项目 6 配置与管理 FTP 服务器-实训任务指导书（6-3）

企业级 FTP 服务器虚拟账号设置与应用：

FTP 若采用本地用户登录，会直接将本地用户暴露在互联网中，如果没有相关的安全设置，FTP 用户会便用该用户去登陆你的计算机，其次如果有大量的本地用户，FTP 管理员还需要创建大量的本地用户，本地用户越多就越不利于管理，又给安全带来很大的挑战。基于安全因素，引入虚拟帐户代替本地实名用户登录 FTP 服务器，并实现分级管理。虚拟用户就是没有实际的系统上的用户存在，创建虚拟用户 jianan1 和 jianan2，并分别设置密码，虚拟目录及用户配置文件，通过映射到一个真实的用户上，设置相应的权限来实现验证。

vsftpd 虚拟用户企业案例配置步骤如下：

一、安装 Vsftpd 软件包以及虚拟用户需用到的软件及认证模块：

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

[root@server7-1] yum install pam* libdb-utils libdb* -y

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

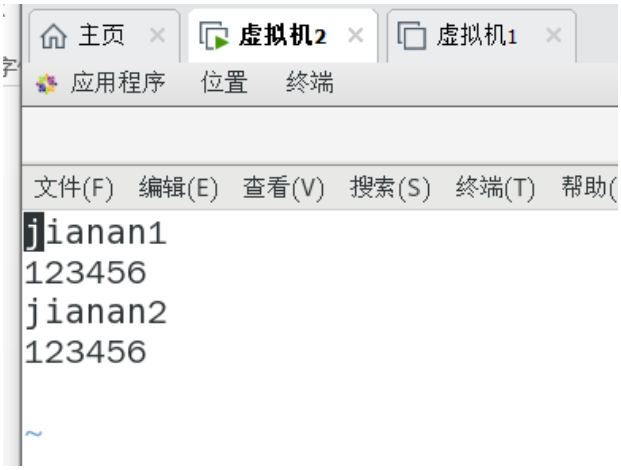
```
[root@server7-1 ~]# systemctl start vsftpd
[root@server7-1 ~]# systemctl enable vsftpd
Created symlink from /etc/systemd/system/multi-user.target.wants/v
sftpd.service to /usr/lib/systemd/system/vsftpd.service.
```

三、创建用户数据库

（1）创建用户文本文件。

使用 vim 编辑器创建虚拟用户临时文件 vim /etc/vsftpd/ftpusers.txt，添加虚拟账号 jianan1，jianan2，两个虚拟用户。新建虚拟用户和密码，如下所示。

[root@server7-1]# vim /etc/vsftpd/ftpusers.txt



保存退出

（2）生成 Vsftpd 虚拟用户数据库认证文件

[root@server7-1]# db_load -T -t hash -f /etc/vsftpd/ftpusers.txt

/etc/vsftpd/vsftpd_login.db

db_load 命令的作用是将用户信息文件转换为数据库并使用 hash 加密，如果需要保存虚拟帐号和密码的文本文件且不让被系统帐号直接调用，我们就需要使用 db_load 命令生成 db 数据库。

-T 选项-T 允许应用程序能够将文本文件转译载入进数据库。 由于我们之后是将虚拟用户的信息以文件方式存储在文件里的，为了让 Vsftpd 这个应用程序能够通过文本来载入用户数据，必须要使用这个选项。如果指定了选项-T，那么一定要追跟子选项-t

-t 子选项-t， 追加在在-T 选项后，用来指定转译载入的数据库类型 。扩展介绍下，-t 可以指定的数据类型有 Btree、Hash、Queue 和 Recon 数据库。

-f 参数后面接 包含用户名和密码的文本文件 ，文件的内容是： 奇数行用户名、偶数行密码

（3）修改数据库文件访问权限，设置其权限为 700。

[root@server7-1]# chmod 700 /etc/vsftpd/vsftpd_login.db

[root@server7-1]# ll　　/etc/vsftpd

```
[root@192 jianan1]# ls -l /etc/vsftpd
总用量 32
-rw-------. 1 root root   125 6月   10 2021 ftpusers
-rw-r--r--. 1 root root    31 5月   14 17:49 ftpusers.txt
-rw-------. 1 root root   361 6月   10 2021 user_list
-rw-------. 1 root root   362 5月   14 18:09 vsftpd.conf
-rwxr--r--. 1 root root   338 6月   10 2021 vsftpd_conf_migrate.sh
-rwx------. 1 root root 12288 5月   14 17:52 vsftpd_login.db
drwxr-xr-x. 2 root root    21 5月   14 18:16 vsftpd_user_conf
```

四．配置 PAM 认证文件，/etc/pam.d/vsftpd 行首加入如下两行

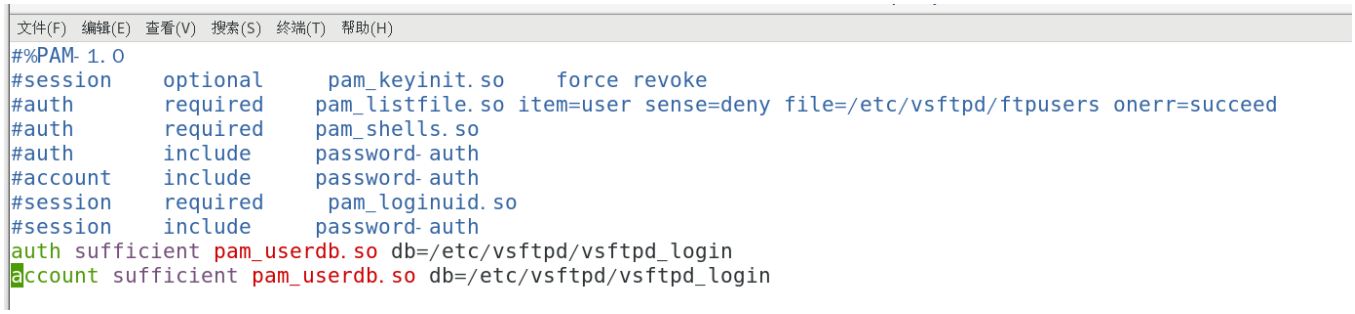
PAM（Pluggable Authentication Modules ）是由 Sun 提出的一种认证机制。它通过提供一些动态链接库和一套统一的 API，将系统提供的服务和该服务的认证方式分开，使得系统管理员可以灵活地根据需要给不同的服务配置不同的认证方式而无需更改服务程序，同时也便于向系统中添加新的认证手段。在执行前首先要对启动它的用户进行认证，符合一定的要求之后才允许执行，例如 login，su 等。在 Linux 中进行身份或是状态的验证程序是由 PAM 来进行的，PAM（Pluggable Authentication Modules）可动态加载验证模块，因为可以按需要动态的对验证的内容进行变更，所以可以大大提高验证的灵活性。

[root@server7-1]# vim　　/etc/pam.d/vsftpd

```
#PAM-1.0
#session    optional     pam_keyinit.so    force    revoke
#auth    required    pam_listfile.so      item=user    sense=deny
#file=/etc/vsftpd/ftpusers onerr=succeed
#auth    required    pam_shells.so
auth     sufficient  pam_userdb.so      db=/etc/vsftpd/vsftpd_login
```

account sufficient pam_userdb.so db=/etc/vsftpd/vsftpd_login

如下图：



保存退出

五．创建虚拟账户对应系统用户

所有的 Vsftpd 虚拟用户需要映射到一个系统用户，该系统用户不需要密码，也不需要登录，主要用于虚拟用户映射使用，创建命令如下：

创建一个不需要进行登录的用户 vftpuser

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

六、修改 vsftpd 配置文件内容如下： /etc/vsftpd/vsftpd.conf

[root@server7-1]# truncate -s 0 /etc/vsftpd/vsftpd.conf

[root@server7-1]# vim /etc/vsftpd/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_std_format=YES

listen=NO

listen_ipv6=YES

pam_service_name=vsftpd

userlist_enable=YES

tcp_wrappers=YES

guest_enable=YES

guest_username=ftpuser

user_config_dir=/etc/vsftpd/vsftpd_user_conf

virtual_use_local_privs=YES
```

特别注意设置以下参数的含义

```
pam_service_name=vsftpd        虚拟用户启用pam认证;
guest_enable=YES           启用虚拟用户;
guest_username=ftpuser         映射虚拟用户至系统用户ftpuser;
user_config_dir=/etc/vsftpd/vsftpd_user_conf      设置虚拟用户配置文件所在目录;
virtual_use_local_privs=YES 虚拟用户使用本地用户相同的权限;
```

可以巧用 grep -v “#” vsftpd.conf 进行编辑。

七、创建虚拟用户配置文件主目录和虚拟用户各自的配置文件

到目前为止所有虚拟用户共同基于/home/ftpuser 主目录实现文件的上传与下载，可以在/etc/vsftpd/vsftpd_user_conf 目录创建虚拟用户各自的配置文件，创建虚拟用户配置文件主目录。

（1）创建虚拟用户配置文件主目录

[root@ server7-1] # mkdir -p /etc/vsftpd/vsftpd_user_conf/

（2）可分别为 jianan1 和 jianan2 两个虚拟用户创建虚拟目录下的配置文件：（以 jianan1 为例）

vim /etc/vsftpd/vsftpd_user_conf/jianan1

```
local_root=/home/ftpuser/jianan1
write_enable=YES
anon_world_readable_only=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES
anon_other_write_enable=YES
```

```
1 local_root=/home/ftpuser/jianan1     jianan1虚拟用户配置文件路径;
2 write_enable=YES      允许登录用户有写权限;
3 anon_world_readable_only=YES      允许匿名用户下载，然后读取文件;
4 anon_upload_enable=YES   允许上传文件，只有在write_enable=YES是生效;
5 anon_mkdir_write_enable=YES 允许匿名用户创建目录，同上生效;
  anon_other_write_enable=YES 允许匿名用户其他权限，删除、重命名等。
```

八. 创建虚拟用户各自虚拟目录：（以 jianan1 为例）

[root@ server7-1] # mkdir -p /home/ftpuser/jianan1

[root@ server7-1] # chown -R ftpuser:ftpuser /home/ftpuser

最后重启 Vsftpd 服务

[root@server7-1] #systemctl restart vsftpd

九、配置服务器的防火墙策略，添加允许 FTP 服务，并永久生效，并设置 selinux 为允许。

（1）.配置服务器的防火墙策略，添加允许 FTP 服务，并永久生效

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

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

```
[root@server7-1 ~]# firewall-cmd --permanent --add-service=ftp
success
[root@server7-1 ~]# firewall-cmd --reload
success
[root@server7-1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ftp ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

（2）.查看防火墙配置,开启防火墙中的匿名上传服务

通过 getsebool -a | grep ftp 我们可以看到 selinux 是禁止了所有的 ftp 服务，

需要开启防火墙中的匿名上传服务。

```
[root@server7-1 ~]# getsebool -a|grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@server7-1 ~]# setsebool  ftpd_anon_write  on
[root@server7-1 ~]# getsebool -a|grep ftp
ftpd_anon_write --> on
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@server7-1 ~]# getenforce
Enforcing
[root@server7-1 ~]# setenforce  0
[root@server7-1 ~]# getenforce
Permissive
[root@server7-1 ~]#
```

设置 FTP 服务完全访问为允许

[root@ server7-1]# setsebool -P ftpd_ full_access=on

（3）.防火墙配置完成，需要重启 vsftpd 服务

[root@server7-1] #systemctl restart vsftpd

十、测试：使用虚拟账号 jianan1 登录 FTP 服务器，进行测试，会发现虚拟账号登录成功，并显示 FTP 服务器目录信息。

（1）.先在 jianan1 目录中创建三个文件

[root@server7-1] # cd /home/ftpuser

[root@server7-1] # ll

总用量 0

drwxr-xr-x. 2 ftpuser ftpuser 6 5 月 14 18:18 jianan1

[root@server7-1] #cd jianan1

[root@server7-1] #touch {1..3}.txt

[root@server7-1] #ls

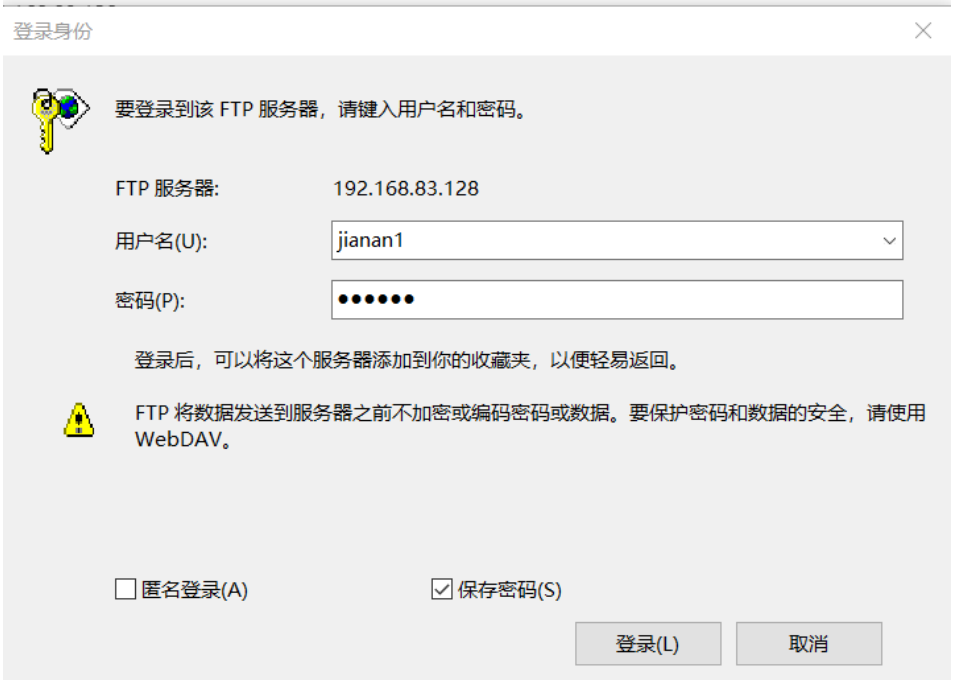
1.txt 2.txt 3.txt

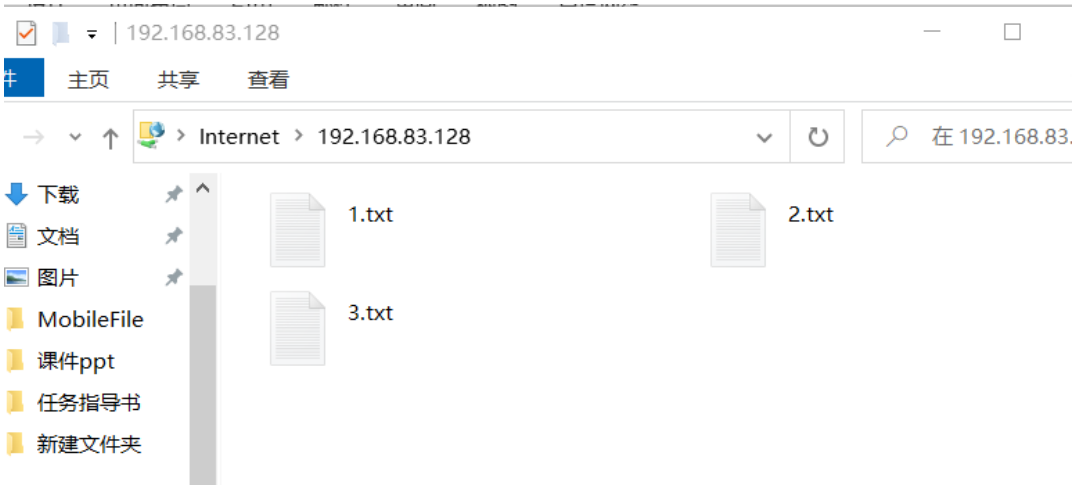
[root@server7-1] # ifconfig

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.83.128  netmask 255.255.255.0  broadcast
192.168.83.255
        inet6 fe80::b9bc:46be:e31d:dd38  prefixlen 64  scopeid 0x20<link>
```

```
        ether 00:0c:29:0f:dc:75  txqueuelen 1000  (Ethernet)
        RX packets 59027  bytes 82574997 (78.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24599  bytes 1632572 (1.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

（2）. Window 中登录测试，Window 中打开我的电脑,输入：ftp://192.168.83.128，右键选“登录”，输入虚拟用户名 jianan1，密码：123456，显示如下。





补充知识：服务器端 vsftp 的主被动模式配置

（1）主动模式配置 Port_enable=YES 开启主动模式

Connect_from_port_20=YES 当主动模式开启的时候，是否启用默认的 20 端口监听

Ftp_date_port=%portnumber% 上一选项使用 NO 参数时指定数据传输端口

（2）被动模式配置 connect_from_port_20=NO

PASV_enable=YES 开启被动模式

PASV_min_port=%number% 被动模式最低端口

PASV_max_port=%number% 被动模式最高端口