

LDAP

Saint-Graal de l'administrateur système

Fabrice Lorrain (Fabrice.Lorrain@univ-mlv.fr)

Centre de Ressources Informatiques
Université de Marne-la-Vallée



PLAN

- • LDAP : définition
- • Quelle utilisation dans un campus
- • LDAP appliqué : l'authentification système
- • LDAP à l'UMLV
- • Conclusion

LDAP : protocole

- Lightweight Directory Access Protocol
- Protocole de communication public et normé IETF
- Architecture client/serveur
- Distribution/répliquatation des serveurs (répliquat)
- Délégation d'une branche de l'arbre (referral)
- Sécurisé (acl, sasl)

LDAP : support de contenu

- Structure hiérarchique, arborescente
- Optimisé pour lecture
- Très bonne tenue en montée en charge
- Squelette de l'infrastructure
- Habillé par les schémas

LDAP : schémas

- Définition des données stockées
- OID (Object IDentifier) et attributs
- Sous forme de “pluggins”
- Orienté objet : héritage
- Enormement de schémas prédéfinis
- Avec possibilité de définir ses propres schémas
- C'est l'enveloppe de LDAP

LDAP : les données

- C'est la chaire de l'infrastructure
- De type informatif (nom, prénom, localisation ...)
- Ou technique (mot de passe, gid ...)
- Textuelle ou binaire (trombinoscope ...)
- LDIF : format text d'échange des données

LDAP : la cuisine

- Les couches clientes bas niveau, ie système (libc, nss, pam, Active Directory)
- Les utilitaires ligne de commande unix (ldap*)
- Les interfaces graphiques gq, webmin, mozilla
- Les API de programmation (perl, python, java, C etc...)

Références sur LDAP (protocole)

- RFC/OID : www.cru.fr/ldap
- Page personnelle de Laurent Mirtain :
www-sop.inria.fr/semir/personnel/Laurent.Mirtain/LDAP.html
- OpenLDAP : www.openldap.org
- Microsoft Active Directory :
<http://www.microsoft.com/windows2000/technologies/directory/ad/default.as>
- Netscape ?
- Base de schémas : <http://ldap.akbkhhome.com>

LDAP mais pour quoi faire ?

(contenu)

- Annuaire pages blanches classique ...
- Et plus évolué (accessible depuis clients mails ...)
- Support intranet (authentification, contenu)
- Infrastructure du Système d'Information (SI)

LDAP mais pour quoi faire ?

(authentification)

- Support messagerie (authentification webmail)
- Support pour la FOAD (gestion des utilisateurs)
- Base à tout faire (gestion utilisateur, gestion des ACL, information materiel etc....)
- Authentification système

LDAP mais pour quoi faire ?

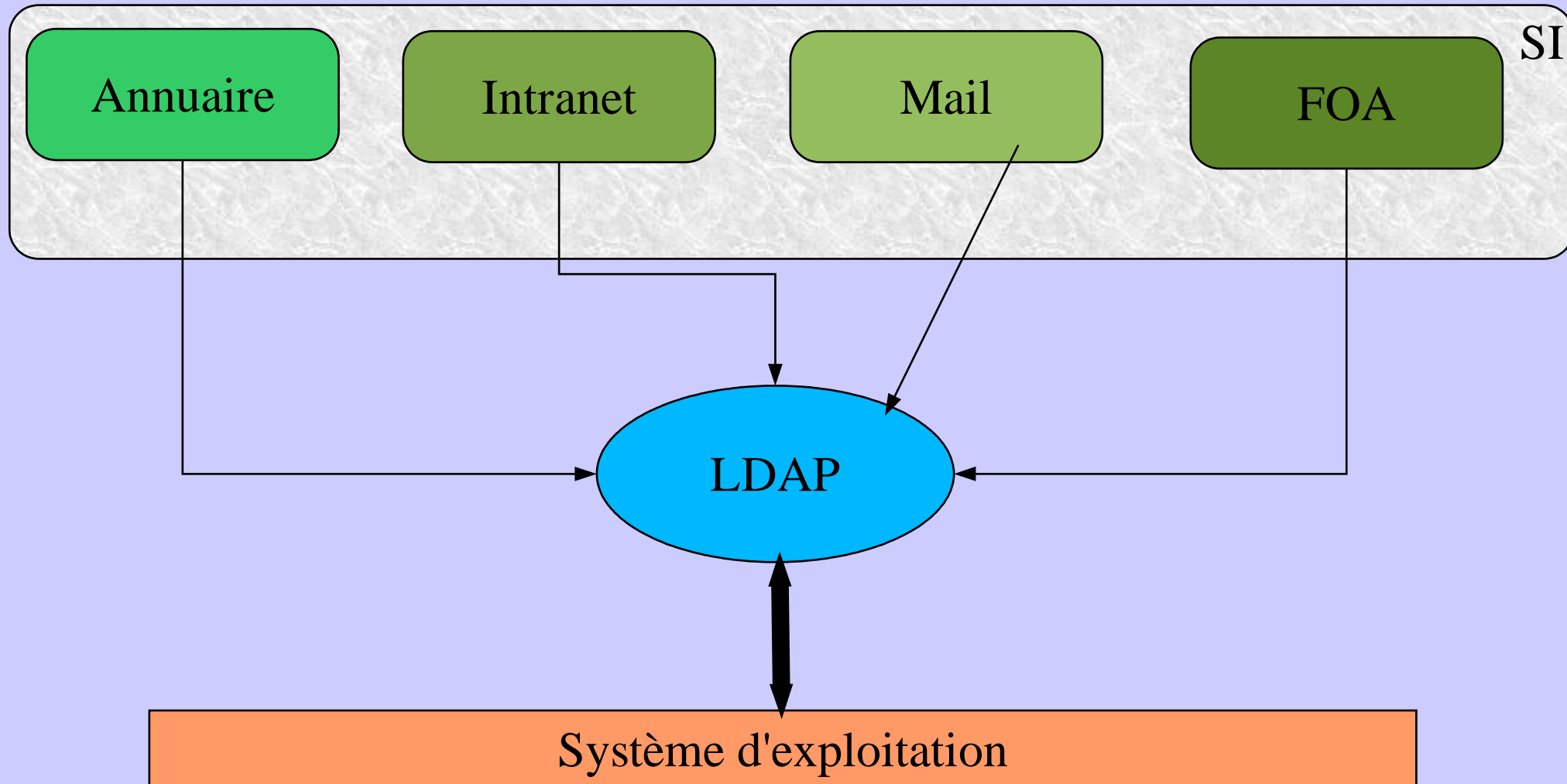
(authentification avec steroids)

- Infrastructure de gestion de clefs (IGC)
- Single Sign On (SSO)
- Authentification utilisateur/matériel (802.1x)

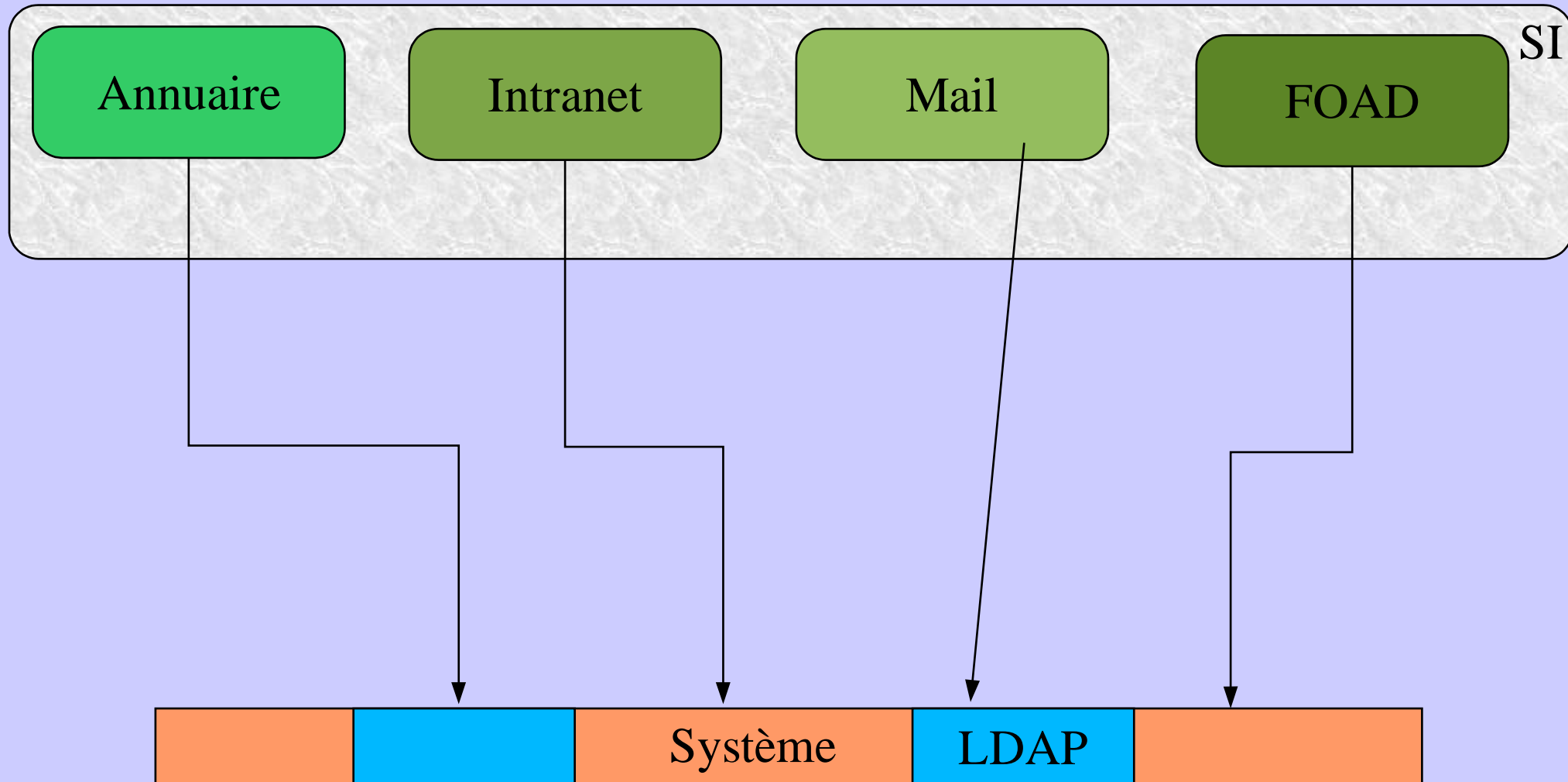
Références sur LDAP (utilisation)

- CRU : www.cru.fr/ldap
- Groupe de travail SUPANN :
<http://www.cru.fr/ldap/supann>
- ATICA : <http://www.atica.pm.gouv.fr/index.php>
- Annuaire LDAP de Nancy 2 :
<http://docs.univ-nancy2.fr/ldap>
- Actes de JRES 1999 et 2001 (
<http://www.jres.org/Archives/JRES2001/jres2001CD.pdf>)

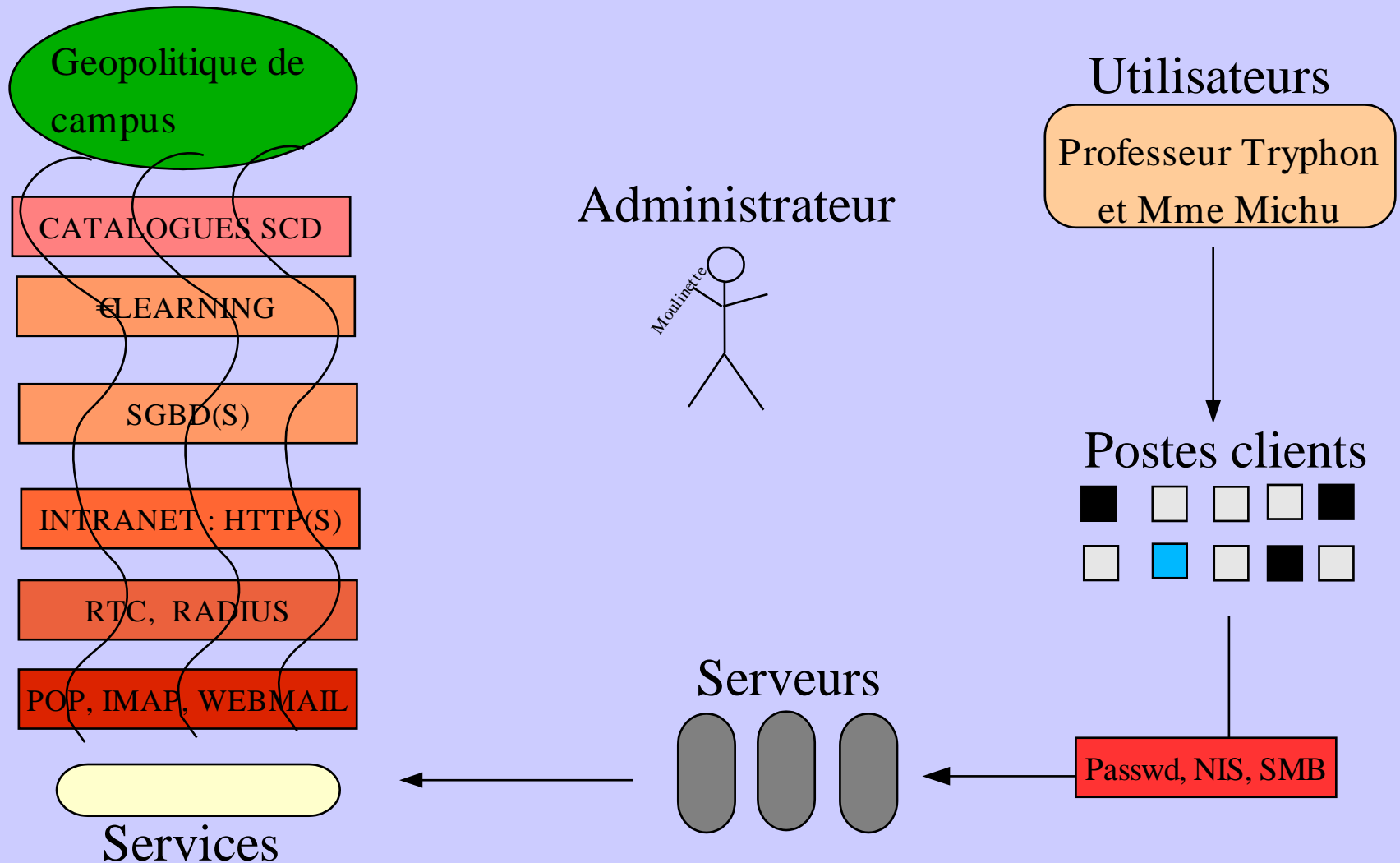
De LDAP support d'infrastructure



A LDAP brique système



L'enfer de l'authentification ...



Est fortement simplifiable avec LDAP

- Regrouper les bases d'authentification
- Protocole d'authentification unique
- Suppression/diminution des passerelles et autres moulinettes
- Passer d'une authentification locale à une authentification globale
- Tout en conservant la structure existante
- Simplification de la structure système

Mieux répondre aux besoins à venir

- Permet d'apporter un service transverse
- Et de créer une brique de base pour un Système d'Information de campus
- Tant au niveau administratif
- Qu'au niveau pédagogique

Les contraintes systèmes

- Le système d'exploitation doit causer LDAP
 - Linux (nsswitch + pam)
 - MS windows (> w2k)
 - Mac OS 10.2 ?
 - Solaris et HPUX
- Ou existence de passerelles (samba 2.2.x)
- Attention à la charge induite sur les serveurs LDAP.

Ainsi que tous les autres services

- Les protocoles nécessitant une authentification (pop, imap, http)
- Comment ceux nécessitant de vérifier l'existence d'un login (SMTP)
- Aujourd'hui, la quasi totalité des services supportent LDAP.

Quel serveur LDAP ?

- Novel NDS
- Sun Iplanet
- Oracle
- Microsoft Active Directory
- OpenLdap (logiciel Libre) <--- celui-ci est bien

Références sur LDAP (implémentation)

- Doc de Jehan Procaccia (MAJ 13/03/2003):
<http://www.int-evry.fr/mci/user/procacci/ldap/index.html>
- LDAP* Howto :
<http://www.tldp.org/HOWTO/LDAP-HOWTO>
- Article de Linux Magazine n° 40 (Juin 2002),
Authentification basée sur LDAP, de S. Twardy
(CRI Université Toulon-Var)
- Liste de diffusion nationale :
<http://listes.cru.fr/wws/info/ldap-fr>

UMLV : contexte pédagogique

- environ 10000 étudiants en 2003
- autour de 900 postes
- environnement MS (NT4, W2k, ~ 600 postes)
- environnement linux (debian, ~300 postes)
- 4 serveurs de comptes (espace disque)
- tout étudiant à un login fournit aux inscriptions

UMLV : avant 2002

- 1 master NIS et 3 slaves
- 4 serveurs samba avec des domaines différents
- extraction des informations de login depuis Apogee
- script perl maison de création/modification des fichiers smbpasswd/nispasswd
- synchronisation des fichiers au travers de tunnels ssh.

UMLV : depuis rentrée 2002

- Un serveur LDAP principal et 3 répliquats
- un PDC samba unique et 3 serveurs samba d'espace disque
- un script perl de création/modification de compte “ldapisé”
- et une base d'authentification unique...

les choix techniques

- utilisation d'openLDAP
- un schéma à plat plutôt que hiérarchique
- utilisation des schémas standards
- une sous branche étudiante unique :
 - ou=Etudiant,dc=univ-mlv.fr,dc=fr
- avec trois entrées :
 - ou=Users, ou=Samba, ou=Groups

Configuration du serveur

- installation d'openLDAP 2.1 (.tgz, .deb, .rpm, etc...)
- configuration dans /etc/ldap/slapd.conf
 - inclusion des schemas
 - définition du mot de passe administrateur
 - définition des ACL d'accès de base (en particuliers aux champs passwd)
 - déclaration des répliquats (démon slurpd)

du poste client

- configuration de NSS
 - installation de la librairie libnss_ldap
 - /etc/nsswitch.conf
 - /etc/libnss_ldap.conf
- configuration de PAM
 - /etc/pam_ldap.conf
 - /etc/pam.d/*
- installation de nscd (option)

et les différents services

- service LDAP natif :
 - activer LDAP (option de compilation, par ex. samba)
 - configurer l'accès au serveur (samba, postfix)
- utilisation de PAM dans les autres cas
- sinon chercher un remplaçant

Conclusion

- LDAP une brique système
- En passe de devenir fondamentale
- Incontournable pour voir venir l'avenir sereinement
- Complexe, ne pas sous évaluer le temps de prise en main / formation.

L'interopérabilité

- Peu de cas concrets d'interopérabilité entre serveurs ?
- Attention à la monoculture d'Active Directory
- Frilosité des éditeurs d'applications à fournir autre chose qu'une boîte noire (ds le cadre d'application tiers) :
 - Risque de voir se multiplier des annuaires incompatibles sur le campus
- Schémas communs incontournables

L'interopérabilité : MS/UNIX

- Répliquer les données d'un serveur LDAP vers l'autre : cf le projet AGALAN
 - <http://crip.ujf-grenoble.fr/AGALAN/technique/technique.html>
- utiliser samba-2.2 en BDC ?
- utiliser les nouvelles fonctionnalités de samba-3.0 ?
- remplacer l'invite d'authentification MS.