文件服务器之三：FTP服务器简介

FTP（File Transfer Protocol）：文件传输协议

工作流程：FTP传输使用的TCP数据包协议，FTP服务器使用两个连接（命令通道、数据通道）。首先客户端随机取一个大于1024的端口与FTP服务器端的21端口连接，通过这个连接来对FTP服务器执行命令。通知FTP服务器端使用active且告知连接的端口号。FTP服务器主动向客户端连接。由20端口向客户端的端口号连接。（数据传输通道是在有数据传输行为时才会建立的通道，并不是一开始连接到FTP服务器就立刻建立的通道）

FTP有两种模式：主动模式和被动模式。

一. 主动模式：客户端端口N（>1024）---->服务器端21　服务器端（20）---->客户端（N+1）

a. 问题：服务器主动连接到NAT等待转递至客户端的连接问题。FTP服务器只能知道NAT的IP而不是客户端的IP，所以FTP服务器会以port20主动向NAT的端口发送主动连接的要求，但是NAT没有启动端口接收FTP的port20。在FTP的主动式连接当中，NAT将会被视为客户端，但不是真正的客户端。

- 解决方法1、使用iptabls提供的FTP检测模块。使用modprobe加载ip_conntrack_ftp和ip_nat_ftp等模块。模块主动分析目标是port21的连接信息，所以可以得到服务器端port20要连接的端口。接收到服务器端的主动连接，就可以将该数据包引向正确的后端主机
- 解决方法2、客户端选择被动式（Passive）连接模式，客户端发起连接

二. 被动模式：客户端端口N（>1024）---->服务器端21　客户端（N+1）---->服务器端（P）

不论哪种模式，都是由客户端决定的。通常情况下，如果客户端只有内网IP，建议使用被动模式，一般来说，我们使用FTP，都会选择被动模式。而且大部分的ftp软件默认也是被动模式。

FTP服务器软件vsftpd

vsftpd（very secure ftp daemon）非常安全的ftp的deamon，特点就是安全。FTP通过tcp来实现，目前它并不支持udp。它的deamon监听两个端口，一个是用来传输数据的20端口，一个是用来传递信令的端口21。因为工作模式的不同，传输数据的接口并不是一定是20，也可能是一个随机的端口。

服务器配置

```
[root@test ~]# yum install vsftpd -y
[root@test ~]# yum install ftp -y
[root@test ~]# vim /etc/sysconfig/selinux
[root@test ~]# systemctl stop firewalld
[root@test ~]# systemctl disable firewalld
[root@test ~]# systemctl mask firewalld
[root@test ~]# systemctl start vsftpd
[root@test ~]# systemctl enable vsftpd

[root@test ~]# cd /var/ftp # vsftpd默认匿名用户登录的根目录。
```

实例一、主动模式连接（不推荐）anonymous

```
[root@test vsftpd]# cat /etc/vsftpd/ftpusers  # 查看文件内容，取消禁止root用户登录ftp服务器
[root@test vsftpd]# cp /etc/vsftpd/vsftpd.conf  /etc/vsftpd/vsftpd.conf.bak # 修改配置文件之前，先备份配置文件
[root@test ~]# vim /etc/vsftpd/vsftpd.conf
anonymous_enable=YES # 允许匿名用户登录ftp服务器
local_enable=YES     # 允许本地用户登录ftp服务器
write_enable=YES     #允许写
local_umask=022      # 文件权限过滤符
anon_upload_enable=YES # 允许匿名用户的上传
anon_mkdir_write_enable=YES # 允许匿名用户的创建文件夹
dirmessage_enable=YES
xferlog_enable=YES # 日志
connect_from_port_20=YES # 开启主动连接
xferlog_file=/var/log/xferlog # 日志的地址
xferlog_std_format=YES #日志的格式
ascii_upload_enable=YES  # 以ascii形式上传数据
ascii_download_enable=YES #
ftpd_banner=Welcome to monoid's ftp server.
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

注意：

```
[root@RHEL6 vsftpd]# ftp localhost
Trying ::1...
ftp: connect to address ::1拒绝连接
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220-hello
220
Name (localhost:root): root
331 Please specify the password.
Password:
500 OOPS: cannot change directory:/root
Login failed.
```

这是因为SELinux的问题。默认情况下SELinux不允许实体账号登录取得用户主目录数据的

```
[root@RHEL6 vsftpd]# getsebool -a |grep ftp
allow_ftpd_anon_write --> off
allow_ftpd_full_access --> off
allow_ftpd_use_cifs --> off
allow_ftpd_use_nfs --> off
ftp_home_dir --> off      将这个改为on[root@RHEL6 vsftpd]# setsebool -P ftp_home_dir=1
ftpd_connect_db --> off
httpd_enable_ftp_server --> off
sftpd_anon_write --> off
sftpd_enable_homedirs --> off
sftpd_full_access --> off
sftpd_write_ssh_home --> off
tftp_anon_write --> off

[root@test vsftpd]# chmod 777 /var/ftp/ # 设置匿名用户根目录的权限
```

实例二、对用户（包括未来新建用户）进行chroot。默认让实体用户全部被chroot

```
[root@test vsftpd]# vim vsftpd.conf
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
```

```
xferlog_enable=YES
connect_from_port_20=YES
xferlog_file=/var/log/xferlog
xferlog_std_format=YES
idle_session_timeout=600
data_connection_timeout=120
ascii_upload_enable=YES
ascii_download_enable=YES
ftpd_banner=Welcome to blah FTP service.
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES # 千万别忘记这个参数
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
# 手动生成chroot_list，/etc/vsftpd/chroot_list中的用户没有被chroot
```

实例三、对用户上传的文件chown。

实例四、建立严格的可使用FTP的账号列表

```
userlist_enable=YES
userlist_deny=NO
# 如果userlist_deny=NO，只允许出现在本文件中的用户登录ftp服务器
# 如果userlist_deny=YES ，不允许出现在本文件中的用户登录ftp服务器
userlist_file=/etc/vsftpd/user_list
```

实例四、匿名登录的相关设置

```
[root@RHEL6 vsftpd]# vim vsftpd.conf
anonymous_enable=YES
local_enable=NO
no_anon_password=YES
anon_max_rate=1000000
data_connection_timeout=60
idle_session_timeout=60
max_clients=50
max_per_ip=5
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
listen=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
use_localtime=YES
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
write_enable=YES
anon_other_write_enable=YES
anon_mkdir_write_enable=YES
anon_upload_enable=YES
```

首先文件权限的问题，匿名用户的身份是ftp，如果想上传数据，必须将uploads的所有者等进行修改chown ftp uploads/

再修改SELinux的内容

```
1、[root@RHEL6 ftp]# setsebool -P allow_ftpd_anon_write=1
2、[root@RHEL6 ftp]# setsebool -P allow_ftpd_full_access=1
```

实例五、让匿名用户具有上传权限，没有下载匿名用户上传的东西的权限

```
[root@RHEL6 vsftpd]# vim vsftpd.conf
anonymous_enable=YES
local_enable=NO
no_anon_password=YES
anon_max_rate=1000000
data_connection_timeout=60
idle_session_timeout=60
max_clients=50
max_per_ip=5
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
listen=YES
```

```
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
use_localtime=YES
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
write_enable=YES
anon_mkdir_write_enable=YES
anon_upload_enable=YES
chown_uploads=YES
chown_username=daemon
[root@RHEL6 vsftpd]# ftp localhost
Trying ::1...
ftp: connect to address ::1拒绝连接
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:root): anonymous
500 OOPS: vsftpd: refusing to run with writable anonymous root
这个原因产生是因为，权限设置不对。 chown  root /vat/ftp    chmod  /var/ftp/uploads/ 777
```

实例六、加入/var/log/messages的支持

在配置文件中加入

```
dual_log_enable=YES
vsftpd_log_file=/var/log/vsftp.log

#一般服务器系统设置的项目
max_clients=50
max_per_ip=5
use_localtime=YES
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=YES
pam_service_name=vsftpd
tcp_wrappers=YES
banner_file=/etc/vsftpd/welcome.txt
dual_log_enable=YES
vsftpd_log_file=/var/log/vsftpd.log
pasv_min_port=65400
pasv_max_port=65410
```

实例七、被动式连接端口的限制

被动式数据连接，服务器随机取没有使用的端口建立被动式连接，我们可以指定固定范围内的端口作为FTP的被动式数据连接之用。防火墙设置：加入iptabls的ip_nat_ftp和ip_conntrack_ftp模块。虽然我们加入了模块，但是我们要修改系统文件

```
[root@test vsftpd]# iptables -A INPUT -p TCP -i eth0 --dport 21 --sport 1024:65534 -j ACCEPT
[root@test vsftpd]# iptables -A INPUT -p TCP -i eth0 --dport 65400:65410 --sport 1024:65534 -j ACCEPT

[root@test vsftpd]# vim vsftpd.conf
pasv_enable=YES支持数据流的被动式连接模式
pasv_min_port=10000
pasv_max_port=12000
[root@test ~]# vim /etc/vsftpd/ftpusers
[root@test ~]# vim /etc/vsftpd/user_list
```

https://www.cnblogs.com/helonghl/articles/5533857.html

史上最详细的vsftpd配置文件讲解