

VsFTPd

Ce tutoriel développe la mise en place d'un serveur vsFTPd, qui acceptera les connexions FTP anonymes (lecture uniquement des données) et les connexions FTP over SSL ([FTPS](#)) pour les utilisateurs authentifiés (lecture, écriture) auprès d'un annuaire LDAP.

Un montage NFS sera utilisé pour que les utilisateurs authentifiés accèdent à leur home directory.

Installation des packages

Sur ftp.alex.dmz :

```
vsftpd openssl libnss-ldap libpam-ldap nscd nfs-common
```

Modifiez le fichier `/etc/network/interfaces` :

```
# The loopback network interface
auto lo eth0 eth1
iface lo inet loopback

# The primary network interface
allow-hotplug eth0 eth1
iface eth0 inet static
address 123.45.67.6
netmask 255.255.255.240
gateway 123.45.67.14

iface eth1 inet static
address 172.16.0.3
netmask 255.255.255.0
up route add -net 172.17.0.0/16 gw 172.16.0.254
up route add -net 172.18.0.0/16 gw 172.16.0.254
```

Modifiez le fichier `/etc/hosts` :

```
127.0.0.1    localhost
123.45.67.6  ftp.alex.fr
172.16.0.3   ftp.alex.dmz  ntp.alex.dmz  ftp  ntp
```

Modifiez le fichier `/etc/resolv.conf` :

```
search alex.dmz alex.lan srl.alex.lan
nameserver 172.16.0.1
nameserver 172.17.0.1
```

Schéma ftp pour OpenLDAP

Voici le schéma "[proxy-ftp.schema](#)" qui contient un attribut nommé "FTPAccountActive" afin d'autoriser les utilisateurs à accéder au service FTP.

J'ai utilisé le préfixe OID LDAP "entreprise" (1.3.6.1.4.1) avec un numéro libre non attribué, voir [IANA](#) (99999).

Mon schéma contient deux objectclass et deux attributs puisque j'ai réuni les informations pour l'authentification au proxy. Les informations qui nous intéressent pour FTP sont les suivantes :

- FTPAccount (*pour un compte utilisateur*)
 - FTPAccountActive (*si le compte est actif ou pas*)

Configuration de la partie cliente LDAP

Copiez depuis le serveur ldap2.alex.dmz le certificat du serveur ldap1 et ldap2, après avoir créé le répertoire /etc/ldap/tls :

```
ftp:~# mkdir /etc/ldap/tls
ftp:~# scp
root@172.16.0.20:/etc/ldap/tls/ldap_ldap*_cert.pem /etc/ldap/tls/
```

Modifiez le fichier /etc/ldap/ldap.conf :

```
TLS_CACERTDIR /etc/ldap/tls
TLS_REQCERT allow

BASE dc=meta
URI ldaps://ldap2.alex.dmz ldaps://ldap1.alex.dmz
```

Modifiez le fichier /etc/libnss-ldap.conf :

```
base dc=meta

uri ldaps://ldap2.alex.dmz ldaps://ldap1.alex.dmz

ldap_version 3

scope sub

timelimit 30

bind_timelimit 30
```

```
bind_policy soft

pam_filter objectclass=posixaccount

pam_login_attribute uid

# Nous filtrons uniquement les utilisateurs qui disposent de l'attribut
# FTPAccountActive=yes :
nss_base_passwd      dc=meta?sub?FTPAccountActive=yes
nss_base_group       dc=meta?sub

ssl on
```

Faites un lien symbolique de /etc/libnss-ldap.conf vers /etc/pam_ldap.conf :

```
ftp:~# ln -sf /etc/libnss-ldap.conf /etc/pam_ldap.conf
```

Modifiez le fichier /etc/pam.d/vsftpd :

```
# Standard behaviour for ftpd(8).
authrequired      pam_listfile.so item=user sense=deny
file=/etc/ftpusers onerr=succeed

# Note: vsftpd handles anonymous logins on its own.  Do not enable
# pam_ftp.so.

# Standard blurb.
#@include common-account
#@include common-session
#@include common-auth

account required  pam_unix.so
account sufficient pam_ldap.so

session required  pam_limits.so
session required  pam_unix.so
session optional  pam_ldap.so

auth required     pam_env.so
auth sufficient    pam_unix.so nullok_secure
auth sufficient    pam_ldap.so use_first_pass

authrequired      pam_shells.so
```

Modifiez le fichier /etc/nsswitch.conf :

```
passwd:      compat ldap
```

```
group:      compat ldap
shadow:     compat ldap

hosts:      files dns
networks:   files

protocols:  db files
services:   db files
ethers:     db files
rpc:        db files

netgroup:   nis
```

Lancez la commande "id *un_compte_ldap*" pour vérifier la liaison avec l'annuaire.

Configuration de vsFTPD

Modifiez le fichier /etc/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.
#

# Pour que vsFTPD soit lancé en tant que démon (IPv4).
listen=YES
# Ou en Ipv6.
#listen_ipv6=YES

# Adresse d'écoute, sinon toutes les interfaces sont écoutées.
#listen_address=123.45.67.6

# Port d'écoute.
listen_port=21

# Pour emprisonner le démon vsftpd.
secure_chroot_dir=/var/run/vsftpd

# Utilisateur pour les opérations sans privilèges.
nopriv_user=nobody

# Pour s'assurer que les données FTP (ftp-data) partent du port 20.
connect_from_port_20=YES

# Ne pas activer cette option pour des raisons de sécurité.
#async_abor_enable=YES

# Ne pas activer ces options pour des raisons de sécurité.
```

```
#ascii_upload_enable=YES
#ascii_download_enable=YES

# Active le mode FTP passif.
pasv_enable=YES

# Définition de la plage de ports à utiliser pour les connexions FTP
# passives.
pasv_min_port=40000
pasv_max_port=40200

# Combien de clients peuvent être connectés au maximum.
max_clients=200

# Le nombre maximum de clients connectés depuis la même adresse IP
source.
max_per_ip=4

# Désactive le listage récursif des répertoires par la commande "ls -R",
# afin d'éviter trop d'appels sur le système de fichier.
# Certain clients FTP comme "ncftp" ou "mirror" réclame l'option "-R"
# pour fonctionner.
ls_recurse_enable=NO

# Force l'affichage des données cachées, commençant par un "."
force_dot_files=YES

# Commandes autorisées. Voir la liste des commandes.
#cmds_allowed=PASV,RETR,QUIT

# Données refusées.
#deny_file={*.mp3,*.mov,.private}

# Données qui seront cachées.
#hide_file={*.mp3,.hidden,hide*,h?}
hide_file={Maildir,.spamassassin}

# Bannière affichée au login des clients.
ftpd_banner>Welcome to Alex FTP service.

# Supprime l'affichage de message pour certain répertoire.
dirmessage_enable=NO

# Autorise les connexions FTP anonymes.
anonymous_enable=YES

# Refuse les connexions SSL pour les clients anonymes.
allow_anon_ssl=NO

# Ne demande pas de mot de passe aux clients anonymes.
no_anon_password=YES
```

```
# Vous pouvez lister les adresses mail à refuser pour les clients
# anonymes. Utile pour combattre certaines attaques DoS.
#deny_email_enable=YES
#banned_email_file=/etc/vsftpd.banned_emails

# Indique dans quel répertoire seront dirigés les clients anonymes.
anon_root=/home/ftp

# Tous les paramètres commençant par "anon_", concernent les connexions
# anonymes. Si vous souhaitez autoriser l'upload et d'autres opérations
# d'écriture, vous devez activer l'option write_enable.
#
# Refuser l'upload.
anon_upload_enable=NO

# Refuse la création de répertoire.
anon_mkdir_write_enable=NO

# Refuse les opérations d'écriture.
anon_other_write_enable=NO

# Pour que les clients anonymes voient uniquement les données
# lisibles par tout le monde.
anon_world_readable_only=YES

# Pour limiter le taux de transfert (montant/descendant) des clients
# anonymes en Octets par seconde.
anon_max_rate=260

# Autorise les utilisateurs "locaux" à se connecter (authentifiés via
PAM)
local_enable=YES

# Nom du service PAM à utiliser pour l'authentification.
pam_service_name=vsftpd

# Active le module SSL.
ssl_enable=YES

# Emplacement du certificat RSA à utiliser pour les connexions SSL.
rsa_cert_file=/etc/vsftpd-ssl/vsftpd.pem

# Autorise les protocoles suivants :
ssl_tlsv1=YES
ssl_sslv3=YES

# Refuse le protocole suivant :
ssl_sslv2=NO

# Force les transactions d'authentification non anonymes via SSL.
```

```
force_local_logins_ssl=YES

# Force le transfert des données via SSL.
force_local_data_ssl=YES

# Pour refuser certain utilisateurs d'après une liste contenue dans un
# fichier.
#userlist_enable=YES
#userlist_deny=YES
#userlist_file=/etc/vsftpd.user_list

# Pour restreindre les utilisateurs locaux dans leur home directories.
chroot_local_user=YES

# Vous pouvez spécifier une liste d'utilisateurs à chrooter si vous
# n'activez pas le paramètre "chroot_local_user".
# Par contre, si vous l'activez, cette liste contiendra les utilisateurs
# à ne pas chrooter.
#chroot_list_enable=YES
#chroot_list_file=/etc/vsftpd.chroot_list

# Autorise les opérations d'écriture.
write_enable=YES

# Je considère que les utilisateurs locaux ont un accès FTP pour gérer
# les données de leur site Web. De ce fait, j'applique un masque sur les
# données pour que Apache puisse les lire et écrire. Je refuse
# l'utilisation de la commande FTP "chmod".
#
# Masque appliqué par défaut.
#local_umask=022
local_umask=007
#
# Désactive la commande FTP "chmod".
chmod_enable=NO

# Pour afficher "ftp" comme propriétaire et groupe.
hide_ids=YES

# Pour limiter le taux de transfert (montant/descendant) des utilisateurs
# locaux en Octets par seconde.
local_max_rate=1100

# Active les logs pour les transferts montant/descendant.
xferlog_enable=YES

# Pour obtenir les logs FTP au format standard xferlog.
xferlog_std_format=YES

# Fichier de log par défaut.
#xferlog_file=/var/log/vsftpd.log
```

```
# Timeout d'une session.
idle_session_timeout=600

# Timeout pour l'échange de données.
data_connection_timeout=120
```

Création du certificat SSL

Créez un répertoire /etc/vsftpd-ssl qui contiendra le certificat SSL.
Pour générer le certificat SSL :

```
ftp:~# cd /etc/vsftpd-ssl

ftp:/etc/vsftpd-ssl# openssl req -x509 -nodes -days 3650 -newkey rsa:1024
-keyout vsftpd.pem -out vsftpd.pem

Generating a 1024 bit RSA private key
.....++++++
.++++++
writing new private key to 'vsftpd.pem'
-----

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Haute-Savoie
Locality Name (eg, city) []:Alex
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Alex
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:ftp.alex.fr
Email Address []:root@alex.fr
ftp:/etc/vsftpd-ssl#
```

Changez les droits sur le certificat :

```
ftp:/etc/vsftpd-ssl# chmod 600 vsftpd.pem
```

Configuration du partage NFS sur le serveur nas

Ajoutez dans le fichier /export/etc/exports :

```
/export 172.16.0.3(rw, sync, fsid=0, acl, no_subtree_check, no_root_squash)
172.16.0.8(rw, sync, fsid=0, acl, no_subtree_check, root_squash)
172.16.0.13(rw, sync, fsid=0, acl, no_subtree_check, no_root_squash)
172.16.0.14(rw, sync, fsid=0, acl, no_subtree_check, no_root_squash)
172.16.0.15(rw, sync, fsid=0, acl, no_subtree_check, no_root_squash)
```

Relancez le partage NFS :

```
nas1:~# exportfs -r

nas1:~# exportfs -v
/export
172.16.0.3(rw, wdelay, no_root_squash, no_subtree_check, fsid=0, anonuid=65534,
anongid=65534)
/export
172.16.0.8(rw, wdelay, root_squash, no_subtree_check, fsid=0, anonuid=65534, ano
ngid=65534)
/export
172.16.0.13(rw, wdelay, no_root_squash, no_subtree_check, fsid=0, anonuid=65534
, anongid=65534)
/export
172.16.0.14(rw, wdelay, no_root_squash, no_subtree_check, fsid=0, anonuid=65534
, anongid=65534)
/export
172.16.0.15(rw, wdelay, no_root_squash, no_subtree_check, fsid=0, anonuid=65534
, anongid=65534)
nas1:~#
```

Sur ftp.alex.dmz, ajoutez cette ligne dans le fichier /etc/fstab :

```
...
# Partage /home du serveur NFS nas.alex.dmz.
172.16.0.19:/home /home nfs4 rsize=32768, wsize=32768, soft 0 0
```

Montez le partage NFSv4 :

```
ftp:~# mount /home
```

Pour vérifier :

```
ftp:~# mount | grep home
172.16.0.19:/home on /home type nfs4
(rw, rsize=32768, wsize=32768, soft, addr=172.16.0.19)
ftp:~#
```

Créez un répertoire /home/ftp pour les clients anonymes et changez les droits :

```
ftp:~# mkdir /home/ftp
ftp:~# chmod 755 /home/ftp
ftp:~# chgrp nogroup /home/ftp
```

Si ce serveur FTP sert à déposer des données pour des sites Web, vous pouvez changer les droits (héritage) et le groupe sur les home directories des utilisateurs concernés pour que Apache puisse lire et écrire :

```
ftp:~# chgrp www-data /home/arnofear
ftp:~# chmod 2770 /home/arnofear
```

Redémarrez le service vsftpd :

```
ftp:~# /etc/init.d/vsftpd restart
Restarting FTP server: vsftpd.
ftp:~#
```

Configuration du logiciel client FTP

Installez un client FTP qui supporte le FTP over SSL, comme [Filezilla](#).

Configurez Filezilla :

menu "Fichier" > "Gestionnaire de Sites..." > "Nouveau Site"

Hôte : *ftp.alex.dmz*

Type de serveur : **FTPES - FTP sur TLS/SSL - Chiffrement explicite**

Type d'authentification : Normale

Utilisateur : *arnofear*

Mot de passe :

Puis Connexion et acceptez le certificat.

Document mis à jour : 09/01/08



Ce document est publié sous licence [Creative Commons Attribution, Partage à l'identique, Contexte non commercial 3.0](http://creativecommons.org/licenses/by-nc-sa/3.0/deed.fr) :
<http://creativecommons.org/licenses/by-nc-sa/3.0/deed.fr>