Introducció a LDAP

El problema

- /etc/passwd
- /ets/group

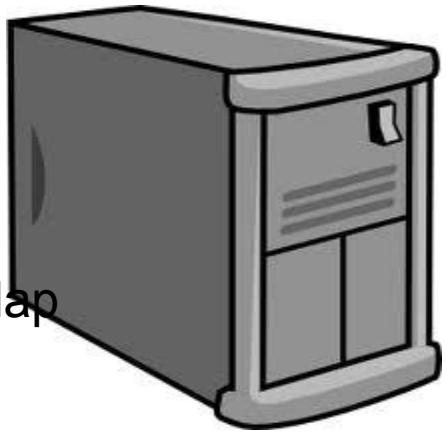
- /etc/passwd
- /ets/group

- /etc/passwd
- /ets/group

Una solució

● client ldap

● client ldap



● servidor ldap

● client ldap

Què és LDAP?

- Servei de directoris
- Guarda dades basades en atributs
- El volum de lectures és molt més gran que el volum de canvis
  - Sense transaccions
  - Sense rollback
- Model client-servidor
- Basat en entrades
  - Una entrada és una col·lecció d'atributs
  - Té un distinguished name (DN)

Per què hem d'usar LDAP?

- Administrar centralitzadament usuaris, grups i altres dades
- Evitar tenir un sistema de directoris separat per cada aplicació
- Distribuir la gestió de les dades a la gent adequada
- Permetre als usuaris retrobar informació que necessiten
- Possibilitat de distribuir els servidors allà on calen

LDAP vs Databases

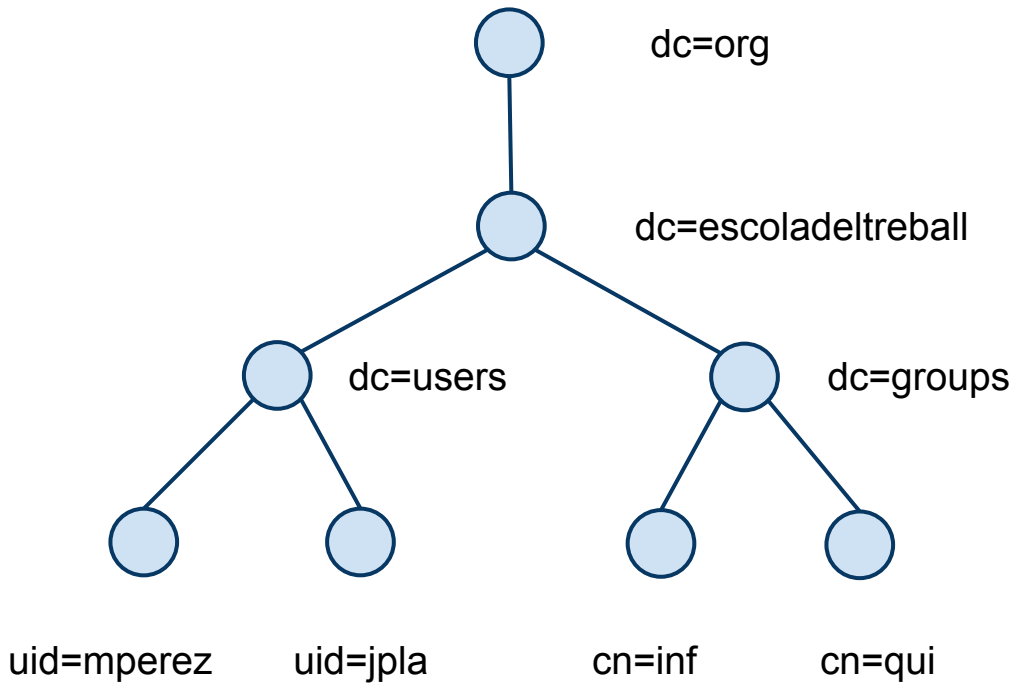
- Ratio lectura-escriptura - LDAP està optimitzat per a lectura
- Estàndards - els clients LDAP es poden comunicar amb qualsevol servidor LDAP

Acrònims

LDAP	Lightweight Directory Access Protocol
DN	Distinguish Name
RDN	Relative Distinuished Name
DIT	Directory Information Tree
LDIF	LDAP Data Interchange Format
OID	Object Identifier

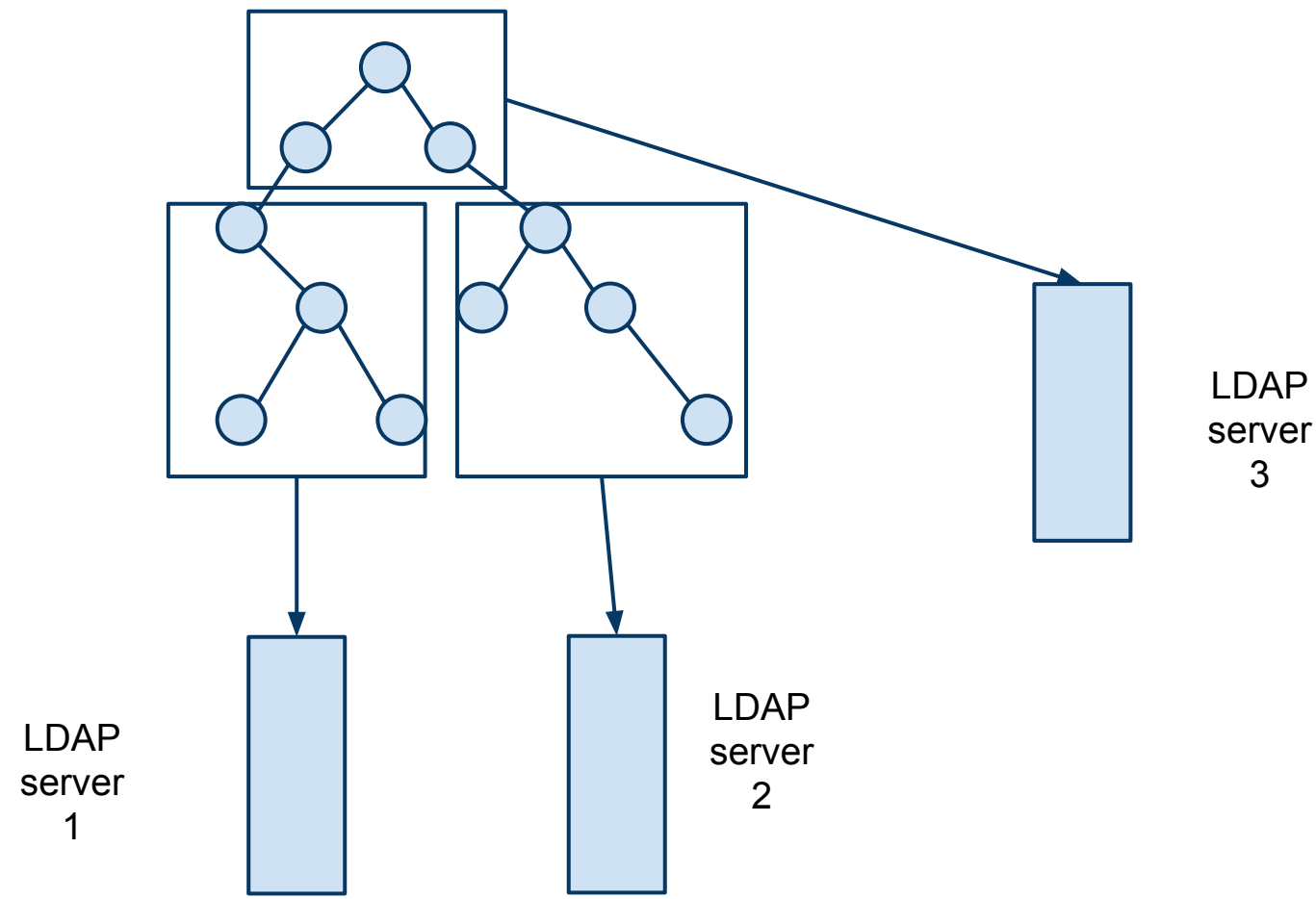
Espais de noms

- Estructura de dades jeràrquica
- Cada entrada a l'LDAP pot contenir dades i ser, alhora, un contenidor
- Els DN es llegeixen d'abaix cap a dalt, al revés que en un arbre de directoris unix



Vista global

Cada servidor ha de contenir un sub-arbre



Distinguished Names

- S'escriuen començant per baix i connectant cada nivell amb comes
- Té dues parts:
  - La de l'esquerra es diu Relative Distinguished Name
  - La resta és la Base Distinguished Name

Per exemple: uid=mperez,ou=users,dc=escoladeltreball,dc=org

  - el RDN és uid=mperez
  - el Base DN és ou=users,dc=escoladeltreball,dc=org

- A cada Base DN cada RDN és únic, així no hi ha dos entrades amb el mateix DN

LDAP Entry

- Les entrades es componen d'atributs
- Els atributs consisteixen de tipus amb múltiples valors
- El tipus descriu què és la informació
- El valor és la informació en format de text
- Els atributs tenen una sintaxi específica pel tipus de dada

LDAP Schema (1)

- Conjunt de regles que descriu quin tipus de dades es guarden
- Manté la consistència i la qualitat de les dades
- Redueix la duplicació de les dades
- Assegura que les aplicacions tenen interfícies consistent a les dades
- L'atribut de classe d'objecte determina les regles de l'esquema que l'entrada ha de cumplir

LDAP Schema (2)

L'esquema conté:

- Els atributs obligatoris
- Els atributs permesos
- Com comparar atributs
- Limita què es pot guardar en l'atribut: enter, etc
- Restringeix quina informació es pot guardar: no duplicats, etc

LDAP Schema: Objectclass

S'usa per a agrupar informació

Proporciona les següents regles:

- Atributs requerits
- Atributs permesos
- Una forma fàcil d'obtenir grups d'informació

Les entrades poden tenir múltiples classes d'objecte

- Els atributs requerits i permesos són la unió dels atributs de cada classe

LDAP Schema: Atributs

Els atributs tenen:

- Nom - identificador únic
- OID - seqüència d'enters separats per punts
- Sintaxi
  - Què és pot guardar: enter, etc
  - Com es fan les comparacions
- Si és multivalor o no

LDAP LDIF

- LDAP Data Interchange Format
  - Representa entrades LDAP en text pla
  - És llegible
  - És fàcil de modificar
  - És útil per fer canvis massius
  - Permet l'ús de plantilles
  - És bo per a fer backups i exportar/importar dades a un altre sistema
- Utilitats per a exportar de la BD a ldif i viceversa
  - slapcat: db a ldif
  - slapadd: ldif a db

LDAP LDIF exemple

```
dn: uid=bmarshal,ou=People,
        dc=pisoftware,dc=com
uid: bmarshal
cn: Brad Marshall
objectclass: account
objectclass: posixAccount
objectclass: top
loginshell: /bin/bash
uidnumber: 500
gidnumber: 120
homedirectory: /mnt/home/bmarshal
gecos: Brad Marshall,,,,
userpassword: {crypt}KDnOoUYN7Neac
```

LDAP filtres de cerca

Expressen els criteris que s'han de complir per localitzar l'entrada

Els operadors són:

&	and
|	or
!	not
~=	approx equal
>=	greater than or equal
<=	less than or equal
*	any

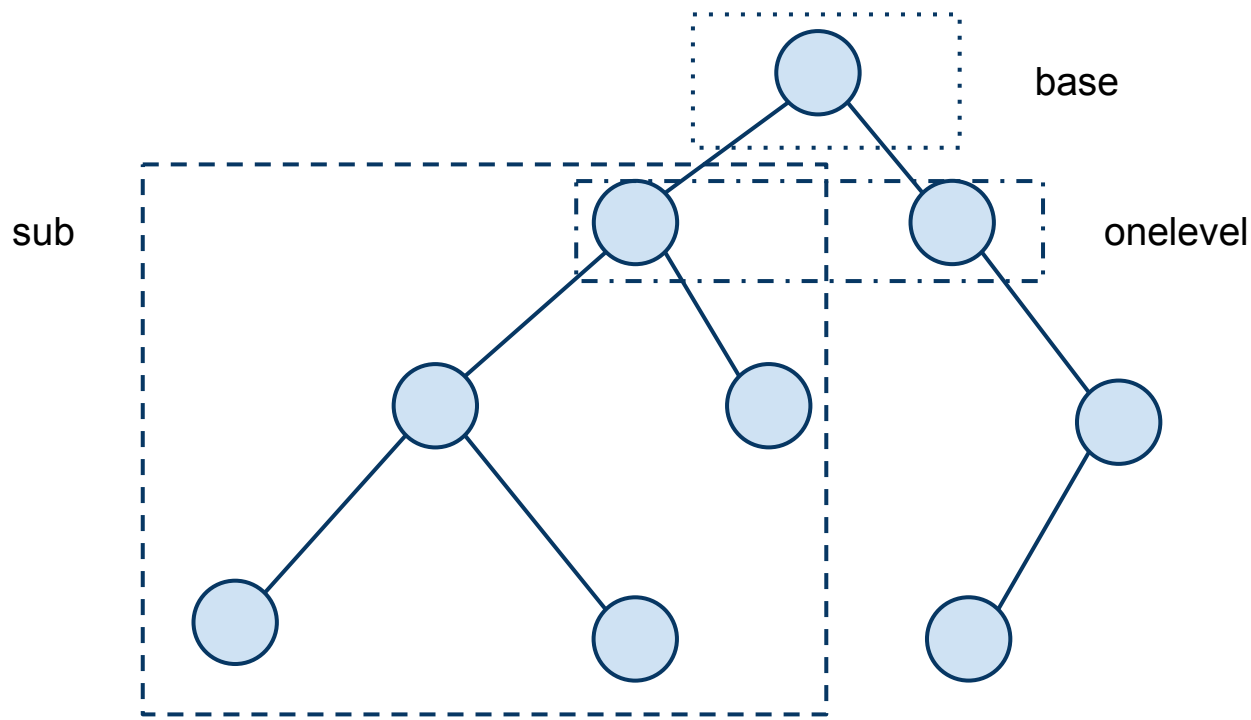
LDAP filtres de cerca. Exemples

- (objectclass=posixAccount)
- (cn=Mickey M*)
- (|(uid=fred)(uid=bill))
- (&(|(uid=jack)(uid=jill))(objectclass=posixAccount))

LDAP Search Scope

Tipus d'abast.

- base - limitat a l'objecte base
- onelevel - limitat als fills immediats
- sub - tot el sub-arbre des de la base



LDAP URLs

Definició d'URL:

<ldapurl> ::= "ldap://" [<hostport>]
"/" <dn> ["?" <attributes>
["?" <scope> "?" <filter>]]
<hostport> ::= <hostname>
[":" <portnumber>]
<dn> ::= a string as defined in RFC 1485
<attributes> ::= NULL | <attributelist>
<attributelist> ::= <attributetype>
| <attributetype>
["," <attributelist>]
<attributetype> ::= a string as defined
in RFC 1777
<scope> ::= "base" | "one" | "sub"
<filter> ::= a string as defined in RFC 1558

LDAP URLs exemples

- ldap://foo.bar.com/dc=bar,dc=com
- ldap://argle.bargle.com/dc=bar,dc=com??sub?uid=barney
- ldap://ldap.bedrock.com/dc=bar,dc=com?cn?sub?
  uid=barney

LDAP slapd.conf (1)

```
#
# See slapd.conf(5) for details
#   on configuration options.
# This file should NOT be world readable.
#
include         /etc/openldap/slapd.at.conf
include         /etc/openldap/slapd.oc.conf
schemacheck     off
pidfile         /var/run/slapd.pid
argsfile        /var/run/slapd.args
defaultaccess read
```

LDAP slapd.conf (2)

```
access to attr=userpassword
   by self write
   by * read
access to *
   by self write
   by dn=".+" read
   by * read
```

LDAP slapd.conf (3)

```
#######################################
# ldbm database definitions
#######################################
database ldbm
suffix    "dc=pisoftware, dc=com"
rootdn    "cn=Manager,dc=pisoftware,dc=com"
rootpw    {crypt}lAn4J@KmNp9
replica host=replica.bne.pisoftware.com:389
    binddn="cn=Manager,dc=pisoftware,dc=com"
    bindmethod=simple credentials=secret
    replogfile /path/to/replication.log
# cleartext passwords, especially for
# the rootdn, should be avoid. See
# slapd.conf(5) for details.
directory       /var/lib/openldap/
```

LDAP ACLs

- Poden restringir per:
  - Distinguished Name
  - Filtre per alguns atributs
  - Atributs
- Poden restringir amb:
  - Usuaris anònims
  - Usuaris autenticats
  - El propi usuari
  - Distinguished Name
  - Adreça IP o nom DNS
- Prioritat de control d'accés:
  - BD local
  - Regles globals
  - Segons l'ordre de les regles
  - La primera regla que compleix és la que es segueix

LDAP ACLs exemples

```
access to attribute=userpassword
    by dn="cn=Manager,dc=pisoftware,
        dc=com" write
    by self write
    by * read
access to dn="(.*,)?dc=pisoftware,dc=com"
        attr=homePhone
    by self write
    by dn="(.*,)?dc=pisoftware,dc=com" search
    by domain=.*\.pisoftware\.com read
    by anonymous auth
```

LDAP utilització

```
ldappasswd -W -D ’uid=bmarshal,ou=People,
        dc=pisoftware,dc=com’ ’uid=bmarshal’

ldapsearch -L ’uid=*’
ldapsearch -L ’objectclass=posixGroup’
ldapsearch -L ’objectclass=posixAccount’
ldapsearch -D ’uid=bmarshal,ou=People,dc=pisoftware,dc=com’ -W -L
      ’uid=bmarshal’

ldapmodify -W -r -D "cn=Manager,dc=pisoftware,dc=com" < bmarshal.ldif
```