpd/vsftpd_login.db # 生成 vsftpd 的认证文件
[root@linux01 ~]# file /etc/vsftpd/vsftpd_login.db # 查看文件类型
/etc/vsftpd/vsftpd_login.db: Berkeley DB (Hash, version 8, native byte-order)
[root@linux01 ~]# chmod 600 /etc/vsftpd/vsftpd_login.db # 设置文件只对 root 读写
[root@linux01 ~]# ls -l /etc/vsftpd/vsftpd_login.db
-rw------- 1 root root 12288 Jun 1 20:30 /etc/vsftpd/vsftpd_login.db
[root@linux01 ~]#

（3）建立虚拟用户所需的 PAM 配置文件

[root@linux01 ~]# touch /etc/pam.d/vsftpd.vu # 新建文件
[root@linux01 ~]# vi /etc/pam.d/vsftpd.vu # 编辑

auth required /lib/security/pam_userdb.so db=/etc/vsftpd/vsftpd_login
account required /lib/security/pam_userdb.so db=/etc/vsftpd/vsftpd_login
~
~
"/etc/pam.d/vsftpd.vu" 2L, 141C written
[root@linux01 ~]# cat /etc/pam.d/vsftpd.vu # 查验
auth required /lib/security/pam_userdb.so db=/etc/vsftpd/vsftpd_login
account required /lib/security/pam_userdb.so db=/etc/vsftpd/vsftpd_login
[root@linux01 ~]#

（4）建立虚拟用户及要访问的目录并设置权限

[root@linux01 ~]# useradd -d /home/ftpsite virtual # 建立虚拟用户所需的目录及系统帐号
[root@linux01 ~]# chmod 700 /home/ftpsite/ # 设置宿主目录的权限
[root@linux01 ~]# ls -l /home/
total 16
drwx------ 3 virtual virtual 4096 Jun 1 20:39 ftpsite # 刚健的虚拟宿主目录，为所有虚拟用户使用
drwx------ 3 test01 test01 4096 Jun 1 18:58 test01 # 之前的本地用户 test01 宿主目录
[root@linux01 ~]#

（5）设置 vsftpd.conf 配置文件
[root@linux01 vsftpd]# cp vsftpd.conf vsftpd.conf_bake # 首先进入/etc/vsftpd 目录，然后备份，以防有问题
[root@linux01 vsftpd]# vi vsftpd.conf
Example config file /etc/vsftpd/vsftpd.conf
#
        ……..
guest_enable=YES # 添加的内容
guest_username=virtual # 添加的内容
pam_service_name=vsftpd.vu # 添加的内容
"vsftpd.conf" 120L, 4484C written
[root@linux01 vsftpd]#

（6）重启 vsftpd 服务
root@linux01 vsftpd]# service vsftpd restart
Shutting down vsftpd: [OK]
Starting vsftpd for vsftpd: [OK]
[root@linux01 vsftpd]#

（7）测试虚拟用户帐号 （注意：虚拟帐号和本地用户帐号默认不可同时生效）
root@linux01 vsftpd]# touch /home/ftpsite/afile # 建立也测试文件
[root@linux01 vsftpd]# chown virtual.virtual /home/ftpsite/afile # 赋予权限
[root@linux01 vsftpd]# ls -l /home/ftpsite
total 4
-rw-r--r-- 1 virtual virtual 0 Jun 1 20:53 afile
[root@linux01 vsftpd]#
[root@redhatCLI ~]# ftp 192.168.7.2
Connected to 192.168.7.2.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.7.2:root): mike
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
227 Entering Passive Mode (192,168,7,2,246,249)

150 Here comes the directory listing.
226 Transfer done (but failed to open directory).
ftp>bye

9、典型 FTP 服务器设置

```
[root@linux01 Server]# cat /etc/vsftpd/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
anonymous_enable=YES     # 允许匿名登录
local_enable=YES      # 允许本地帐户登录
.
write_enable=YES     # 开放对本地用户的写权限
local_umask=022      # 本地用户的文件生成掩码
#anon_upload_enable=YES   # 匿名用户是否可以上传文件默认注释掉了
#anon_mkdir_write_enable=YES   # 匿名用户是否创建目录，默认注释掉了
dirmessage_enable=YES      # 显示目录下的.message
xferlog_enable=YES      # 启用上传和下载日志
connect_from_port_20=YES   # 启用 FTP 数据端口
#chown_uploads=YES
#chown_username=whoever
#xferlog_file=/var/log/vsftpd.log
xferlog_std_format=YES     # 使用标准的 ftpd xferlog 日志格式
#idle_session_timeout=600
#data_connection_timeout=120
#nopriv_user=ftpsecure
#async_abor_enable=YES
#ascii_upload_enable=YES
#ascii_download_enable=YES
#deny_email_enable=YES
#banned_email_file=/etc/vsftpd/banned_emails
#chroot_list_enable=YES
#chroot_list_file=/etc/vsftpd/chroot_list
#ls_recurse_enable=YES
listen=YES     # FTP 服务器处于独立启动模式（相对于受 xinnetd 管理的启动模式）
#listen_ipv6=YES

pam_service_name=vsftpd     # PAM 认证服务的配置文件名称，/etc/pam.d/vsftpd
userlist_enable=YES     # FTP 将检查 userlist_file(/etc/vsftpd/user_list)中用户是否可以访问 FTP 服务器
tcp_wrappers=YES   # 使用 tcp_wrappers 作为主机访问控制方式，/etc/host.allow 和/etc/hosts.deny。
chroot_list_enable=YES   # 禁锢用户在宿主目录中
max_clients=100   # 限制客户端的最大连接数
max_per_ip=5   # 同一 ip 与 FTP 服务器连接的最大连接数
local_max_rate=500000   # 本地用户传输最大为 500KB/s
anon_max_rate=200000     # 匿名用户传输最大为 200KB/s
[root@linux01 Server]#
```

ftp 密码用户登录方式

ftp://username:password@host:port 可以以 username 为用户名,password 为密码从端口 port 登录到 host