

项目 6 配置与管理 FTP 服务器-实训任务指导书 (6-2)

任务 2 配置本地模式的常规 FTP 服务器案例

公司内部现在有一台 FTP 服务器和 Web 服务器，FTP 主要用于维护公司的网站内容，包括上传文件、创建目录、更新网页等。为了方便实现对网站的维护公司，将 FTP 服务器和 Web 服务器做在一起。现有两个部门负责维护任务，两者分别适用 team1 和 team2 账号进行管理。先要求仅允许 team1 和 team2 账号登录 FTP 服务器，但不能登录本地系统，并将除这两个账号之外账号的根目录限制为/web/www/html，其他账号不能进入该目录以外的任何目录。为了增强安全性，首先需要使用仅允许本地用户访问，并禁止匿名用户登录。

项目准备：

需要两台虚拟机，一台作为 FTP 服务器 主机名 server7-1，IP 地址为 192.168.1.2/24；FTP 客户端，主机名 client7-2，IP 地址为 192.168.1.3/24，DNS 为 192.168.1.2；Windows 客户端：Windows 7 IP 地址为 192.168.1.30，直接在网卡 VMnet 上设置 IP 地址为：192.168.1.30/24。

具体实训步骤

一、分别在 FTP 服务器 server7-1 上和 FTP 客户端 client7-2 上安装 FTP 软件包。

1. 打开 FTP 服务器主机修改为 server7-1，安装 vsftpd 服务。（网络 NAT 模式下，可选用 ens33 连接）

```
[root@server7-1]# yum clean all //安装前先清除缓存
```

```
[root@server7-1]# yum install vsftpd -y
```

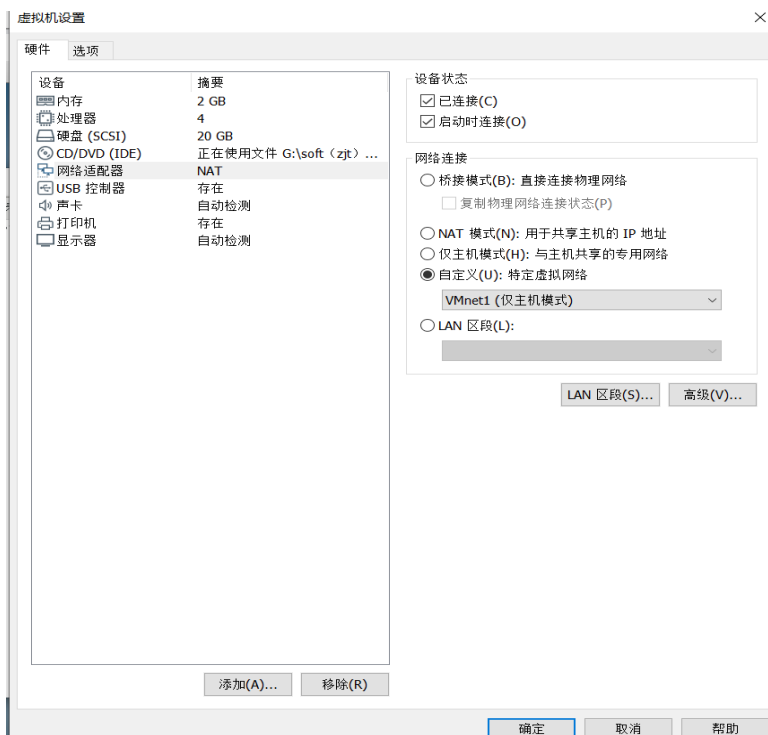
```
[root@server7-1]# rpm -qa |grep vsftpd //检查安装组件是否成功
```

2. 打开 FTP 客户端主机主机名修改为 client7-2，安装 ftp 服务。（网络 NAT 模式下，可选用 ens33 连接）

```
[root@client7-2]# yum clean all //安装前先清除缓存
```

```
[root@client7-2]# yum install ftp -y //同时安装 ftp 软件包
```

3. 软件包安装完成后，分别进行网络配置，FTP 服务器 server7-1，IP 地址设为 192.168.1.2/24 ，默认网关 192.168.1.1；FTP 客户端 client7-2，IP 地址为 192.168.1.3/24，默认网关 192.168.1.1，DNS 为 192.168.1.2，两台主机网络设置模式均修改设置为自定义 VMnet1 仅主机模式，实现网络互联。



二、在 FTP 服务器主机 server7-1 上，启动 vsftpd 服务启动，并设置开机自动加载。

```
[root@ server7-1]# systemctl start vsftpd
```

```
[root@ server7-1]# systemctl enable vsftpd
```

三、建立维护网站内容的 FTP 账号 team1 、 team2 和 user1 并禁止本地登录，然后为其设置密码。

```
[root@server7-1]# useradd -s /sbin/nologin team1
```

```
[root@server7-1]# useradd -s /sbin/nologin team2
```

```
[root@server7-1]# useradd -s /sbin/nologin user1
```

```
[root@server7-1]# passwd team1
```

```
[root@server7-1]# passwd team2
```

```
[root@server7-1]# passwd user1
```

四、配置 vsftpd.conf 主配置文件并做相应修改。（写入配置文件时，注释一定去掉，语句前后不要加空格，切记！另外，可以把任务 1 的配置文件恢复到最初状态，以免实训间互相影响。）

```
[root@server7-1]# vim /etc/vsftpd/vsftpd.conf
```

```
anonymous_enable=NO #禁止匿名用户登录（12行）
```

```
local_enable=YES #允许本地用户登录（16行）
```

```
local_root=/web/www/html #设置本地用户的根目录为/web/www/html（添加）
```

```
chroot_local_user= YES #是否限制本地用户，这也是默认值，可以省略（101行）
```

```
chroot_list_enable=YES #激活 chroot 功能（102行）
```

```
chroot_list_file=/etc/vsftpd/chroot_list #设置锁定用户在根目录中的列表文件（104行）
```

allow_writeable_chroot=YES #只要启用 chroot 就一定加入这条：允许 chroot 限制！！

否则出现连接错误。切记。（添加）

实现锁定目录有**两种**实现方法。

第一种是除列表内的用户外，其他用户都被限定在固定目录内。即列表内用户自由，列表外用户受限制。（这时启用 chroot_local_user=YES）**为了安全，建议使用第一种。**

chroot_local_user=YES

chroot_list_enable=YES

chroot_list_file=/etc/vsftpd/chroot_list

allow_writeable_chroot=YES

第二种是除列表内的用户外，其他用户都可自由转换目录。即列表内用户受限制，列表外用户自由（这时启用 chroot_local_user=NO）。

chroot_local_user=NO

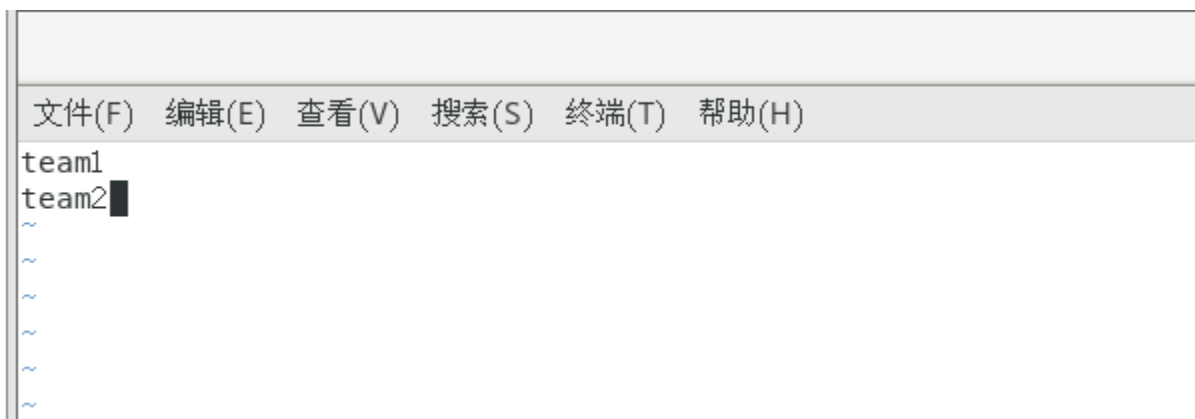
chroot_list_enable=YES

chroot_list_file=/etc/vsftpd/chroot_list

allow_writeable_chroot=YES

五、建立/etc/vsftpd/chroot_list 文件，添加 team1 和 team2 账号。

```
[root@server7-1]# vim /etc/vsftpd/chroot_list
```



```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
team1
team2
~
~
~
~
~
~
```

六、防火墙放行和 SELinux 允许，重启 FTP 服务。（若防火墙已配置可省略）

```
[root@server7-1]# firewall-cmd --permanent --add-service=ftp
```

```
[root@server7-1]# firewall-cmd --reload
```

```
[root@server7-1]# firewall-cmd --list-all
```

```
[root@server7-1]# setenforce 0
```

```
[root@server7-1]# systemctl restart vsftpd
```

七、修改本地权限，其他用户可以写入。

```
[root@server7-1]# mkdir /web/www/html -p
```

```
[root@server7-1]# cd /web/www/html
```

```
[root@server7-1]# touch /web/www/html/test.txt
```

```
[root@server7-1]# touch /web/www/html/sample.txt
```

```
[root@server7-1]# ll -d /web/www/html
```

```
[root@server7-1]# chmod -R o+w /web/www/html //其他用户可以写入!
```

```
[root@server7-1]# ll -d /web/www/html
```

八、在 FTP 客户端主机 client7-2 使用 ftp 命令，进行登录验证。

①如果出现以下错误，请在 FTP 服务器主机 server7-1 按一下操作修改/etc/shells 文件。

服务器中 useradd -s /sbin/nologin xxx 创建用户后客户端发现竟然不能登录，报 530 错误
检查本地配置没有问题，使用正常用户也可以登录。

```
[root@localhost ~]# ftp 192.168.203.102
Connected to 192.168.203.102 (192.168.203.102).
220 (vsFTPd 3.0.2)
Name (192.168.203.102:root): ftp
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
```

因：vsftpd 默认会检查用户的 shell，如果用户的 shell 在/etc/shells 没有记录，则无法登陆 ftp

解决办法：在/etc/shells 文件里面添加用户的 shell 解释器

```
[root@localhost ftp]# vim /etc/shells
```

```
/bin/sh
/bin/bash
/usr/bin/sh
/usr/bin/bash
/bin/tcsh
/bin/csh
/sbin/nologin
~
~
```

解释：/etc/shells 文件的作用

1.系统某些服务在运行过程中，回去检查用户使用的 shells，而这些 shell 查询就是借助/etc/shells 这个文件。

2.修改该文件不会影响用户登陆服务器主机的权限，该文件提供给解释器给系统的某些服务判断一个用户是否是有效用户，例如我创建的 ftp 用户解释器为/sbin/nologin，我系统的/etc/shells 文件里面没有添加/sbin/nologin，所以我创建的 ftp 用户登陆不了 ftp 服务，后面将/sbin/nologin 添加进/etc/shells 文件，则问题解决。

```
[root@server7-1]vim /etc/shells
```

```
/bin/sh
/bin/bash
/usr/bin/sh
/usr/bin/bash
/bin/tcsh
/bin/csh
/sbin/nologin
~
test
```

保存退出。

②在 FTP 客户端主机 client7-2 使用 ftp 命令，进行登录验证。

●在 client7-2 客户机上，使用 team1 和 team2 用户能转换目录，也能建立新文件夹，可以将/etc/passwd 文件下载到主目录。（显示的目录是“/”，其实是/web/www/html 文件夹）

```
[root@client7-2]# ftp 192.168.1.2
Connected to 192.168.1.2 (192.168.1.2).
220 (vsFTPd 3.0.2)
Name (192.168.1.2:root): team1 //锁定用户测试
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" //显示是“/”，其实是/web/www/html，从列示的文件中就知道。
ftp> mkdir testteam1
257 "/testteam1" created
ftp> ls
227 Entering Passive Mode (192,168,1,2,46,226).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 0 Jul 21 01:25 test.sample
drwxr-xr-x 2 1001 1001 6 Jul 21 01:48 testteam1
226 Directory send OK.
ftp> cd /etc
250 Directory successfully changed. //允许更改目录
ftp> get passwd //成功下载密码文件 passwd 到/root，可以退出后查看
local: passwd remote: passwd
227 Entering Passive Mode (192,168,1,2,91,43).
150 Opening BINARY mode data connection for passwd (2491 bytes).
```

```
226 Transfer complete.
2491 bytes received in 4.8e-05 secs (51895.83 Kbytes/sec)
ftp> cd /web/www/html
250 Directory successfully changed.
ftp> ls -la
227 Entering Passive Mode (192,168,1,2,105,26).
150 Here comes the directory listing.
drwxr-xrwx   4 0       0           40 May 04 14:29 .
drwxr-xr-x   3 0       0           18 May 04 13:57 ..
drwxr-xr-x   2 1001    1001          6 May 04 14:24 testteam1
drwxr-xr-x   2 1003    1003          6 May 04 14:29 testuser1
226 Directory send OK.
ftp> exit
221 Goodbye.
```

●在 client7-2 客户机上，使用 user1 用户能转换目录，也能建立新文件夹，不可以将/etc/passwd 文件下载到主目录。

```
[root@client7-2]# ftp 192.168.1.2
Connected to 192.168.1.2 (192.168.1.2).
220 (vsFTPd 3.0.2)
Name (192.168.1.2:root): user1           //列表外的用户是自由的
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/web/www/html"
ftp> mkdir testuser1
257 "/web/www/html/testuser1" created
ftp> cd /etc           //不能转换到/etc 目录
550 Failed to change directory.
```