Installation, paramétrage, et mise en œuvre d'un LDAP

Installation

Auteur : CGI et Région Île-de-France

Version : 0.13

Gestion des changements de version

Ce tableau gère les modifications apportées au document au-delà de sa version initiale. Les petites modifications de type erreurs de frappe ou changements de syntaxe ne font pas l'objet d'un suivi. Toute nouvelle version du document ne conserve pas systématiquement les changements apportés lors de la version précédente.

Version	Date	Auteur	Objet de la mise à jour
0.1	15/11/13	SRIT	Version initiale
0.2	09/01/14	MMAR	MAJ pour version 2.1.5
0.3	25/03/14	SRIT	MAJ pour version 2.1.7
0.4	19/06/14	SRIT	MAJ pour version 2.1.8
0.5	13/10/14	SRIT	MAJ pour version 2.1.9
0.6	14/01/15	SRIT	MAJ pour version 2.1.10
0.7	29/01/15	SRIT	MAJ pour version 2.1.11
0.8	04/03/15	SRIT	MAJ pour version 2.1.12
0.9	11/05/15	SRIT	MAJ pour version 2.1.13
0.10	17/08/15	SRIT	MAJ pour version 2.1.14
0.11	25/08/15	SRIT	MAJ pour version 2.1.15
0.12	27/09/15	SRIT	MAJ pour version 2.2.0
0.13	16/11/15	SRIT	MAJ pour version 2.2.1

SOMMAIRE

Table des matières

1 Récupération des paquets

Cette documentation est relative à l'installation du LDAP **2.2.1.** de l'ENT Lilie d'Île-de-France.

Il est necessaire de recuperer l'ensemble des paquets du LDAP.
Les paquets peuvent être récupérés sur la forge de l'ADULLACT (http://www.adullact.org).
Ils sont disponibles a l'adresse https://adullact.net/projects/openent dans l'onglet Fichiers :

L'installation du LDAP est effectué sur un serveur Linux Debian.

✔ Documentation d'installation et d'exploitation

- **lilie-installation-ldap-pdf.zip**

Ce fichier contient la documentation d'installation et d'exploitation

✔ Composants LDAP

- **openldap-2.4.35.tgz**

Les sources Openldap. OpenLDAP est une implémentation open source du protocole Lightweight Directory Access

- **schema-2.2.1.zip**

Les schémas LDAP.

- **scripts-ldap-2.2.1.zip**

Des scripts utiles pour le LDAP.

✔ Batch pour le LDAP

- **bat-repriseldap-2.2.1.zip**

Les fichiers et configurations utiles pour la reprise des données de la base annuaire dans le LDAP.

- **bat-alimentationldap-2.2.1.zip**

Les fichiers et configurations utiles pour l'alimentation des données académiques dans le LDAP.

- **bat-exportannuaire-ldap-2.2.1.zip**

Un export LDIF pour intégration dans l'annuaire eliot_scolarite

- **bat-connecteur-ldif-2.2.1.zip**

L'import dans les bases temporaires eliot_scolarite de l'export LDIF

- **bat-exportannuaire-ldap-2.2.1.zip**

L'import dans l'annuaire eliot_scolarite depuis les bases temporaires

- **gen_code_activation-2.2.1.zip**

La mise à jour des codes d'activation parents dans le LDAP.

- **initialisation_ldap-2.2.1.zip**

Des scripts d'initialisation du LDAP.

✔ **Doonées pour le LDAP**

- **lilie-jeu-essai-import-2.2.1.zip**

Données pour alimenter le ldap. Le déposer dans un répertoire (exemple : /appli/ldap/scripts/ANNUAIRES/Complet/)

2 Installation LDAP

La procédure ci-dessous décrit l'installation du LDAP situé sur le même serveur que l'ENT. Il est évidemment possible de mettre le LDAP sur un autre serveur ou sur une machine virtuelle . La procédure doit alors être légèrement adaptée en fonction de votre architecture.

La documentation suivante suppose qu'un répertoire **/appli/ldap/** est créé à la racine du système de fichier du serveur.

2.1 Librairies et dépendances nécessaires au ldap et aux scripts d'exploitation

Il faut installer /vérifier les présences des librairies suivantes :
Si nécessité de proxy, ajouter le proxy (http_proxy=http://proxy.noc.lan :3128)

```
apt-get install libdbi-perl libpq5 libdbd-pg-perl libnet-ldap-perl libdatetime-perl dos2unix
xsltproc
```

Il faut installer tidy sur toutes les machines qui peuvent faire tourner l'alimentation :

```
apt-get install tidy
puis ln -s /usr/bin/tidyp /usr/bin/tidy
```

2.2 Installation OpenLDAP par la méthode de compilation

Berkeley DB famille de l'open source, bases de données intégrables fournit aux développeurs rapidité, fiabilité et persistance locale avec zéro administration. Souvent déployé en tant que «garde» des bases de données, Berkeley DB famille fournit de très hautes performances, la fiabilité, l'évolutivité et de disponibilité pour les cas d'utilisation d'applications qui ne nécessitent pas SQL.

```
apt-get install db4.8 libdb4.8-dev
```

Décompression/compilation du paquet sans accesslog :

```
cd /opt
tar -xvzf openldap-2.4.35.tgz
mv openldap-2.4.35 src_openldap-2.4.35
cd src_openldap-2.4.35
./configure --prefix=/opt/openldap-2.4.35
make
make depend
make install
```

Création d'un lien symbolique OpenLDAP pour en simplifier son utilisation :

```
cd /opt
ln -s /opt/openldap-2.4.35/ openldap
```

Répertoire des binaires :

```
ls -ltr /opt/openldap/bin/*
lrwxrwxrwx 1 root root     10 21 janv. 14:07 ldapadd -> ldapmodify
-rwxr-xr-x 1 root root 258624 17 janv. 09:20 ldapcompare
-rwxr-xr-x 1 root root 259040 17 janv. 09:20 ldapdelete
-rwxr-xr-x 1 root root 259264 17 janv. 09:20 ldapexop
-rwxr-xr-x 1 root root 270912 17 janv. 09:20 ldapmodify
-rwxr-xr-x 1 root root 258656 17 janv. 09:20 ldapmodrdn
-rwxr-xr-x 1 root root 257888 17 janv. 09:20 ldappasswd
-rwxr-xr-x 1 root root 281312 17 janv. 09:20 ldapsearch
-rwxr-xr-x 1 root root 151200 17 janv. 09:20 ldapurl
-rwxr-xr-x 1 root root 256256 17 janv. 09:20 ldapwhoam
```

Répertoire du daemon openldap (exécutable) :

```
ls -ltr /opt/openldap/libexec/*
-rwxr-xr-x 1 root root 1808576 17 janv. 09:20 slapd
```

Répertoire des fichiers de configurations par défaut :

```
ls -ltr /opt/openldap/etc/openldap
-rw------- 1 root root  845 17 janv. 09:20 DB_CONFIG.example
-rw-r--r-- 1 root root  245 17 janv. 09:19 ldap.conf
-rw-r--r-- 1 root root  245 17 janv. 09:19 ldap.conf.default
drwxr-xr-x 2 root root 4096 17 janv. 09:20 schema
-rw------- 1 root root 2179 17 janv. 09:20 slapd.conf
-rw------- 1 root root 2179 17 janv. 09:20 slapd.conf.default
-rw------- 1 root root 2664 17 janv. 09:20 slapd.ldif
-rw------- 1 root root 2664 17 janv. 09:20 slapd.ldif.default
```

Arborescence cible données OpenLDAP :

/opt/openldap à Binaires OpenLDAP (lien vers /opt/openldap-2.x.yyy)
/opt/openldap-2.3.35 → Binaires OpenLDAP
/appli/ldap → Racine des données, conf OpenLDAP
    /conf → fichiers de conf du ldap (slapd.conf et slapd_traitement.conf)
        /schema → Schéma utilisés (standard + ENT)
    /tmp → Fichiers temporaires d'OpenLDAP (pid, args…)
    /logs → Fichiers de logs
    /data → Stockage des données
        /slapd → stockage des données ENT du ldap TP

Création du socle OpenLDAP sur tous les serveurs ldap :

```
cd /appli/ldap
```

```
mkdir /appli/ldap/conf
mkdir /appli/ldap/conf/schema
mkdir /appli/ldap/tmp
mkdir /appli/ldap/logs
mkdir /appli/ldap/data
mkdir /appli/ldap/data/slapd
```

Script de démarrage :

Créer un nouveau fichier ent.openldap dans /etc/init.d :

```
#!/bin/bash
### BEGIN INIT INFO
# Provides:         ent.openldap
# Required-Start:    $remote_fs $network $syslog
# Required-Stop:     $remote_fs $network $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: OpenLDAP standalone server (Lightweight Directory Access Protocol)
### END INIT INFO

# Specify path variable
PATH=/opt/openldap/libexec:/opt/openldap/bin:/opt/openldap/sbin:/sbin:/usr/sbin:/bin:/usr/b
in

. /lib/lsb/init-functions

# Kill me on all errors
set -e

# Set the paths to slapd as a variable so that someone who really
# wants to can override the path in /etc/default/slapd.
SLAPD=/opt/openldap/libexec/slapd

# Stop processing if slapd is not there
[ -x $SLAPD ] || exit 0

# debconf may have this file descriptor open and it makes things work a bit
# more reliably if we redirect it as a matter of course.  db_stop will take
# care of this, but this won't hurt.
exec 3>/dev/null

# Source the init script configuration
# if [ -f "/etc/default/slapd" ]; then
#       . /etc/default/slapd
# fi

# System account to run the slapd server under. If empty the server
```

```
# will run as root.
SLAPD_USER="root"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="root"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.conf by
# default)
SLAPD_PIDFILE=
# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
SLAPD_SERVICES="ldap://0.0.0.0:389 ldapi:///"

# If SLAPD_NO_START is set, the init script will not start or restart
# slapd (but stop will still work).  Uncomment this if you are
# starting slapd via some other means or if you don't want slapd normally
# started at boot.
#SLAPD_NO_START=1

# If SLAPD_SENTINEL_FILE is set to path to a file and that file exists,
# the init script will not start or restart slapd (but stop will still
# work).  Use this for temporarily disabling startup of slapd (when doing
# maintenance, for example, or through a configuration management system)
# when you don't want to edit a configuration file.
# SLAPD_SENTINEL_FILE=/etc/ldap/noslapd

# For Kerberos authentication (via SASL), slapd by default uses the system
# keytab file (/etc/krb5.keytab).  To use a different keytab file,
# uncomment this line and change the path.
# export KRB5_KTNAME=/etc/krb5.keytab

# Additional options to pass to slapd
SLAPD_OPTIONS=""

# Load the default location of the slapd config file
SLAPD_CONF=/appli/ldap/conf/slapd.conf

# Stop processing if the config file is not there
if [ ! -r "$SLAPD_CONF" ]; then
  log_warning_msg "No configuration file was found for slapd at $SLAPD_CONF."
  # if there is no config at all, we should assume slapd is not running
  # and exit 0 on stop so that unconfigured packages can be removed.
  [ "x$1" = xstop ] && exit 0 || exit 1
```

```
fi

# extend options depending on config type
if [ -f "$SLAPD_CONF" ]; then
        SLAPD_OPTIONS="-f $SLAPD_CONF $SLAPD_OPTIONS"
elif [ -d "$SLAPD_CONF" ] ; then
        SLAPD_OPTIONS="-F $SLAPD_CONF $SLAPD_OPTIONS"
fi

# Find out the name of slapd's pid file
if [ -z "$SLAPD_PIDFILE" ]; then
        # If using old one-file configuration scheme
        if [ -f "$SLAPD_CONF" ] ; then
                SLAPD_PIDFILE=`sed -ne 's/^pidfile[[:space:]]\+\(.\+\)/\1/p' \
                        "$SLAPD_CONF"`
        # Else, if using new directory configuration scheme
        elif [ -d "$SLAPD_CONF" ] ; then
                SLAPD_PIDFILE=`sed -ne \
                        's/^olcPidFile:[[:space:]]\+\(.\+\)[[:space:]]*/\1/p' \
                        "$SLAPD_CONF"/'cn=config.ldif'`
        fi
fi

# XXX: Breaks upgrading if there is no pidfile (invoke-rc.d stop will fail)
# -- Torsten
if [ -z "$SLAPD_PIDFILE" ]; then
        log_failure_msg "The pidfile for slapd has not been specified"
        exit 1
fi

# Make sure the pidfile directory exists with correct permissions
piddir=`dirname "$SLAPD_PIDFILE"`
if [ ! -d "$piddir" ]; then
        mkdir -p "$piddir"
        [ -z "$SLAPD_USER" ] || chown -R "$SLAPD_USER" "$piddir"
        [ -z "$SLAPD_GROUP" ] || chgrp -R "$SLAPD_GROUP" "$piddir"
fi

# Pass the user and group to run under to slapd
if [ "$SLAPD_USER" ]; then
        SLAPD_OPTIONS="-u $SLAPD_USER $SLAPD_OPTIONS"
fi

if [ "$SLAPD_GROUP" ]; then
        SLAPD_OPTIONS="-g $SLAPD_GROUP $SLAPD_OPTIONS"
fi
```

```
# Check whether we were configured to not start the services.
check_for_no_start() {
        if [ -n "$SLAPD_NO_START" ]; then
                echo 'Not starting slapd: SLAPD_NO_START set in /etc/default/slapd' >&2
                exit 0
        fi
        if [ -n "$SLAPD_SENTINEL_FILE" ] && [ -e "$SLAPD_SENTINEL_FILE" ]; then
                echo "Not starting slapd: $SLAPD_SENTINEL_FILE exists" >&2
                exit 0
        fi
}

# Tell the user that something went wrong and give some hints for
# resolving the problem.
report_failure() {
        log_end_msg 1
        if [ -n "$reason" ]; then
                log_failure_msg "$reason"
        else
                log_failure_msg "The operation failed but no output was produced."

                if [ -n "$SLAPD_OPTIONS" -o \
                   -n "$SLAPD_SERVICES" ]; then
                     if [ -z "$SLAPD_SERVICES" ]; then
                          if [ -n "$SLAPD_OPTIONS" ]; then
                               log_failure_msg "Command line used: slapd $SLAPD_OPTIONS"
                          fi
                     else
                          log_failure_msg "Command line used: slapd -h '$SLAPD_SERVICES'
$SLAPD_OPTIONS"
                     fi
                fi
        fi
}

# Start the slapd daemon and capture the error message if any to
# $reason.
start_slapd() {
        if [ -z "$SLAPD_SERVICES" ]; then
                reason="`start-stop-daemon --start --quiet --oknodo \
                        --pidfile "$SLAPD_PIDFILE" \
                        --exec $SLAPD -- $SLAPD_OPTIONS 2>&1`"
        else
                reason="`start-stop-daemon --start --quiet --oknodo \
                        --pidfile "$SLAPD_PIDFILE" \
                        --exec $SLAPD -- -h "$SLAPD_SERVICES" $SLAPD_OPTIONS 2>&1`"
        fi
```

```
        # Backward compatibility with OpenLDAP 2.1 client libraries.
        if [ ! -h /var/run/ldapi ] && [ ! -e /var/run/ldapi ] ; then
                ln -s slapd/ldapi /var/run/ldapi
        fi
}

# Stop the slapd daemon and capture the error message (if any) to
# $reason.
stop_slapd() {
        reason="`start-stop-daemon --stop --quiet --oknodo --retry TERM/10 \
                --pidfile "$SLAPD_PIDFILE" \
                --exec $SLAPD 2>&1`"
}

# Start the OpenLDAP daemons
start_ldap() {
        trap 'report_failure' 0
        log_daemon_msg "Starting OpenLDAP" "slapd"
        start_slapd
        trap "-" 0
        log_end_msg 0
}

# Stop the OpenLDAP daemons
stop_ldap() {
        trap 'report_failure' 0
        log_daemon_msg "Stopping OpenLDAP" "slapd"
        stop_slapd
        trap "-" 0
        log_end_msg 0
}

case "$1" in
start)
check_for_no_start
                start_ldap
;;
                stop)
                stop_ldap
;;
                restart|force-reload)
                check_for_no_start
                stop_ldap
                start_ldap
                ;;
                status)
                status_of_proc -p $SLAPD_PIDFILE $SLAPD slapd
```

```
        ;;
        *)
        echo "Usage: $0 {start|stop|restart|force-reload|status}"
        exit 1
        ;;
esac
```

Copier le fichier de démarrage slapd dans /etc/init.d
Modifier les droits sur le fichier /etc/init.d/ent.openldap pour le rendre exécutable :

```
chmod 755 /etc/init.d/ent.openldap
```

2.3 Fichier de configuration slapdconf (ldap “standalone”)

Dans ce fichier de configuration, tous les index sont présents
Editer le fichier /appli/ldap/conf/slapd.conf :

```
#######################################################################
#######################################################################
# Partie commune

# Schema and objectClass definitions
include       /appli/ldap/conf/schema/core.schema
include       /appli/ldap/conf/schema/cosine.schema
include       /appli/ldap/conf/schema/nis.schema
include       /appli/ldap/conf/schema/inetorgperson.schema

# Schema de l annuaire defini dans le SDET des ENT
include       /appli/ldap/conf/schema/sdet.schema
include       /appli/ldap/conf/schema/ent.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile       /appli/ldap/tmp/slapd.pid

# List of arguments that were passed to the server
argsfile      /appli/ldap/tmp/slapd.args

# Read slapd.conf(5) for possible values
loglevel      none
logfile       /appli/ldap/logs/slapd.log

# Where the dynamically loaded modules are stored
modulepath    /opt/openldap/lib
```

```
moduleload      back_hdb

# The maximum number of entries that is returned for a search operation anonymous
sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.
tool-threads 2
threads 16

backend        hdb

########################################################################
########################################################################
# Database ENT
database       hdb

# Base de la database ENT
suffix         "dc=ent,dc=fr"
directory      "/appli/ldap/data/slapd"
rootdn         "cn=admin,ou=system,dc=ent,dc=fr"
rootpw         {MD5}utj7R6ggLv1F6bvRi+Do1w==
password-hash   {MD5}

cachesize  100000
idlcachesize 300000

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 524288000 0
dbconfig set_flags DB_LOG_AUTOREMOVE

# Number of objects that can be locked at the same time.
dbconfig set_lk_max_objects 5000
# Number of locks (both requested and granted)
dbconfig set_lk_max_locks 10000
# Number of lockers
dbconfig set_lk_max_lockers 5000

#Globaux
index   objectClass                     eq
index   active                        eq
index   ou                              eq
index   cn,uid                        eq
index   sn                              pres,sub,eq
index   entryCSN,entryUUID              eq
#Personnes
```

```
index   ENTPersonJointure                  eq
index   ENTPersonLogin                     eq
index   mail                              eq
index   snNormalise                          pres,sub,eq
index   ENTPersonneDN                      eq,pres
index   ENTPersonProfils                   eq
index   ENTPersonAlias                     eq
index   givenNameNormalise                   sub,eq
index   ENTCodeActivationParent            eq
index   cnNormalise                          pres,sub,eq
index   ENTAuxPersonInit                   eq
index   ENTEleveStructRattachId            eq
index   ENTAuxPersonCompteAAF                eq
index   ENTAuxPersRelEleveEleve            eq
index   ENTPersonStructRattach             eq
index   ENTAuxOtherEtab                      eq
index   ENTPersonCodePostal                  eq
index   ENTCodeActivationEleve             eq
index   ENTAuxPersonDeleteDate               eq
index   ENTEleveClasses                    eq
index   ENTEleveMEF                           eq
index   ENTGroupeAnnuaireFiliere           eq
index   userPassword                      eq
index   ENTPersonNomPatro                    eq
index   givenName                            pres,sub,eq
index   ENTAuxPersonEtabAcces              eq

#Structures
index   ENTStructureJointure             eq
index   ENTPorteurCode                     eq
index   ENTEtablissementStructRattachFctl  eq
index   ENTStructureNomCourant               pres,sub,eq
#Groupes
index   description                          pres,sub,eq
index   descriptionNormalise             pres,sub,eq
index   ENTGroupeAnnuaireTitreNormalise    pres,sub,eq
index   member                               pres,eq
index   owner                              eq
index   ENTGroupeAdminLocal                    eq
index   ENTProfilDN                          pres,eq
index   ENTReferentielCode                   eq
index   ENTGroupeAnnuaireFonction            pres,eq

index   ENTGroupeAnnuaireClasseId            eq
index   ENTGroupeAnnuaireType              eq
index   ENTGroupeAnnuaireMefId               eq
index   ENTGroupeAnnuaireFiliereId           eq
```

```
index   ENTDisciplineDN                    eq
index   ENTGroupeAdminPere                     eq
index   ENTFonctionDN                    eq
index   ENTClasseDN                        eq
index   ENTGroupeAnnuaireClasse          pres
index   ENTAdminLocalEtab                 eq
index  ENTAdminLocalCreateur              eq
#Suivi de passage des annuaires
index   ENTSuiviAnnuaireId              eq

# Save the time that the entry gets modified, for database #1
lastmod        on

# Checkpoint the BerkeleyDB database periodically in case of system
# failure and to speed slapd shutdown.
dbnosync
checkpoint      50000 2

# The admin dn has full write access, everyone else
# can read everything.
access to *
        by dn="cn=admin,ou=system,dc=ent,dc=fr" write
        by * read
```

Il faut ensuite déziper l'archive **schema-2.2.1.zip** dans le répertoire **/appli/ldap/conf.** Afin de rajouter les schémas dans le repertoire conf du ldap.

3 Migration des données LDAP à partir de la base de données et alimentation LDAP

Afin d'initialiser correctement le fichier de configuration (DB_CONFIG), il est nécessaire d'effectuer 2 démarrages :

```
/etc/init.d/ent.openldap stop
/etc/init.d/ent.openldap start
```

3.1 Initialisation

Dézipper initialisation_ldap-**2.2.1**.zip dans /appli/ldap/scripts.

Vérifier le fichier /appli/ldap/scripts/initialisation_DIT/parametres.sh

```
#!/bin/bash
#LDAP
ILDAPDN="dc=ent,dc=fr"
IROOTDN="cn=admin,ou=system,dc=ent,dc=fr"
LDAPSERVEUR="ldap.local.lilie.org"
LDAPPORT="389"
LDAPPWD="lilie"

#Binaires LDAP
LDAPADD_EXEC="/opt/openldap/bin/ldapadd"

#WORKDIR
WORKDIR=/appli/ldap/init/tmp
```

Passer le script d'initialisation de la racine :

```
/appli/ldap/scripts/initialisation_DIT/initracine.sh
```

Passer le script d'initialisation des porteurs pour chaque porteur de la plateforme :

```
/appli/ldap/scripts/initialisation_DIT/initporteur.sh <porteur>
```

Il faut ensuite modifier les informations liées au porteur dans le ldap, pour cela il faut passer le fichier LDIF suivant :

```
dn: ou=LOCAL,dc=ent,dc=fr
changetype: modify
replace: ENTPorteurMail
ENTPorteurMail: ne-pas-repondre@openENT.com

dn: ou=LOCAL,dc=ent,dc=fr
changetype: modify
replace: ENTPorteurDomainMail
ENTPorteurDomainMail: local.lilie.org

dn: ou=LOCAL,dc=ent,dc=fr
changetype: modify
replace: ENTPorteurUrlAcces
ENTPorteurUrlAcces: https://local.lilie.org/

dn: ou=LOCAL,dc=ent,dc=fr
changetype: modify
replace: ENTPorteurUrlRetourLogout
ENTPorteurUrlRetourLogout: https://local.lilie.org/

dn: ou=LOCAL,dc=ent,dc=fr
changetype: modify
replace: ENTPorteurUrlRetourLogout
ENTPorteurUrlRetourLogout: https://local.lilie.org/portal/c/portal/logout

dn: ou=LOCAL,dc=ent,dc=fr
changetype: modify
replace: ENTPorteurRegexpFile
ENTPorteurRegexpFile: openENT.*
```

Le champs ***ENTPorteurRegexpFile*** *permet de préciser le début des fichiers annuaires pour l'alimentation ldap.*

Puis passer le LDIf avec la requête suivante :

```
/opt/openldap/bin/ldapmodify -h ldap.local.lilie.org:389 -D
"cn=admin,ou=system,dc=ent,dc=fr" -w lilie -f fichier_ldif.ldif
```

3.2 Reprise LDAP

Si vous avez déjà des personnes dans la base annuaire, vous pouvez effectuer la reprise LDAP.

Dézipper bat-repriseldap-**2.2.1**.zip dans /appli/ldap/scripts.

Vérifier le paramétrage dans les fichiers conf.properties et parametres.sh

Le script se lance de la façon suivante :

```
cd /appli/ldap/scripts/bat_repriseldap/
./repriseldap.sh  <paramètres>
```

Paramètres :

1 Ou du porteur dans le LDAP
ex : CRIF
2 Activation de la phase de chargement de la base annuaire dans les tables temporaires
ex : 1
3 Activation de la phase de génération du LDIF
ex : 1
4 Activation de la phase d'import du LDIF sur le LDAP
ex : 1

3.3 Alimentation LDAP

Si vous voulez importer un annuaire, vous pouvez effectuer une alimentation LDAP.
Dézipper bat-alimentationldap-**2.2.1**.zip dans /appli/ldap/scripts.
Vérifier le paramétrage dans les fichiers conf.properties et parametres.sh

Lancer la commande d'import :

```
cd /appli/ldap/scripts/bat-alimentationldap/
./alimldap.sh <paramètres>
```

Paramètres :

-dossier_menesr : Chemin absolue vers les fichiers XML (ex : -dossier_menesr /appli/ldap/scripts/ANNUAIRES/Complet/)
-porteur : Ou du porteur dan le LDAP (ex : -porteur LOCAL)
-academie : Nom de l'académie (ex : -academie Paris)
-import_xml (optionnel) : Etape de l'import des xml en base de travail importannuaire
-generation_ldif (optionnel) : Etape de la génération du LDIF
-import_ldif (optionnel) : Etape de l'import LDIF
-complet : 1 pour complet, 2 pour delta (ex : -complet 1)
-supp_logique (optionnel) : A ajouter pour effectuer l'alimentation avec la suppression logique
-force_xml : Force le traitement des xml même si leur analyse statistique est mauvaise. Par défaut s'il y a un trop grand écart de taille ou de nombre d'entrée avec le complet précédent, l'alimentation sort en erreur. Ce paramètre n'a pas pour vocation à être utiliser dans un mode nominal.
-force_ldif : Force le traitement du ldif même si l'analyse statistique du rapport entrée/supprimé est mauvaise. Par défaut s'il y a un nombre trop grand de personnes supprimé, l'alimentation sort en erreur. Ce paramètre n'a pas pour vocation à être utiliser dans un mode nominal.

NB : Le paramètre académie doit faire partie de la liste des noms d'académies suivantes en respectant la casse :

Aix-Marseille
Nancy-Metz
Amiens
Nantes
Besançon
Nice
Bordeaux
Orléans-Tours
Caen
Paris
Clermont-Ferrand
Poitiers
Corse
Reims
Créteil
Rennes
Dijon
Rouen
Grenoble
Strasbourg
Lille
Toulouse
Limoges
Versailles
Lyon
Agricole
Montpellier
Collectivité
Demo

Le traitement de fusion des données et de génération du fichier « out » à destination du LDAP trace dans le fichier/appli/ldap/scripts/logs/importannuaire.log
Le fichier de log est configurable dans le fichier log4j.xml.

Le traitement rejette des données non conformes ou hors du périmètre.
Ces rejets sont tracés dans le fichier <WORKANNUAIREDIR>/lignesEnErreurLOCAL<Academie>.csv

L'annuaire LDAP peut rejeter des modifications que le programme lui envoie.
Ces rejets sont tracés dans le fichier <WORKANNUAIREDIR>/LDAP_detailLOCAL<ACADEMIE>_<x>.log

WORKANNUAIREDIR est configurable dans le fichier parametres.sh

3.4 Réindexation LDAP

Lancer le script reindexation.sh (présent dans scripts-ldap-**2.2.1**.zip) qui réindex tout (après une reprise ou une alimentation) :

```
./reindexation.sh
```

3.5 Export LDAP pour eliot_scolarite

Pour alimenter la base de données eliot_scolarite, il est nécéssaire d'effectuer plusieurs opération. La première consiste à exporter des données LDAP.

Dézipper bat-exportannuaire-ldap-**2.2.1**.zip dans /appli/ldap/scripts.
Vérifier le paramétrage dans le fichier parametres.sh

Lancer la commande :

```
cd /appli/ldap/scripts/bat-exportannuaire-ldap
./principal_export.sh /appli/ldap/scripts/bat-exportannuaire-ldap/tmp LOCAL_ 201309110000
LOCAL -tousadm
```

Paramètres :

Param1 : REPERTOIRE DE SORTIE DES FICHIERS

Param2 : PREFIXE DES FICHIERS

Param3 : Date de debut de recherhce dans l'annuaire (AAAAMMJJHHMM)

Param4 : Code PORTEUR

option : -tousadm = export de tous les administrateurs, et de tous les adminstrateurs locaux sans utiliser la date de recherche

3.6 Connecteur LDIF

Pour alimenter la base de données eliot_scolarite, il est nécéssaire d'effectuer plusieurs opération. La deuxième consiste à importer le LDIF dans des tables temporaires.

Dézipper bat-connecteurldif-**2.2.1**.zip dans /appli/ldap/scripts.
Vérifier le paramétrage dans le fichier config/config_eliot-connecteur-ldif.properties

Lancer la commande :

```
cd /appli/ldap/scripts/bat-connecteur-ldif/bin
./eliot-connecteur-ldif.sh /appli/ldap/scripts/bat-exportannuaire-ldap/tmp/LOCAL_*COMPLET.ldif LOCAL
```

Paramètres :

Param1 : chemin du fichier LDIF à traiter
Param2 : code porteur correspondant au fichier LDIF à traiter

3.7 Annuaire Interface

Pour alimenter la base de données eliot_scolarite, il est nécéssaire d'effectuer plusieurs opération. La dernière consiste à importer dans la base eliot_scolarite depuis les tables temporaires.

Dézipper bat-annuaire-interface-**2.2.1**.zip dans /appli/ldap/scripts.
Vérifier le paramétrage dans le fichier config/config_eliot-annuaire-interface.groovy

Cependant pour que l'annuaire ne rajoute pas le porteur les établissements, il faut les ajouter dans les tables ent.porteur_ent et ent.etablissement dans la database eliot_scolarité.

Voici les requêtes :

REQUETE PORTEUR :

```
INSERT INTO ent.porteur_ent VALUES (1,'code_porteur','nom_porteur','nom_porteur','ne-pas-repondre@domaine.fr','https://url_deconnexion','https://url_connexion',true,null,null,2,true);
```

REQUETE ETABLISSEMENTS

```
INSERT INTO ent.etablissement VALUES
(22,2,'nom_etablissement',1,'uai','code_porteur',id_porteur,null,'type_etablissement','ministere_tutelle','academie',true,null,null,2,true,'adresse',null,'code_postal','ville');
INSERT INTO ent.preference_etablissement VALUES
(1,id_etablissement,5,3,0,'nom_etablissement','','','','','','',false,'',1,'',false,true,'STS',true);
```

Voici un exemple des requêtes :

```
psql -d eliot_scolarite
INSERT INTO ent.porteur_ent VALUES (1,'LOCAL','LOCAL','LOCAL','ne-pasrepondre@local.ent.fr','https://local.lilie.org/portal/logout','https://local.lilie.org',true,null,null,(SELECT  demande_import_id from annuaire_interface.etablissement LIMIT 1),true);
```

```
INSERT INTO ent.etablissement VALUES (22,2,'CLG CAMILLE
JADE',1,'0750004N',1,null,'COLLEGE','MINISTERE DE L EDUCATION
NATIONALE','Paris',true,null,null,(SELECT  demande_import_id from
annuaire_interface.etablissement LIMIT 1),true,'25 BIS RUE SALOME',null,'75007','PARIS');
INSERT INTO ent.preference_etablissement VALUES (1,22,5,3,0,'LGT JEREMY
ROLAND','','','','','','',false,'',1,'',false,true,'STS',true);

[... Pour chaque établissement...]
```

Lancer la commande :

```
cd /appli/ldap/scripts/bat-annuaire-interface/bin
./annuaire-importe-tous.sh
```

3.8 Génération des codes d'activation parents

Pour générer les codes d'activation des parents dans le LDAP, il est nécéssaire de lancer un script.
Dézipper gen_code_activation-**2.2.1**.zip dans /appli/ldap/scripts

Il faut tout d'abord installer la librairie perl net::LDAP :

```
cpan net::ldap
```

Puis lancer le script :

```
cd /appli/ldap/scripts/gen_code_activation/
./gen_code_activation_cron.pl -h ldap.local.lilie.org:389 -D cn=admin,ou=system,dc=ent,dc=fr
-w lilie -p LOCAL
```

3.9 Importation des fichiers pour la gestion de la scolarité de l'ENT

Afin de faciliter le travail installation et effectuer des tests, un jeu d'essai anonymisé est mis à disposition dans le fichier **openENT-import-services-structures.zip** avec des fichiers XML permettant d'alimenter des emplois du temps et la création automatique des cahiers de textes classe et des agendas scolaires.

Ces fichiers correspondent au chargement d'annuaire des établissements à partir du répertoire suivant : **openENT-annuaire-version-AAF-VE1102.**

Les fichiers nécessaires à l'importation sont :

- **STS_emp_<n° établissement>_<Année scolaire>.xml** : issu de STS_WEB
- **emp_STS_<n° établissement>_<Année scolaire>.xml** : issu du logiciel d'emploi du temps.

Déposer les fichiers pour la gestion de scolarité de l'ENT à partir du menu « vie scolaire » (Cf. manuel utilisateur).

Il est également possible d'utiliser des fichiers UDT (non fournis) pour la gestion de la scolarité. Pour cela il est nécéssaire de dézipper l'archive **lilie-connecteur-udt-2.2.1.zip** dans /appli/batch/ et de rendre exécutable le fichier shell.

Il faut également passer la requête suivante sur la base eliot_scolarite :

```
update ent.preference_etablissement set import_udt_manuel_actif = true;
```