CentOS 7. Установка пакета ProFTPD и интеграция с Windows 2008 R2 AD.

Подключаем **EPEL** репозиторий:

rpm -iUvh http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-5.noarch.rpm

или

yum install epel-release

Устанавливаем пакет **ProFTPD**:

yum -y update
yum -y install proftpd

Установим пакет **openldap-clients**, если его еще нет в системе, он нужен для тестирования соединения с контроллером домена:

yum install openldap-clients

Пробуем теперь подключиться к контроллеру домена **developer.com** и прочитать данные от имени пользователя **user**:

ldapsearch -x -h 192.168.111.3 -D 'user@developer.com' -W -b 'dc=developer,dc=com'

Далее вводим пароль и если есть связь с контроллером и пользователь опознан, вернутся данные о пользователях в этом домене.

Открываем файл **/etc/proftpd.conf** и приводим к виду:

```
ServerName "ProFTPD server"
ServerIdent on "Hello"
ServerAdmin root@localhost
ServerType standalone
DefaultServer on
AccessGrantMsg "User %u logged in."
DeferWelcome off

# Use pam to authenticate (default) and be authoritative
AuthPAMConfig proftpd

# Do not perform ident nor DNS lookups (hangs when the port is filtered)
IdentLookups off
UseReverseDNS off

# Port 21 is the standard FTP port.
Port 21

# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
```

```
Umask 022

# Default to show dot files in directory listings
ListOptions "-a"

# Allow to resume not only the downloads but the uploads too
AllowRetrieveRestart on
AllowStoreRestart on

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances 20

# Set the user and group that the server normally runs at.
User nobody
Group nobody

# Disable sendfile by default since it breaks displaying the download speeds in
# ftptop and ftpwho
UseSendfile no

# This is where we want to put the pid file
ScoreboardFile /var/run/proftpd.score


########################################################################################
# Начало. Необходимое для LDAP авторизации пользователей и работы                      #
########################################################################################

# Отключаем то, что не используем
RootLogin off
LoginPasswordPrompt off

# Класс для ограничения скорости канала внешней загрузки и выгрузки, т.е. закачка снаружи
<Class external>
From !192.168.0.0/16
</Class>

# Класс для ограничения скорости канала внутренней загрузки и выгрузки, т.е. закачка
внутри
<Class internal>
From 192.168.0.0/16
</Class>

# Ограничение скорости канала загрузки и выгрузки для класса external
TransferRate RETR,STOR,APPE 1024 class external
```

```
# Ограничение скорости канала загрузки и выгрузки для класса internal
TransferRate RETR,STOR,APPE 10240 class internal

# Ограничения подключений
MaxClients 10 "Слишком много соединений с сервером"
MaxClientsPerHost 3 "%m клиент уже подключен с Вашего хоста, больше нельзя"
MaxLoginAttempts 3 "Слишком много попыток войти"

# Ограничения по времени
TimeoutIdle 180
TimeoutLogin 120
TimeoutNoTransfer 360
TimeoutStalled 640

# Закрываем всех в chroot. Выйты выше своей папки расположенной в /home/ftp/users/%u
нельзя.
DefaultRoot /home/ftp/users/%u
#######

RequireValidShell off
#######

PersistentPasswd off
#######

# подгружаем модуль LDAP
LoadModule mod_ldap.c

# подключение пользователей методом LDAP
<IfModule mod_ldap.c>
AuthOrder mod_ldap.c

LDAPServer 192.168.111.3
LDAPAttr  uid sAMAccountName uidNumber gidNumber
LDAPAuthBinds on

LDAPBindDN "user@developer.com" "123456"
LDAPUsers "ou=Структура Компьютеры и Пользователи,dc=developer,dc=com"
(&(sAMAccountName=%u)(memberOf=cn=proftpd,ou=proxy,dc=developer,dc=com))
LDAPGroups "ou=Структура Компьютеры и Пользователи,dc=developer,dc=com"
(&(sAMAccountName=%u)(memberOf=cn=proftpd,ou=proxy,dc=developer,dc=com))

LDAPDefaultUID 99
LDAPDefaultGID 99

LDAPForceDefaultUID on
LDAPForceDefaultGID on

LDAPGenerateHomedir on
```

```
LDAPForceGeneratedHomedir on

LDAPGenerateHomedirPrefix /home/ftp/users
CreateHome on 0755

</IfModule>
#######

# Рабочая область загрузки и выгрузки
<Directory /home/ftp/users*>

AllowOverwrite        yes
<Limit ALL>
AllowAll
</Limit>

<Limit ALL SITE_CHMOD>
AllowAll
</Limit>

</Directory>
#######


# Формат лог файлов
LogFormat default "%h %l %u %t \"%f\" \"%r\" %s %b"
LogFormat auth "%v [%P] %h %t \"%r\" %s"
LogFormat write "%h %l %u %t \"%f\" \"%r\" %s %b"

# Куда, и что пишем в лог файлы
SystemLog /var/log/proftpd/proftpd.log
TransferLog /var/log/proftpd/xfer.log
ExtendedLog /var/log/proftpd/proftpd_access.log WRITE,READ write
ExtendedLog /var/log/proftpd/proftpd_auth.log AUTH auth

# Запрет перебора
DenyFilter \*.*/


##########################################################################
# Конец. Необходимое для LDAP авторизации пользователей и работы         #
##########################################################################
```

Самое главное в конфиге это в этой строке:
LDAPUsers "ou=Структура Компьютеры и Пользователи,dc=developer,dc=com"
(&(sAMAccountName=%u)(memberOf=cn=proftpd,ou=proxy,dc=developer,dc=com))

Пользователи которым разрешено подключаться к **FTP** находятся в **орг-юните** "**Структура**

Компьютеры и Пользователи" в корне домена.

Эти пользователи принадлежат группе "**proftpd**", которая находится в **орг-юните** "**proxy**" так же в корне домена. Т.е. , чтобы пользователь получил доступ его нужно добавить в группу "**proftpd**".

Конфигом настроено ограничение выхода пользователя из своей папки. Т.е. все пользователи заперты в своих папках. Выставлено разное ограничение скорости загрузки и выгрузки при подключении из локальной сети и из интернета.

Прописываем сервис в автозапуск:
systemctl enable proftpd.service

Запускаем:
systemctl start proftpd.service