

Intégrer un annuaire LDAP sur le serveur AbulÉdu

Installer slapd

```
sudo apt-get install slapd ldap-utils
```

Configurer slapd

Fichier /etc/ldap/slapd.conf

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

#####
# Global Directives:

# Features to permit
#allow bind_v2

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

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck  on

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

# List of arguments that were passed to the server
argsfile     /var/run/slapd.args

# Read slapd.conf(5) for possible values
loglevel     0

# Where the dynamically loaded modules are stored
modulepath   /usr/lib/ldap
moduleload   back_bdb

#####
```

```
# SSL:
# Uncomment the following lines to enable SSL and use the default
# snakeoil certificates.
#TLSCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
#TLSCertificateKeyFile    /etc/ssl/private/ssl-cert-snakeoil.key

#####
# Specific Backend Directives for bdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend      bdb
checkpoint  512 30

#####
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
#backend      <other>

#####
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this database until another
# 'database' directive occurs
database      bdb

# The base of your directory in database #1
suffix        "dc=abuledu,dc=info"

rootdn        "cn=admin,dc=abuledu,dc=info"
rootpw        "password"

# Where the database file are physically stored for database #1
directory     "/var/lib/ldap"

# Indexing options for database #1
index          objectClass eq

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

# Where to store the replica logs for database #1
# replogfile    /var/lib/ldap/replog

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attrs=userPassword
    by dn="cn=admin,dc=abuledu,dc=info" write
```

```

    by anonymous auth
    by self write
    by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms. Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read
# defaultaccess read
# The admin dn has full write access, everyone else
# can read everything.
access to *
    by dn="cn=admin,dc=abuledu,dc=info" write
    by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
#access to dn=".*,ou=Roaming,o=morsnet"
#    by dn="cn=admin,dc=nodomain" write
#    by dnattr=owner write

#####
# Specific Directives for database #2, of type 'other' (can be bdb too):
# Database specific directives apply to this database until another
# 'database' directive occurs
#database          <other>

# The base of your directory for database #2
#suffix            "dc=debian,dc=org"

```

Reconstruire slapd

```

/etc/init.d/slapd stop
rm /var/lib/ldap/*

```

Fichier de base

/tmp/abuledu.ldiff

```

dn: dc=abuledu,dc=info
objectClass: top

```

```
objectClass: dcObject
objectClass: organization
o: abuledu
dc: abuledu
structuralObjectClass: organization
entryUUID: a73871a0-f82a-102c-8532-efbd96efb5ab
creatorsName: cn=anonymous
modifiersName: cn=anonymous
createTimestamp: 20080806174132Z
modifyTimestamp: 20080806174132Z
entryCSN: 20080806174132Z#000001#00#000000

dn: cn=admin,dc=abuledu,dc=info
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: azaz
structuralObjectClass: organizationalRole
entryUUID: a74cdb5e-f82a-102c-8533-efbd96efb5ab
creatorsName: cn=anonymous
modifiersName: cn=anonymous
createTimestamp: 20080806174132Z
modifyTimestamp: 20080806174132Z
entryCSN: 20080806174132Z#000002#00#000000

dn: ou=utilisateurs,dc=abuledu,dc=info
objectClass: top
objectClass: organizationalUnit
ou: utilisateurs
description: Branche de l'annuaire pour les utilisateurs
```

Ajouter ce fichier dans l'annuaire pour constituer sa racine

```
slapadd -l /tmp/abuledu.ldiff
slapindex
slapcat -> vérification
```

Ajouter des entrées

Fichier de test.ldiff

```
dn: uid=eric.seigne,ou=utilisateurs,dc=abuledu,dc=info
objectClass: account
objectClass: posixAccount
cn: Eric Seigne
uid: eric.seigne
uidNumber: 10001
```

```
gidNumber: 1024
homeDirectory: /home/eleves/eric.seigne
userPassword: azaz
loginShell: /bin/sh
gecos: eric.seigne
description: eric.seigne
```

Tentative d'import dans la base:

```
ldapadd -W -D "cn=admin,dc=abuledu,dc=info" -x -H ldap://localhost -f
/tmp/test.ldiff
```

Vérification avec slapcat puis ldapsearch

```
ldapsearch -x -H ldap://localhost -b "dc=abuledu,dc=info" "(uid=eric*)"
```

Pour l'instant l'annuaire LDAP est utilisé sur des serveurs AbulÉdu pour gérer un annuaire "classique" mais pas des utilisateurs locaux. Dans un avenir il est probable que la gestion des utilisateurs bascule directement sur l'annuaire et nous permettra ainsi de ne plus avoir de problèmes à ce niveau là.

From:
<https://docs.abuledu.org/> - **La documentation d'AbulÉdu**

Permanent link:
https://docs.abuledu.org/abuledu/developpeur/annuaire_ldap?rev=1218048395

Last update: **2008/08/06 20:46**

