Redhat FTP vsftpd Configuration

Default filetransfer daemon is vsftpd.

VSFTP Configuration for specific application accounts

This configuration allows to configure specific accounts having read-write or readonly access.

Configuration vsftpd /etc/vsftpd/vsftpd.conf

This configuration needs specific parameter. Observe the following parmeters: guest_enable, guest_username, pam_service_name, user_config_dir, userlist_enable. There is a specific guest account to be configured and specific application accounts using pam (pam_service_name) and a user configuration is a specific directory (user_config_dir).

```
[root@vaix1d ~]# grep -v "#" /etc/vsftpd/vsftpd.conf  | sort | grep -v "^$"
allow_writeable_chroot=YES
anon_other_write_enable=YES
anon_umask=022
anon_upload_enable=YES
anon_world_readable_only=YES
anonymous_enable=NO
chroot_local_user=YES
connect_from_port_20=YES
dirmessage_enable=YES
dual_log_enable=YES
ftpd_banner=Welcome to AixBOMS FTP service
guest_enable=YES
guest_username=virtual
listen_ipv6=NO
listen_port=21
listen=YES
local_enable=YES
local_umask=022
pam_service_name=vsftpd
syslog_enable=YES
tcp_wrappers=YES
use_localtime=YES
user_config_dir=/etc/vsftpd_user_conf
userlist_enable=YES
vsftpd_log_file=/var/log/vsftpd.log
write_enable=YES
xferlog_enable=YES
xferlog_file=/var/log/xferlog
```

```
xferlog_std_format=NO
[root@vaix1d ~]#
```

PAM vsftpd Settings

in the PAM configuration there is a specific username-password module configured /etc/vsftpd_login, which ist processed by the PAM module

```
[root@vaix1d ~]# cat /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 required /lib64/security/pam_userdb.so db=/etc/vsftpd_login
account required /lib64/security/pam_userdb.so db=/etc/vsftpd_login

#auth       include     password-auth
#account    include     password-auth
#session    required     pam_loginuid.so
#session    include     password-auth
[root@vaix1d ~]#
```

Specific User Configuration Hash /etc/vsftpd_login

The following accounts to be configured, are treated as guest user accounts. There is a user and password database configured. The original file is situated unter the root account as hidden file

```
[root@vaix1d ~]# cat vsftpd_config/.users.txt
user1
passwd1
user2
passwd2
```

Now this user account file gets compiled as hash to be processed by the PAM module. Of course, each time a user account changes, the hash needs to be recompiled.

```
# db_load -T -t hash -f /root/vsftpd_config/.users.txt /etc/vsftpd_login.db
```

User Access Configuration

All user access configuration data is configured under the directory /etc/vsftpd_user_conf, as defined in /etc/vsftpd/vsftpd.conf in parameter “user_config_dir”. For each user Account there is a specific file with the access rights specified.

```
[root@vaix1d ~]# ls -l /etc/vsftpd_user_conf/
total 40
-rw-r--r--. 1 root root 54 Mar 23 11:34 user1
-rw-r--r--. 1 root root 54 Mar 23 11:34 user2
[root@vaix1d ~]# cat /etc/vsftpd_user_conf/user1
local_root=/data/datatransfer/user1
write_enable=YES
[root@vaix1d ~]# cat /etc/vsftpd_user_conf/user2
local_root=/data/datatransfer/user2
write_enable=NO
[root@vaix1d ~]#
```

Configuration Account Directories

The account directories of course need to exist and need to have the guest user protection.

```
[root@vaix1d ~]# ll /data/datatransfer
total 0
drwxr-xr-x. 2 virtual users 6 Mar 23 11:34 user1
drwxr-xr-x. 2 virtual users 6 Mar 23 11:34 user2
[root@vaix1d ~]#
```

SELinux settings when using vsftpd with guest accounts

The following SELinux booleans need to be configured permanently

```
[root@vaix1d ~]# getsebool -a | grep ftp | grep on$
ftpd_anon_write --> on
ftpd_connect_all_unreserved --> on
ftpd_full_access --> on
ftpd_use_passive_mode --> on
[root@vaix1d ~]#
```

FTP Access test

On the ftp server a file gest placed in the account directory. Then the ftp server gets accessed using ftp. When listing the directory one can see the previously placed file. This is the prove that the jailing of the account is working.

```
[root@vaix1d ~]# cd /data/datatransfer/user2/
[root@vaix1d user2]# touch file_in_user2
```

On the client side access file transfer using ftp. Above account user2 is configured as readonly (write_enable=NO), so ftp put is not permitted.

```
[root@vaix2d ~]# ftp vaix1d
Connected to vaix1d (172.18.9.22).
220 Welcome to AixBOMS FTP service
Name (vaix1d:root): user2
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (172,18,9,22,231,117).
150 Here comes the directory listing.
-rw-r--r--    1 0        0               0 Mar 23 11:04 file_in_user2
226 Directory send OK.
ftp> pwd
257 "/"
ftp> put ks-post.log
local: ks-post.log remote: ks-post.log
227 Entering Passive Mode (172,18,9,22,228,215).
550 Permission denied.
ftp> quit
221 Goodbye.
[root@vaix2d ~]#
```

VSFTP Settings when used with NFS and Firewall

FTP transfer behind firewall requires all connects being opened from ftp client side only. In fact, when the ftp clients first request a session from the ftp server, ftp server communicates a data transfer port to the ftp client. ftp client then sends / gets the data over this special port, which is different to the ftp port 21/tcp. This procedure has consequences to SELinux configuration

SELinux Booleans needed

when having FTP Accounts on NFS and making transfer over firewall one needs the following SElinux boolean to be enabled:

```
[root@vkrpe1 ~]# getsebool -a | grep ^ftp | grep " on"
ftpd_connect_all_unreserved --> on
ftpd_full_access --> on
ftpd_use_nfs --> on
ftpd_use_passive_mode --> on
[root@vkrpe1 ~]#
```

SELinux booleans explained

Redhat SELinux policy has two booleans which control opening ports from FTP server: ftpd_connect_all_unreserved and ftpd_use_passive_mode

```
       If you want to determine whether ftpd can  connect  to  all
unreserved
       ports,  you  must turn on the ftpd_connect_all_unreserved boolean.
Dis&#8208;
       abled by default.

       setsebool -P ftpd_connect_all_unreserved 1


       If  you want to determine whether ftpd can bind to all unreserved
ports
       for passive mode, you must turn on the  ftpd_use_passive_mode
boolean.
       Disabled by default.

       setsebool -P ftpd_use_passive_mode 1
```

SELinux ftp defined ports

```
[root@v000u5 ~]# semanage port --list | grep ftp
ftp_data_port_t                tcp      20
ftp_port_t                     tcp      21, 989, 990
ftp_port_t                     udp      989, 990
tftp_port_t                    udp      69
[root@v000u5 ~]#
```

VSFTP Settings

The following VSFTP settings are configured for specific user accounts working with group write access

---

User Account with GID privileges

```
[rebermi@vkrpe1 ~]$ grep sappkr11 /etc/passwd
sappkr11:x:1011:900:SAP Transfer User Upload:/pkr1/appl/sap/sapin:/bin/false
[freyu@vkrpe1 ~]$ grep 900 /etc/group
spoadm:x:900:sbwaage,oracle
[rebermi@vkrpe1 ~]$
```

HOME Directory with GID write Access

Observe the rws in the gid field below. This GID bit “s” configures the group write access to be inherited on all data in this directory

```
[rebermi@vkrpe1 ~]$ ls -lsa /pkr1/appl/sap | grep sapin
  12 drwxrwsr--.  4 spo spoadm   12288 Sep 12 07:32 sapin
[rebermi@vkrpe1 ~]$
```

VSFTPD Configuration

In the VSFTPD configuration umask needs to be set to group write access 00n. Observe the local_umask setting below. As one can also see below, ftp-data port 20 is enabled. This requires SELinux boolean ftpd_connect_all_unreserved –> on to be enabled. PASV method gets enabled by default: pasv_enable: Default: YES / Set to NO if you want to disallow the PASV method of obtaining a data connection.

```
[root@vkrpe1 ~]# grep -v "#" /etc/vsftpd/vsftpd.conf | grep -v ^$
use_localtime=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=007
dirmessage_enable=YES
```

```
xferlog_enable=YES
connect_from_port_20=YES
xferlog_file=/var/log/xferlog
xferlog_std_format=YES
chroot_local_user=YES
allow_writeable_chroot=YES
listen=YES
listen_ipv6=NO
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
[root@vkrpe1 ~]#
```

Last update: **2019/03/11 14:52**