LDAP : pour quels besoins ?

Authentification centralisée *(même identifiant/mot de passe pour l'accès à différents services) :*

- POP(S), IMAP(S), SMTPS
- SSO-CAS (Portail Intranet...)
- Accès à d'autres sites Lille 1
- WiFi (radius), VPN...

Relayage messagerie, alias (listes sympa), redirections d'adresses e-mail...

Pages blanches (synchronisation avec l'autocom).

LDAP : pour quelles populations ?

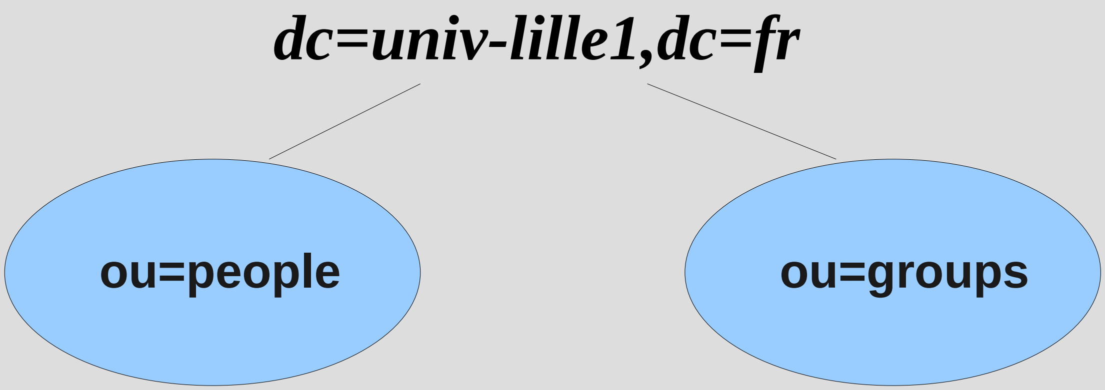
Etudiants : importés depuis le fichier de scolarité.

Personnels : titulaires, contractuels, hébergés (cnrs, inria, autres établissements...), entrés par les correspondants dans les structures (outil portail). Post-synchronisation avec Harpège.

Invités, *stagiaires*, *vacataires*, *extérieurs :* entrés par les correspondants des structures ou par des personnes habilitées (outil portail).

LDAP : organisation

Modèle d'annuaire à plat (recommandations nationales SUPANN) : bien adapté pour faire de l'authentification.



dn: uid=dupont,ou=people,dc=univ-lille1,dc=fr
...

dn: cn=LABO,ou=groups,dc=univ-lille1,dc=fr
...

LDAP : organisation

dn: uid=mdupont,ou=people,dc=univ-lille1,dc=fr
objectClass: person
  cn: Dupont Martin
  telephoneNumber: +33 3 20 43 43 43
  uid: mdupont
  userPassword:: XXXXXXX
objectClass: posixAccount
  uidNumber: 1111
  gidNumber: 222
  homeDirectory: /home/mdupont
  loginShell: /bin/false
objectClass: radiusProfile
  radiusGroupName: personnel
objectClass: inetLocalMailRecipient
  mailLocalAddress: Martin.Dupont@univ-lille1.fr
  mailRoutingAddress: mdupont@serveur1.univ-lille1.fr
objectClass: ustlPerson
  ustlZoneDns: 134.206.200.0/24
  ustlrole: DNS-users

LDAP : organisation, configuration

2 serveurs annuaires d'établissement identiques, virtualisés (VMware).

Logiciel libre « openldap ».

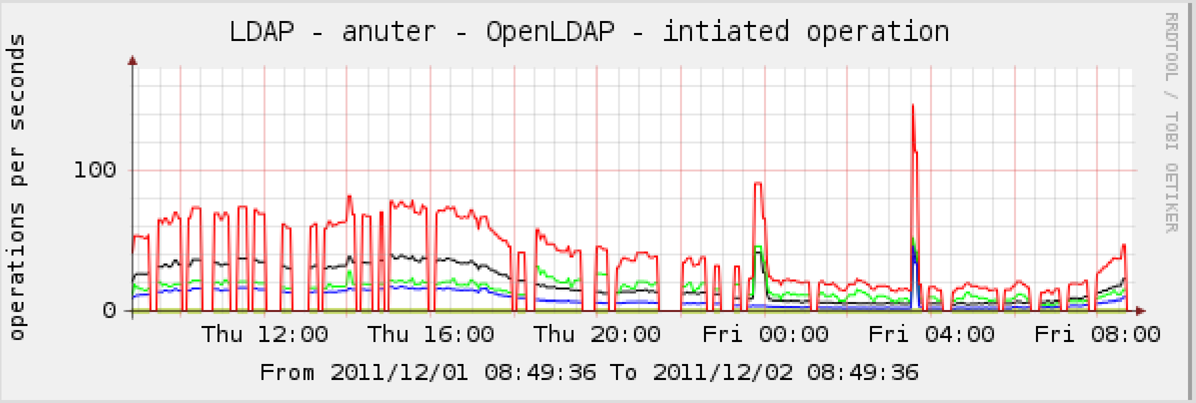
Répartition de charge.

Indexer les attributs très sollicités pour de bons temps de réponse (relayage messagerie...)

Université Lille1
Sciences et Technologies

LDAP : performances

Surveillance journalière par Cacti (greffon ldap) :



Détecter les anomalies dans les logs : applications gourmandes, requêtes mal construites...

Scripts de scrutation de log (adresses IP, types de requête..)

Université Lille1 Sciences et Technologies

LDAP : surveillance, sauvegardes

Surveillance NAGIOS : cas ou le daemon *slapd* est présent mais ne répond plus aux requêtes. Dégrade le service car les applications ne basculent pas sur le second annuaire.

Sauvegardes sous forme de fichiers .LDIF (dump annuaire) plus d'une fois par jour.

LDAP : sécurisation

Niveau 1 : protocole LDAP non accessible de l'extérieur (politique de l'établissement).

Niveau 2 : contrôle par *iptable* des accès. Seul le réseau de service a accès par défaut aux annuaires. Accès LDAPS préconisé pour les serveurs des autres structures qui doivent accéder aux annuaires.

Université Lille1 Sciences et Technologies

LDAP : sécurisation

Niveau 3, ACLs LDAP : authentification par comptes 'admin' particuliers pour récupérer des attributs sensibles, effectuer des modifications... :

access to attr=ustlRole
by dn= 'uid=portail-lille1,ou=admins,dc=univ-lille1,dc=fr' write
by dn= 'uid=portail-lille1,ou=admins,dc=univ-lille1,dc=fr' read
by * none

Attention aux performances !

Université Lille1 Sciences et Technologies

LDAP : authentification de salles

N'est pas faite sur les deux annuaires d'établissement pour deux raisons :

Trop de requêtes (cache *nscd* à installer sur les clients Linux) => risque important de crash annuaire, peut impacter sur les performances.

Trop d'IPs clients à autoriser, dégrade sensiblement le niveau de sécurité.

LDAP : authentification de salles

Salles équipées en postes Linux :

Mise en place au CRI d'un annuaire spécifique ouvert ne contenant que des entrées banalisées d'étudiants (attributs non sensibles), alimenté automatiquement depuis l'annuaire d'établissement (mécanisme *syncrepl* de réplication partielle).

Protection spécifique par ACLs LDAP.

LDAP : authentification de salles

Salles équipées en postes Windows

Mise en place d'annuaires spécifiques gérés par des gestionnaires de parc dont les entrées seront importées depuis l'annuaire d'établissement :

- Annuaires openldap avec serveur Samba et déclarations des postes clients.
- Annuaires Active Directory (script journalier d'importations...)

Université Lille1 Sciences et Technologies

LDAP : réplication

Mécanisme *syncrepl* :

- Maître, esclave(s) (actif, passif),
- N-Way Multi-Master (actif, actif),
- Mirroring (actif, actif),
- Standalone LDAP Proxy,
- Réplication partielle...

Requêtes 'refreshOnly' (polling) ou 'refreshAndPersist' (listening).

LDAP : réplication

Réplication partielle :

```
provider=ldap://ldap-write.univ-lille1.fr
searchbase='ou=people,dc=univ-lille1,dc=fr'
attrs='uid, cn, sn, givenName, homeDirectory, loginShell...'
filter='(&(objectClass=ustlEtuPerson)(objectClass=posixAccount)
   (ustlCurrentYear=TRUE))'
```

Mise en place prochaine d'un annuaire PRES 'pages blanches' qui utilisera ce mécanisme pour s'alimenter.

Université Lille1 Sciences et Technologies