Dernière mise-à-jour : 2020/01/30 03:27

Topic 212 - Sécuriser un Serveur FTP (2/60)

Weight: 2

Description: Candidates should be able to configure an FTP server for anonymous downloads and uploads. This objective includes precautions to be taken if anonymous uploads are permitted and configuring user access.

Key Knowledge Areas:

- Configuration files, tools and utilities for Pure-FTPd and vsftpd
- Awareness of ProFTPd
- Understanding of passive vs. active FTP connections

Terms and Utilities:

- vsftpd.conf
- important Pure-FTPd command line options

Le Serveur FTP

Installation

Le paquet **vsftpd** *Very Secure FTP daemon* se trouve dans les dépôts CentOS.

```
[root@centos6 ~]# yum install vsftpd
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
```

```
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package vsftpd.i686 0:2.2.2-6.el6_2.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                                Arch                                Version
Repository                               Size
================================================================================
================================================================================
Installing:
 vsftpd                                 i686                                2.2.2-6.el6_2.1
updates                                155 k

Transaction Summary
================================================================================
================================================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 155 k
Installed size: 343 k
Is this ok [y/N]: y
Downloading Packages:
vsftpd-2.2.2-6.el6_2.1.i686.rpm
| 155 kB     00:00
Running rpm_check_debug
Running Transaction Test
```

```
Transaction Test Succeeded
Running Transaction
  Installing     : vsftpd-2.2.2-6.el6_2.1.i686
1/1

Installed:
  vsftpd.i686 0:2.2.2-6.el6_2.1

Complete!
```

Par contre le service vsftpd n'est pas démarré par défaut :

```
[root@centos6 ~]# chkconfig --list vsftpd
vsftpd          0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
```

Configurez le service **vsftpd** pour que celui-ci soit activé correctement pour les niveaux d'exécution 3, 4 et 5 :

```
[root@centos6 ~]# chkconfig --level 345 vsftpd on
[root@centos6 ~]# chkconfig --list vsftpd
vsftpd          0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
```

Avant de poursuivre, modifiez le mode de **SELinux** de **enforced** à **permissive** pour la session en cours :

```
[root@centos6 ~]# setenforce permissive
[root@centos6 ~]# getenforce
Permissive
```

Ensuite éditez le fichier **/etc/selinux/config** ainsi :

config.selinux

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
```

```
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Configuration de base

Le fichier de configuration de vsftpd est **/etc/vsftpd/vsftpd.conf** :

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
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
```

```
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# 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
#
# 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
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# 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.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
# 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_local_user=YES
#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
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
```

```
tcp_wrappers=YES
```

Les directives actives de ce fichier sont :

vsftpd.conf.bare

```
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=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

Ces directives sont détaillées ci-après :

Directive	**Valeur par Défaut**	**Description**
anonymous_enable	YES	Si oui, autorise les connexions anonymes
local_enable	YES	Si oui, autorise des connexions par des utilisateurs ayant un compte valide sur le système
write_enable	YES	Si oui, permet l'écriture
local_umask	022	Spécifie la valeur de l'umask lors de la création de fichiers et de répertoires
dirmessage_enable	NO	Si oui, permet d'afficher le contenu du fichier .message quand un utilisateur rentre dans le répertoire
xferlog_enable	NO	Si oui, permet d'activer la journalisation dans le fichier **/var/log/vsftpd.log**
connect_from_port_20	NO	Permet les connexions de ftp-data
listen	NO	Si oui, vfsftpd fonctionne en mode Standalone et non en tant que sous-service de xinetd

Directive	Valeur par Défaut	Description
pam_service_name	S/O	Indique le nom du service PAM utilisé par vsftpd
userlist_enable	NO	Si oui, vsftpd charge une liste d'utilisateurs spécifiés dans le fichier identifié par la directive **userlist_file**. Si un utilisateur spécifié dans la liste essaie de se connecter, la connexion sera réfusée avant la demande d'un mot de passe
tcp_wrappers	NO	Si oui, vsftpd utilise TCP WRAPPERS

/etc/ftpusers

Votre serveur FTP est maintenant configuré pour les connexions en provenance des utilisateurs ayant un compte sur votre système.

Dans le cas où vous souhaiteriez **interdire** la connexion vers le serveur de certaines personnes mais pas de toutes les personnes ayant un compte système, éditez le fichier **/etc/ftpusers**.

Voici la liste des utilisateurs système qu'il convient d'ajouter à ce fichier:

ftpusers

```
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
uucp
operator
gopher
nobody
dbus
vcsa
```

```
rpc
nscd
tcpdump
haldaemon
apache
nslcd
postfix
avahi
ntp
rpcuser
sshd
gdm
vboxadd
named
```

Il est ensuite nécessaire d'inclure une directive supplémentaire dans le fichier /etc/vsftpd/vsftpd.conf :

```
...
userlist_file=/etc/ftpusers
...
```

et de démarrer le serveur :

```
[root@centos6 ~]# service vsftpd start
Démarrage de vsftpd pour vsftpd :                          [  OK  ]
```

Testez maintenant le serveur :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): trainee
331 Please specify the password.
```

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/trainee"
ftp>
```

Bien que trainee puisse se connecter, ce n'est pas le cas pour **root** :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): root
530 Permission denied.
Login failed.
```

Pour **chrooter** l'utilisateur dans son répertoire personnel, il convient d'ajouter la directive suivante au fichier /etc/vsftpd/vsftpd.conf :

```
...
chroot_local_user=YES
...
```

et de redémarrer le serveur :

```
[root@centos6 ~]# service vsftpd restart
Arrêt de vsftpd :                                          [  OK  ]
Démarrage de vsftpd pour vsftpd :                          [  OK  ]
```

Lors de sa prochaine connexion, l'utilisateur voit son répertoire personnel comme la racine du système de fichiers :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
```

```
Name (localhost:trainee): trainee
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp>
```

Serveur vsftpd Anonyme

Configuration

Le serveur anonyme étant déjà configuré par la présence de la directive **anonymous_enable=YES**, il convient de tester celui-ci :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> ls
227 Entering Passive Mode (127,0,0,1,143,6).
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jan 03 01:21 pub
226 Directory send OK.
```

```
ftp> quit
221 Goodbye.
```

Le répertoire pour les connexions anonymes est **/var/ftp** :

```
[root@centos6 ~]# ls -l /var | grep ftp
drwxr-xr-x.  3 root root  4096 31 mai   15:12 ftp
```

Par défaut il contient un répertoire **pub** :

```
[root@centos6 ~]# ls -l /var/ftp
total 4
drwxr-xr-x. 2 root root 4096  3 janv. 02:21 pub
```

Pour permettre aux utilisateurs anonymes de transférer des fichiers vers le serveur, il faut d'abord créer un répertoire **upload** dans **/var/ftp/pub** et de l'affecter à ftp:ftp :

```
[root@centos6 ~]# mkdir /var/ftp/pub/upload
[root@centos6 ~]# chown ftp:ftp /var/ftp/pub/upload
```

Ensuite il faut ajouter la directive suivante au fichier **/etc/vsftpd/vsftpd.conf** :

```
...
anon_upload_enable=YES
...
```

Votre fichier de configuration ressemblera donc à :

vsftpd.conf.anon

```
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=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
userlist_file=/etc/ftpusers
anon_upload_enable=YES
chroot_local_user=YES
```

Testez ensuite votre configuration :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): anonymous
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 (127,0,0,1,70,196).
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 May 31 14:03 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> cd upload
250 Directory successfully changed.
```

```
ftp> put rndc.key
local: rndc.key remote: rndc.key
227 Entering Passive Mode (127,0,0,1,238,121).
150 Ok to send data.
226 Transfer complete.
77 bytes sent in 0,0349 secs (2,21 Kbytes/sec)
ftp> ls
227 Entering Passive Mode (127,0,0,1,230,251).
150 Here comes the directory listing.
-rw-------    1 14       50             77 May 31 14:09 rndc.key
226 Directory send OK.
```

Serveur vsftpd et Utilisateurs Virtuels

Introduction

Le serveur vsftpd utilise le système PAM pour gérer les authentifications. Le module concerné est **pam_userdb**. Ce module consulte une base de données au format Berkeley pour obtenir les coordonnées de connexion des utilisateurs.

Configuration

Pour configurer des utilisateurs virtuels, il convient de créer un fichier de configuration à part, **/root/vftpusers** , dans lequel on inscrit le nom et le mot de passe des utilisateurs virtuels :

vftpusers

```
alexandre
123456789
```

Ce fichier doit ensuite être converti au format Berkeley :

```
[root@centos6 ~]# db_load -T -t hash -f /root/vftpusers /etc/vsftpd/vftpusers.db
```

Modifiez ensuite les permissions sur le fichier **/etc/vsftpd/vftpusers.db** et supprimez le fichier **/root/vftpusers** :

```
[root@centos6 ~]# chmod 600 /etc/vsftpd/vftpusers.db
[root@centos6 ~]# rm -f /root/vftpusers
```

Créez ensuite un fichier PAM **/etc/pam.d/vftpusers** :

vftpusers

```
#%PAM-1.0
auth    required    pam_userdb.so    db=/etc/vsftpd/vftpusers
account required    pam_userdb.so    db=/etc/vsftpd/vftpusers
session required    pam_loginuid.so
```

Notez que **pam_userdb.so** ajoute automatiquement l'extension **.db** aux noms des fichiers de base de données.

Modifiez maintenant le fichier /etc/vsftpd/vsftpd.conf :

```
...
pam_service_name=vftpusers
guest_enable=YES
guest_username=ftp
virtual_use_local_privs=YES
...
```

Votre fichier de configuration ressemblera à :

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=YES
pam_service_name=vftpusers
guest_enable=YES
guest_username=ftp
virtual_use_local_privs=YES
userlist_enable=YES
tcp_wrappers=YES
userlist_file=/etc/ftpusers
anon_upload_enable=YES
chroot_local_user=YES
```

Redémarrez le service vsftpd :

```
[root@centos6 ~]# service vsftpd restart
Arrêt de vsftpd :                                          [  OK  ]
Démarrage de vsftpd pour vsftpd :                          [  OK  ]
```

Testez ensuite la configuration :

```
[root@centos6 log]# ftp localhost
Connected to localhost (127.0.0.1).
```

```
220 (vsFTPd 2.2.2)
Name (localhost:trainee): alexandre
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> ls
227 Entering Passive Mode (127,0,0,1,214,118).
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 May 31 14:03 pub
226 Directory send OK.
```

Notez que les utilisateurs virtuels atterrissent dans le répertoire personnel du compte indiqué par la directive **guest_username** du fichier **/etc/vsftpd/vsftpd.conf**.

LAB #1

A Faire - Configurez votre serveur ftp anonyme et un utilisateur virtuel.
