

ADMIN SYSTÈME TP 2, RAPPELS LDAP

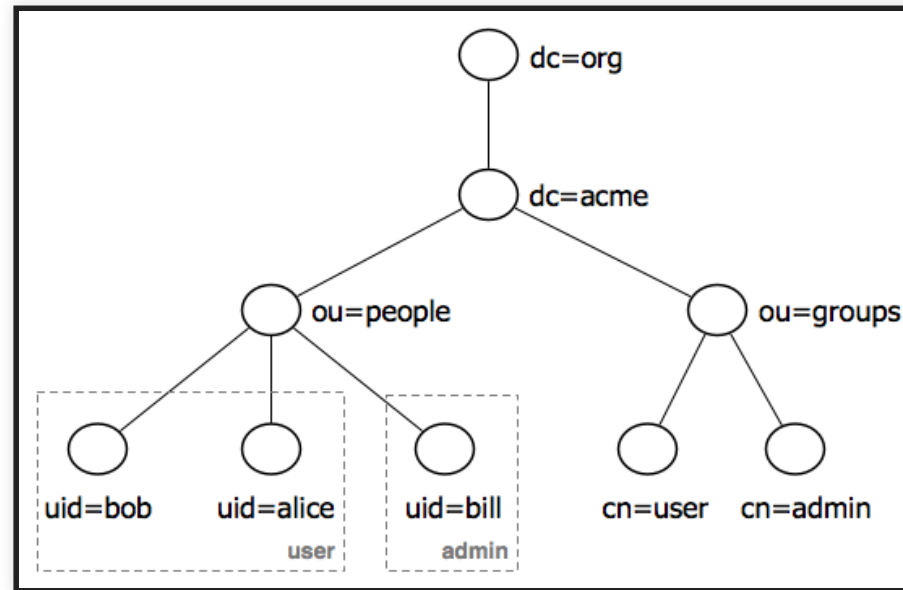
LDAP

- Lightweight Directory Access Protocol
- Modèle de donnée
- protocole

MODÈLE DE DONNÉE

- arborescence
 - DIT, Directory Information Tree

EXEMPLE D'ARBORESCENCE



STRUCTURE DES DONNÉES

- entrées
- dn : distinguished name
- schéma
 - par application (postfix, samba etc.)
- objectClass
- attributs
 - type = entier, chaîne ...
 - contraintes : obligatoire, multi-valué

FORMAT D'ÉCHANGE

- LDIF : LDAP Data Interchange Format

OBJECTCLASS "POSIXACCOUNT"

- certain attributs sont équivalents à des champs de /etc/passwd
- uid : login
- cn, sn : common name (nom prénom), surname (nom de famille)
- userPassword : mot de passe, en clair par défaut
 - s'il est chiffré, format spécifique (SHA1 le plus souvent)
 - {SSHA}dkPjpoj0pj...

OBJECTCLASS "POSIXACCOUNT", SUITE

- homeDirectory
- uidnumber
- gidnumber
- shell

PROTOCOLE

- search
 - base de recherche
 - filtre ldap
- add
- modify
- delete

FILTRE LDAP

- parenthèses autour du filtre
- opérateurs infixés $a \& b \rightarrow (\& (a) (b))$
- filtre de base : attribut=valeur
- combiner les filtres avec ET : $(\&(\text{expr})(\text{expr}))$ OU : $(\&(\text{expr})(\text{expr}))$
- négation : $(!(\text{expr}))$
- NB : attention au quoting shell $'(\&(\dots))'$