Ldap et lc_ldap

BUT DU SEMINAIRE

- Comprendre comment fonctionne un annuaire ldap
- Comprendre son utilisation au Crans, et configurer un ldap
- Lc_ldap, binding python pour ldap au Crans

LDAP

```
dc=org
  |
dc=example
/       \
ou=people    ou=groups
  |
uid=toto
```

Lightweight Directory Access Protocol

Un annuaire

domain components ou **dc=**

organizational units ou **ou=**

common name ou **cn=**

etc

LDAP

2 sections dans l'arbre : dc=org, et dc=config

Les données sont stockées dans l'arbre principal; l'arbre config contient la configuration, les objets et attributs

Des noeuds et des branches… (voir démo)

LDAP

```
                    dc=crans,dc=org (racine)
                    /          |           \
               ou=data   ou=Group        ou=services
               /     \     |              /        \
          aid=3775 mid=1  cn=adm       cn=dns     cn=autostatus
```

Exemple au Crans

Les adhérents sont stockés dans ou=data, (aid=xxx), ainsi que les clubs (cid=xxx)

Les machines et factures sont stockées dans les noeuds adhérents (mid=xxx) et fid=(xxx)

```
ou=data,~ > cd aid=5081
aid=5081,ou=data,~ > ls
fid=1294
fid=2289
fid=2395
fid=2482
fid=2483
fid=2486
fid=2541
fid=2793
fid=4558
fid=5434
fid=890
mid=10098
mid=10104
mid=10278
mid=10673
mid=14297
```

LDAP EN DÉTAIL

Un adhérent Crans :

```
dn: aid=5081,ou=data,dc=crans,dc=org
objectClass: adherent
objectClass: cransAccount
objectClass: posixAccount
objectClass: shadowAccount
aid: 5081
blacklist:: MTQxODY4OTA4MCQxNDE4NjkwMDU1JHVwbG9hZCRkZXRyYXogOiBKZSB0ZXN0ZSBsYSBkw6ljb25uZXhpb24=
blacklist: 1435879320$1435879656$upload$detraz : dstan : upload de moche detraz: abus de droits
canonicalAlias: Gabriel.Detraz@crans.org
charteMA: TRUE
chbre: G418
cn: Gabriel Detraz
compteWiki: Chirac
contourneGreylist: OK
controle: cp
debutAdhesion: 20140829122231+0200
debutAdhesion: 20150830123923+0200
debutAdhesion: 20160831144947+0200
debutConnexion: 20140829122240+0200
debutConnexion: 20150830123934+0200
debutConnexion: 20170831144947+0200
derniereConnexion: 1480902847
droits: Nounou
droits: Bureau
droits: Imprimeur
droits: Cableur
droits: Webmaster
etudes: ENS
```

dn

object class

autres attributs

LE SCHEMA

Regardons le schéma :

```
dn: cn={6}crans,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: {6}crans
structuralObjectClass: olcSchemaConfig
entryUUID: bc6027e6-fee6-1030-9a80-9d8b15437de3
creatorsName: cn=config
createTimestamp: 20120310102251Z
olcObjectClasses: {0}( 1.3.6.1.4.1.25368.3.1 NAME 'proprio' DESC 'Proprietai
 re (classe abstraite)' SUP top ABSTRACT MUST ( nom $ chbre ) MAY ( paiement
  $ info $ blacklist $ controle $ historique $ preferedLanguage $ debutAdhes
 ion $ finAdhesion $ debutConnexion $ finConnexion ) )
olcObjectClasses: {1}( 1.3.6.1.4.1.25368.3.2 NAME 'adherent' DESC 'Adherent'
  SUP proprio STRUCTURAL MUST ( aid $ prenom $ tel $ mail ) MAY ( etudes $ p
 ostalAddress $ mailInvalide $ charteMA $ adherentPayant $ carteRFID ) )
olcObjectClasses: {2}( 1.3.6.1.4.1.25368.3.3 NAME 'club' DESC 'Club' SUP pro
 prio STRUCTURAL MUST ( cid $ responsable ) MAY ( imprimeurClub $ accesRFID
 ) )
olcObjectClasses: {3}( 1.3.6.1.4.1.25368.3.10 NAME 'machine' DESC 'Machine (
 classe abstraite)' SUP top ABSTRACT MUST ( mid $ macAddress $ host ) MAY (
 ipHostNumber $ ip6HostNumber $ rid $ info $ blacklist $ hostAlias $ exempt
 $ portTCPin $ portTCPout $ portUDPin $ portUDPout $ dnsIpv6 $ machineAlias
 $ sshFingerprint $ historique ) )
olcObjectClasses: {4}( 1.3.6.1.4.1.25368.3.11 NAME 'machineCrans' DESC 'Mach
 ine appartenant au Crans' SUP machine STRUCTURAL MAY ( prise $ nombrePrises
  $ statut ) )
olcObjectClasses: {5}( 1.3.6.1.4.1.25368.3.12 NAME 'borneWifi' DESC 'Borne w
 ifi' SUP machine STRUCTURAL MUST ( canal $ puissance ) MAY ( prise $ positi
 onBorne $ pontwifi $ statut $ hotspot ) )
olcObjectClasses: {6}( 1.3.6.1.4.1.25368.3.13 NAME 'machineWifi' DESC 'Machi
 ne wifi' SUP machine STRUCTURAL MUST ipsec )
olcObjectClasses: {7}( 1.3.6.1.4.1.25368.3.14 NAME 'machineFixe' DESC 'Machi
 ne adherent fixe' SUP machine STRUCTURAL )
olcObjectClasses: {8}( 1.3.6.1.4.1.25368.3.20 NAME 'cransAccount' DESC 'Comp
 te  Crans' SUP top AUXILIARY MAY ( mailAlias $ canonicalAlias $ droits $ so
 lde $    contourneGreylist $ rewriteMailHeaders $ derniereConnexion $ homep
 ageAlias $    compteWiki $ mailExt $ gpgFingerprint $ gpgMail ) )
```

Classes structurelles

Classes auxiliaires

LE SCHEMA

Et les attributs

```
olcAttributeTypes: {0}( 1.3.6.1.4.1.25368.2.2 NAME 'nom' DESC 'Nom adherent'
  SUP name )
olcAttributeTypes: {1}( 1.3.6.1.4.1.25368.2.3 NAME 'prenom' DESC 'Prenom adh
 erent' SUP name )
olcAttributeTypes: {2}( 1.3.6.1.4.1.25368.2.4 NAME 'tel' DESC 'Numero de tel
 ephone adherent' EQUALITY telephoneNumberMatch SUBSTR telephoneNumberSubstr
 ingsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.50 )
olcAttributeTypes: {3}( 1.3.6.1.4.1.25368.2.5 NAME 'paiement' DESC 'Annee de
  paiement adherent' EQUALITY integerMatch ORDERING integerOrderingMatch SYN
 TAX 1.3.6.1.4.1.1466.115.121.1.27 )
olcAttributeTypes: {4}( 1.3.6.1.4.1.25368.2.7 NAME 'mailAlias' DESC 'Alias m
 ail' EQUALITY caseIgnoreIA5Match SUBSTR caseIgnoreIA5SubstringsMatch SYNTAX
  1.3.6.1.4.1.1466.115.121.1.26{256} )
olcAttributeTypes: {5}( 1.3.6.1.4.1.25368.2.8 NAME 'canonicalAlias' DESC 'Al
 ias mail canonique' EQUALITY caseIgnoreIA5Match SUBSTR caseIgnoreIA5Substri
 ngsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256} )
olcAttributeTypes: {6}( 1.3.6.1.4.1.25368.2.9 NAME 'etudes' DESC 'Etudes adh
 erent' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3
 .6.1.4.1.1466.115.121.1.15{1024} SINGLE-VALUE )
olcAttributeTypes: {7}( 1.3.6.1.4.1.25368.2.10 NAME 'chbre' DESC 'Chambre ad
 herent' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.
 3.6.1.4.1.1466.115.121.1.44{16} SINGLE-VALUE )
olcAttributeTypes: {8}( 1.3.6.1.4.1.25368.2.11 NAME 'historique' DESC 'Histo
 rique de modifications' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstring
 sMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{2048} )
olcAttributeTypes: {9}( 1.3.6.1.4.1.25368.2.12 NAME 'droits' DESC 'Droits ad
 herent' EQUALITY caseIgnoreMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{64} )
olcAttributeTypes: {10}( 1.3.6.1.4.1.25368.2.13 NAME 'ipsec' DESC 'Clef IPse
 c machine' EQUALITY caseIgnoreMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{64
 } )
```

LES ATTRIBUTS LDAP EN DETAIL

Des attributs monovalués et multivalués

```
mailAlias: stupidon@crans.org
mailAlias: chirac@crans.org
mailAlias: presidentchirac@crans.org
mailAlias: raleur@crans.org
mailAlias: plopus@crans.org
mailAlias: projet-saclay@crans.org
```

LES OUTILS DU LDAP

Shelldap

apt-get install shelldap

TP : Ecrire un .shelldap.rc (sur vo, base de test)

```
`---> cat .shelldap.Rc
zsh: correct '.shelldap.Rc' to '.shelldap.rc' [nyae]? y
---
basedn: cn=config
#basedn: dc=crans,dc=org
binddn: cn=admin,dc=crans,dc=org
# Test
bindpass: 75bdb64f32
cacheage: 300
server: localhost
timeout: 10
```

PROBLEMES : PARLER AU LDAP DANS DES SCRIPTS

```
In [2]: import sys

In [3]: sys.path.append('/usr/scripts')

In [4]: from lc_ldap import shortcuts

In [5]: ldap = shortcuts.lc_ldap_admin()

In [6]: adh = ldap.search('aid=5081')
/usr/bin/ipython:1: DeprecationWarning: search ne devrait utiliser que des unicode comme filtre('aid=5081')
  #! /usr/bin/python

In [7]: adh = adh[0]

In [8]: adh
Out[8]: u'Adh\xe9rent : Gabriel Detraz'

In [9]: adh['nom']
Out[9]: [<class 'lc_ldap.attributs.nom'> : u'Detraz']
```

PROBLEMES : PARLER AU LDAP DANS DES SCRIPTS

```
In [2]: import sys

In [3]: sys.path.append('/usr/scripts')

In [4]: from lc_ldap import shortcuts

In [5]: ldap = shortcuts.lc_ldap_admin()

In [6]: adh = ldap.search('aid=5081')
/usr/bin/ipython:1: DeprecationWarning: search ne devrait utiliser que des unicode comme filtre('aid=
  #! /usr/bin/python

In [7]: adh = adh[0]

In [8]: adh
Out[8]: u'Adh\xe9rent : Gabriel Detraz'

In [9]: adh['nom']
Out[9]: [<class 'lc_ldap.attributs.nom'> : u'Detraz']
```

TP

Aller sur vo

Lancer un shell ipython et ouvrir une connexion ldap (from lc_ldap import ...) avec lc_ldap_test

Chercher l'ensemble des adhérents du crans. (aid=*).... quel problème observe-t-on ?

Cherchez et afficher la chambre de l'aid 5081

LES FILTRES DE RECHERCHE

Un filtre de recherche ldap :

exemple (&(aid=5081)(!(chbre=G420))) : et des 2 conditions

(|(aid=5081)(aid=5082)) renvoie aid 5081 ou aid 5082

TP

Dans le shell python, lancer la recherche des bornes wifi dont l'attribut statut vaut TRUE

Combien de résultats ?

LES ECRITURES

Il faut ouvrir une connexion, avec l'argument optionnel mode='rw'...

adh = ldap.search(u'(aid=5081)', mode='rw')

TP

Changer le nom de toto passoir (aid=4281) en passouare …