Serveur FTP ProFTP

Procédures

Installation

1. Installer le paquetage *proftpd*
2. Choisir une installation « Indépendamment » (le service sera lancé seul, sans passer par le gestionnaire de service *inet* qui lui alloue moins de ressources)
3. Vérifier le fonctionnement à partir d'un navigateur (ou d'un client FTP, port 21) : ftp://@Serveur (s'authentifier avec un compte autre que *root*). Vous devez voir le dossier */home* de l'utilisateur.

Configuration

Les principaux fichiers sont (dans /etc/proftpd):

Fichier	Usage
proftpd.conf	Définit les principales caractéristiques techniques du service FTP : nom de la machine vu sur le réseau, durée de session, nombre de connexions simultanées, modules appelés (SGBD, sécurité, etc), répertoires partagés (pour compte anonyme ou compte authentifiés), éléments de sécurité, ports d'écoute, etc
sql.conf	Définit les options pour la mise en relation avec une base de données (MySQL ou PostGreSQL) : SGBD, mode d'authentification, compte de connexion à la base, tables utilisées
ldap.conf	Définit les options de connexion à un annuaire par le protocole LDAP : nom de connexion, domaine, localisation du serveur, etc
tls.conf	Définit les options de configuration pour l'usage d'une connexion sécurisée : certificat, forcer l'authentification, etc
modules.conf	Précise les modules à charger lors du démarrage du service : base de données, sécurité, quotas, etc
virtuals.conf	Gestion d'hôtes virtuels (un serveur, plusieurs domaines)

Mode opératoire

Le monde libre propose de multiples déclinaisons du protocole FTP sous forme de services : wuFTP, ProFTP, vsFTP... Nous étudierons ici les grandes lignes de ProFTP qui a la réputation d'être un peu complexe d'administration (mais proche d'Apache), « couplable » avec de l'authentification (MySQL ou LDAP), gérant des droits de partage par utilisateur ou groupe, mieux sécurisé vis a vis des failles

que wuFTP par exemple (source à retrouver).

Configuration de base

Fichier proftpd.conf

Ce fichier définit le comportement du service (modules appelés, type d'adressage IP, nom du serveur, etc), mais aussi les listes de partage que l'on met en place et les droits d'accès associés. Il fait appel à d'autres fichiers externes pour préciser certaines valeurs.

Configuration du service

Paramétrage du service (Extraits)

```
Include /etc/proftpd/modules.conf   # appelle le fichier de modules
                    # complémentaires (par exemple module MySQL ou LDAP)
ServerName "Serveur Partage"        # nom du serveur tel qu'il est vu dans
l'explorateur client
ServerType standalone               # serveur qui est lancé sans
l'intermédiaire
                    # du gestionnaire de service inet (meilleure
performance)
DeferWelcome on                 # n'affiche le message d'accueil qu'après
authentification
DefaultServer on                # le serveur prendra en charge les demandes
de  machines non référencées dans les
                                    # configurations
TimeoutNoTransfer 600               # temps sans transfert avant fermeture
de connexion authentifiée
TimeoutStalled 600              # temps sans transfert avant fermeture
connexion
TimeoutIdle 1200                # temps sans échange (transfert, contrôle)
avant fermeture

DisplayLogin welcome.msg            # fichier qui contient le message
d'accueil

DenyFilter *.*/             # expressions régulières refusées
                        # ici, interdit de lister tout le contenu d'un
dossier

DefaultRoot ~                    # bloque les utilisateurs dans leur dossier
/home/nomUtil
                        # on peut aussi préciser un autre répertoire pour
tous

# RequireValidShell off             # autorise/empêche la connexion
```

```
d'utilisateur sans shell
                    # permet de restreindre l'accès à des utilisateurs Linux
Port 21               # port d'écoute pour les connexions (21 par défaut)
                    # Remarque : les transferts se font sur le port 20
MaxInstances 30                         # nombre de connexions simultanées
autorisées
User proftpd                    # compte utilisateur qui lance le service
(sécurité)
Group nogroup                   # groupe de l'utilisateur qui lance le
service (sécurité)
AllowOverwrite on               # permet de remplacer les fichiers partagés
TransferLog /var/log/proftpd/xferlog   # répertoire des journaux liés aux pb
de transfert
SystemLog /var/log/proftpd/proftpd.log  # journaux des problèmes système
(connexion, auth...)
#Include /etc/proftpd/virtuals.conf   # pour gérer les hôtes virtuels dans
un fichier externe
```

Configuration des partages

Répertoire de connexion

Par défaut sur ProFTPd, les utilisateurs se retrouvent à la connexion dans le dossier */home/nomUtilisateur*. On peut le redéfinir par la directive ***DefaultRoot*** qui bloque en outre l'utilisateur et l'empêche de remonter l'arborescence (on dit que l'utilisateur est chrooté). On utilisera la valeur « ~ » qui correspond à */home/nomUtilisateur*, ou un dossier que l'on a choisi (par ex. */var/www* pour les pages Web d'Apache).

Le dossier de connexion est défini par ***DefaultRoot*** :

- globalement pour le serveur (soit directement, soit dans une section ***<Global>***)
- pour une connexion anonyme (***<Anonymous …>***)
- dans un hôte virtuel (***<Virtual Host>***, voir fiche Apache).

Attribution de droits

La limitation des droits d'utilisation des dossiers s'effectue par la directive Limit :

```
<Limit liste_actions>
    AllowUser monCompte     # autorise l'accès pour l'utilisateur monCompte
    DenyAll            # refuse l'accès à tous les autres
</Limit>
```

Les principales actions que l'on peut restreindre par ***LIMIT*** sont décrites dans le tableau ci-dessous :

Options	Explication
ALL	Tous les droits
APPE	Ajouter du contenu à un fichier (Append) → Modifier

Options	Explication
CWD	Se déplacer dans l'arborescence des dossiers (Change Working Directory)
DELE	Suppression de fichiers
MKD/RMD	Créer/ Supprimer des dossiers
RETR	Récupération de fichiers du serveur par le client (Download)
RNFR/RNTO	Renommer des fichiers existant (Rename From, Rename To)
STOR	Envoie de fichiers du client vers le serveur (Upload)
WRITE/READ	Écrire (créer) ou Lire des fichiers

On peut redéfinir des droits à un niveau inférieur du dossier de connexion grâce à la directive ***Directory*** :

```
<Directory /var/RessourcesBTS>       # spécifications pour le dossier
; /var/ressourcesBTS
    <Limit WRITE>             # droit pour l'écriture (dépôt)
        AllowGroup gpProfs  # réservé aux enseignants (groupe gpProfs)
        DenyAll         # refuse l'accès en écriture à tous les autres
    </Limit>
    <Limit READ>            # droit pour la  lecture (récupération)
        AllowAll         # autorisé à tout le monde
    </Limit>
</Directory>
```

Exemple du fichier de base pour un partage anonyme

```
<Anonymous /home/ftp>              # partage anonyme sur le dossier
/home/ftp
    User ftp          # compte qui gère ce partage (compte anonyme)
    Group ftp           # groupe du compte
    UserAlias anonymous ftp   # noms équivalents pour se connecter en
anonyme
    RequireValidShell off      # le compte anonyme n'existe pas sous Linux
    MaxClients 10          # limite à 10 connexions anonymes simultanées
<Directory *>              # tout dossier contenu sous /home/ftp
    <Limit WRITE>          # interdit en écriture
        DenyAll
    </Limit>
</Directory>
</Anonymous>
```

PROFTP et authentification déportée

Par défaut, l'authentification des utilisateurs par ProFTP se fait par les comptes existant sous Linux. Il est possible de reporter sur un système plus souple cette authentification : un fichier de comptes et groupes (non traité), un annuaire, ou une base de données. Pour ce faire, on devra activer certains modules et renseigner certains paramètres dans les fichiers de configuration, après avoir installé les modules correspondant.

Prise en charge de l'authentification par MySQL

ProFTP peut être complété par un module de gestion de la prise en charge de l'authentification par une base de données. Pour MySQL, on installera le paquetage ***proftpd-mysql***. On procèdera aux paramétrages ci-dessous dans les fichiers correspondant.

Fichier proftpd.conf

Dans ce fichier, on se contente d'inclure le paramétrage relatif à SQL présent dans un autre fichier.

```
#Include /etc/proftpd/ldap.conf   # si on utilise un serveur LDAP
Include /etc/proftpd/sql.conf    # à dé-commenter pour l'utilisation d'une base de données
```

Fichier modules.conf

Le fichier indique les modules à charger parmi ceux présents dans le dossier */usr/lib/proftpd*. Dans le cas de l'utilisation d'une base de données MySQL, on dé-commentera les lignes suivantes :

```
LoadModule mod_sql.c            # prise en charge de l'authentification par un SGBD
LoadModule mod_sql_mysql.c  # nom du SGBD avec lequel on est en contact
```

Fichier sql.conf

C'est ici qu'on décrira le type d'authentification, le nom des tables et les champs dans lesquels on ira vérifier les informations d'authentification transmises

```
<IfModule mod_sql.c>     # paramétrage utilisé si le module SQL est  activé
SQLBackend mysql        # nom du SGBD qui contient les tables des comptes
#SQLEngine on
SQLAuthenticate users* groups* # indique le niveau de droits (utilisateurs, groupes, les deux)
SQLAuthTypes Crypt Plaintext    # mode de gestion des mots de passe crypté et/ou en clair
#SQLAuthTypes Backend Crypt     # si on veut que ce soit MySQL qui fasse l'authentification
SQLConnectInfo proftpDB@localhost root mproot   # base, serveur et coordonnées d'un compte MySQL (à adapter)
SQLUserInfo ftpuser userid passwd uid gid homedir shell     # table contenant les comptes d'utilisateurs et champs étudiés
#SQLUserWhereClause "LoginAllowed = 'true'"     # n'accepte que les comptes actifs
SQLGroupInfo ftpgroup groupname gid members     #table/champs étudiés pour groupes
SQLLogFile /var/log/proftpd/mysql.log       #  journaux liés aux échanges
```

```
avec la base
</IfModule>
```

Voir plus loin pour les éléments de création d'une base MySql pour cette configuration.

Prise en charge de l'authentification par un annuaire

ProFTP peut être complété par un module de gestion de la prise en charge de l'authentification par un annuaire LDAP. On installera le paquetage *proftpd-mod-ldap*. On procèdera aux paramétrages ci-dessous dans les fichiers correspondant.

Fichier proftpd.conf

Dans ce fichier, on inclue le paramétrage relatif à LDAP présent dans un autre fichier et on désactive la gestion par Linux.

```
Include /etc/proftpd/ldap.conf     # à dé-commenter pour l'utilisation d'un serveur LDAP
#Include /etc/proftpd/sql.conf    # à dé-commenter pour l'utilisation d'une base de données
RequireValidShell  off     # permet l'utilisation de comptes non présents sous Linux
AuthPAM  off               # évite la recherche des comptes Linux
AuthOrder    mod_ldap.c     # définit l'ordre de recherche pour l'authentification (LDAP en premier)
```

Fichier modules.conf

Le fichier indique les modules à charger parmi ceux présents dans le dossier /usr/lib/proftpd. Dans le cas de l'utilisation d'un annuaire LDAP, on dé-commentera les lignes suivantes :

```
LoadModule mod_ldap.c  # prise en charge de l'authentification par un annuaire
```

Fichier ldap.conf

C'est ici qu'on décrira l'adresse de l'annuaire, le compte pour interroger l'annuaire, le chemin pour chercher les comptes. Seules les options de base sont décrites ici.

```
<IfModule mod_ldap.c>                              # paramétrages si le module LDAP est activé
LDAPServer ldap://adresse_annuaire[:port]      #adresse (IP, FQDN) du serveur d'annuaire
LDAPBindDN "cheminLDAPCompteLecture" "mot_passe"    # compte pour interroger l'annuaire
```

```
LDAPAttr attributAnnuaire variable              # renomme les attributs LDAP
selon les variables du contexte
LDAPUsers "cheminLDAPversOU" "renvoi_vers_le_compte_utilisateur_soumis"
#infos pour l'authentification avec le compte
</IfModule>
```

Exemple de fichier LDAP

```
<IfModule mod_ldap.c>    # paramétrages si le module LDAP est activé
# FQDN de l'annuaire (le serveur ProFTP doit pouvoir résoudre le domaine
gsbeu.intra)
LDAPServer ldap://LABANNU.gsbeu.intra/ ??sub
#Compte utilisé pour parcourir l'annuaire. Ne devrait pas être
l'administrateur du domaine
#mais un compte avec les droits suffisants.
LDAPBindDN "cn=gestAnnuaire,cn=Users,dc=gsbeu,dc=intra" "mp123GES"  #
exemple à adapter selon le contexte
#renommage du champ LDAP cn sous l'intitulé SamAccountName
LDAPAttr cn SamAccountName
#chemin de recherche dans l'unité « services » en utilisant le compte soumis
au serveur FTP
LDAPUsers "ou=services,dc=gsbeu,dc=intra" (SamAccountName=%u)
</IfModule>
```

Client FTP

L'accès à un serveur FTP doit se faire par un client :

- le navigateur internet, qui est généralement limité à la récupération de contenu (mais IE permet l'envoi)
- un client avec interface graphique : type Filezilla
- la ligne de commande (ou du script)
- des fonctions de langage de programmation : voir par exemple ici pour PHP.

Connexion avec un serveur

La connexion à un serveur utilise les éléments suivants : [utilisateur [:motpasse] @] adresse [:port].
Exemples : ftp://monCompte@192.168.0.152
ftp://192.168.0.154:2121
ftp://monCompte:monPWD@192.168.0.189:4400

Eléments de la ligne de commande FTP

(voir plus de possibilités sur comment ça marche)

Commande	Utilisation	Exemples
ftp	Passe en mode ligne de commande et réalise éventuellement la connexion ftp	`ftp 192.168.0.156` `ftp monCompte@192.168.0.152`
open	Ouvre une connexion avec un serveur	`open 192.168.0.156`
ls	Liste le contenu d'un dossier ls	`ls sousDossier`
pwd	(Print Working Directory) Affiche le dossier courant	
mkd / rmd	Crée / Supprime un dossier	

put / get	Envoie / Récupère un document	`//envoie le fichier vers le serveur`
		`put fichierChezMoi`
		`//envoie le fichier et le renomme`
		`put fich1 fich2`
		`// récupère le fichier du serveur`
		`get fichierDistant`
		`//récupère le fichier et le renomme`
		`get ficDist ficLoc`

!	Exécute une commande sur la machine locale	`//se déplace dans l'arborescence locale`
		`!cd ..`
		`///crée un dossier en local`
		`!md nomDossier`

Annexe

Script pour la création de la base

Création de la base et d'un compte de connexion (exemple)

```
-- création de la base de données
CREATE DATABASE proftpBDD;
-- connexion à la base
USE proftpBDD ;
-- création d'un compte MySQL pour gérer la base. Evite d'utiliser le compte root
GRANT USAGE
ON proftpBDD.*
TO proftpRoot@'localhost'
IDENTIFIED BY 'mpProftpRoot'
WITH GRANT OPTION;
```

Création des tables (exemple)

```
-- Table pour les groupes
CREATE TABLE ftpgroup (
groupname VARCHAR(16) NOT NULL DEFAULT '',
gid SMALLINT (6) NOT NULL DEFAULT '5500', -- la valeur 5500 est libre de choix
members VARCHAR(16) NOT NULL DEFAULT '',
PRIMARY KEY (groupname )
) ENGINE=InnoDB COMMENT='Groupes pour ProFTP';
```

```
-- Table pour les utilisateurs
CREATE TABLE ftpuser (
id INT(10) UNSIGNED NOT NULL AUTO_INCREMENT,    -- identifiant dans la base
userid VARCHAR(32) NOT NULL DEFAULT '',    -- nom de connexion
passwd VARCHAR(32) NOT NULL DEFAULT '',    -- mot de passé du compte
uid SMALLINT (6) NOT NULL DEFAULT '5500',  -- id de l'utilisateur, différent
pour chaque compte
gid SMALLINT (6) NOT NULL DEFAULT '5500',  -- meme numéro que dans la table
groupe
email VARCHAR(255) NOT NULL,         -- email
homedir VARCHAR(255) NOT NULL DEFAULT '',  -- dossier de connexion FTP
shell VARCHAR(16) NOT NULL DEFAULT '/bin/false',   -- shell pour les comptes
linux
COUNT INT(11) NOT NULL DEFAULT '0',
accessed DATETIME NOT NULL DEFAULT '0000-00-00 00:00:00',
dl_bytes BIGINT (20) NOT NULL ,
dl_count BIGINT (20) NOT NULL,
ul_bytes BIGINT (20) NOT NULL ,
ul_count BIGINT (20) NOT NULL ,
modified DATETIME NOT NULL DEFAULT '0000-00-00 00:00:00',
LogInAllowed ENUM('true','false') NOT NULL DEFAULT 'true',    -- droit de
connexion (true ou false)
PRIMARY KEY (id)
) ENGINE=InnoDB COMMENT='Utilisateurs pour ProFTP';
```

Insertion des données (exemple)

```
-- insertion d'un compte dans la table pour se connecter
-- ATTENTION ! remplacer le nom et le mot de passe par ceux d'un compte
existant sur
-- le serveur Linux si on a choisi RequireValidShell on dans le fichier
proftpd.conf
-- Remarque : "Encrypt" utilise le cryptage Unix/Linux, ne fonctionne pas
pour MySQL Windows,
-- peut-être que des installations sont possibles pour rendre opérationnel
sous Windows (non testé)
INSERT INTO ftpuser
(id ,userid , passwd ,uid ,gid ,homedir,COUNT ,accessed ,modified
,LogInAllowed )
VALUES ('','utilFTP',encrypt('mpUtilFTP'),
'5500','5500','/home/utilFTP','','','','true');
-- Ajout d'un groupe dont l'utilisateur est membre
INSERT INTO ftpgroup VALUES ('Groupe FTP','5500','utilFTP');
```

Source internet

- http://doc.ubuntu-fr.org/proftpd : quelques explications en français
- http://www.cgsecurity.org/Articles/proftpd.html : détail bien expliqué sur la configuration des accès anonymes et sur les droits sur les partages

- http://www.proftpd.org/docs/directives/linked/configuration.html : en anglais, sur le site de l'outil, la liste des directives, des modules et leur explication précise
- http://doc.ubuntu-fr.org/proftpd_et_mysql : installation *proftpd* et authentification MySQL sur Ubuntu
- Article de Linux Plus Magazine 06/2009
- http://www.bouthors.fr/wiki/doku.php?id=linux:proftpd : site d'un individuel sur le paramétrage de *proftpd*