

# LDAP

*Lightweight Directory Access Protocol*

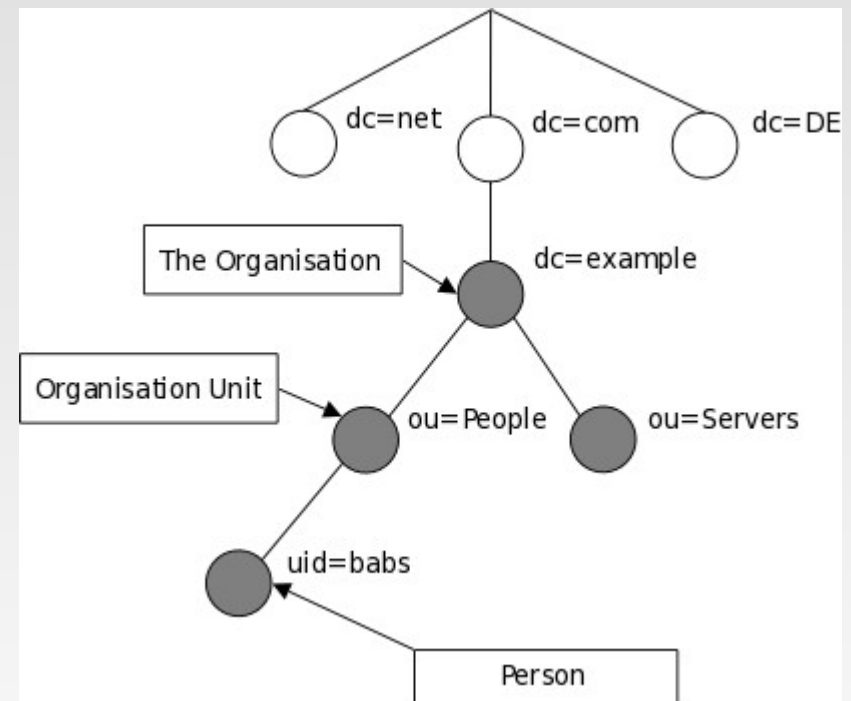
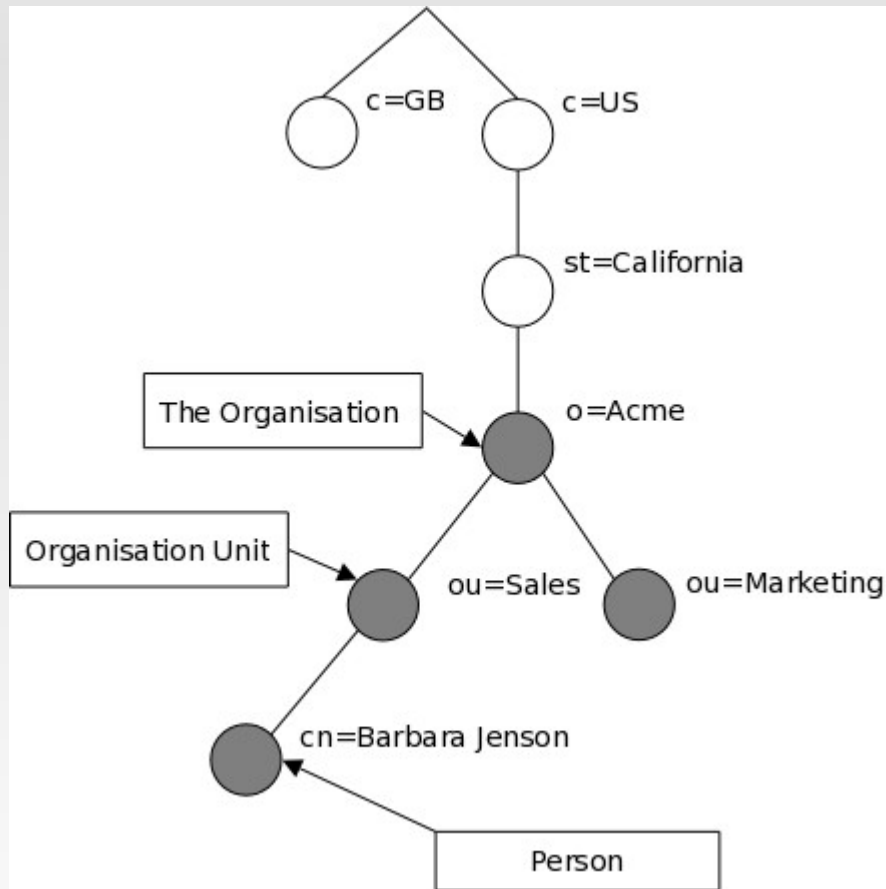
# Introducció

- LDAP és un protocol per accedir via TCP/IP a un directori o base de dades LDAP.
- **Base de dades centralitzada** amb informació d'usuaris, màquines, serveis, dispositius ...
- El directori o **base de dades LDAP** està organitzat en **forma d'arbre** (jerarquia).
- El directori o base de dades LDAP està optimitzat per rebre moltes **consultes de lectura**.
- La seva arquitectura té moltes similituds amb DNS.

# Introducció

- Un directori LDAP té moltes aplicacions pràctiques ja que centralitza la informació d'una organització i la fa accessible utilitzant un protocol estàndard.
  - Autenticació d'usuaris.
  - Autenticació de màquines.
  - Representació de l'organització.
  - Adreça telefònica.
  - Magatzem de configuracions d'aplicacions.
  - Magatzem de d'adreces de correu electrònic.
  - Organització d'usuaris i grups d'usuaris.

# Introducció



# • Arquitectura LDAP

- La base de dades LDAP té forma d'arbre on cada node o entrada pot guardar un conjunt d'atributs o informació.
- Cada node o entrada de l'arbre té un nom únic que l'identifica, és l'anomenat

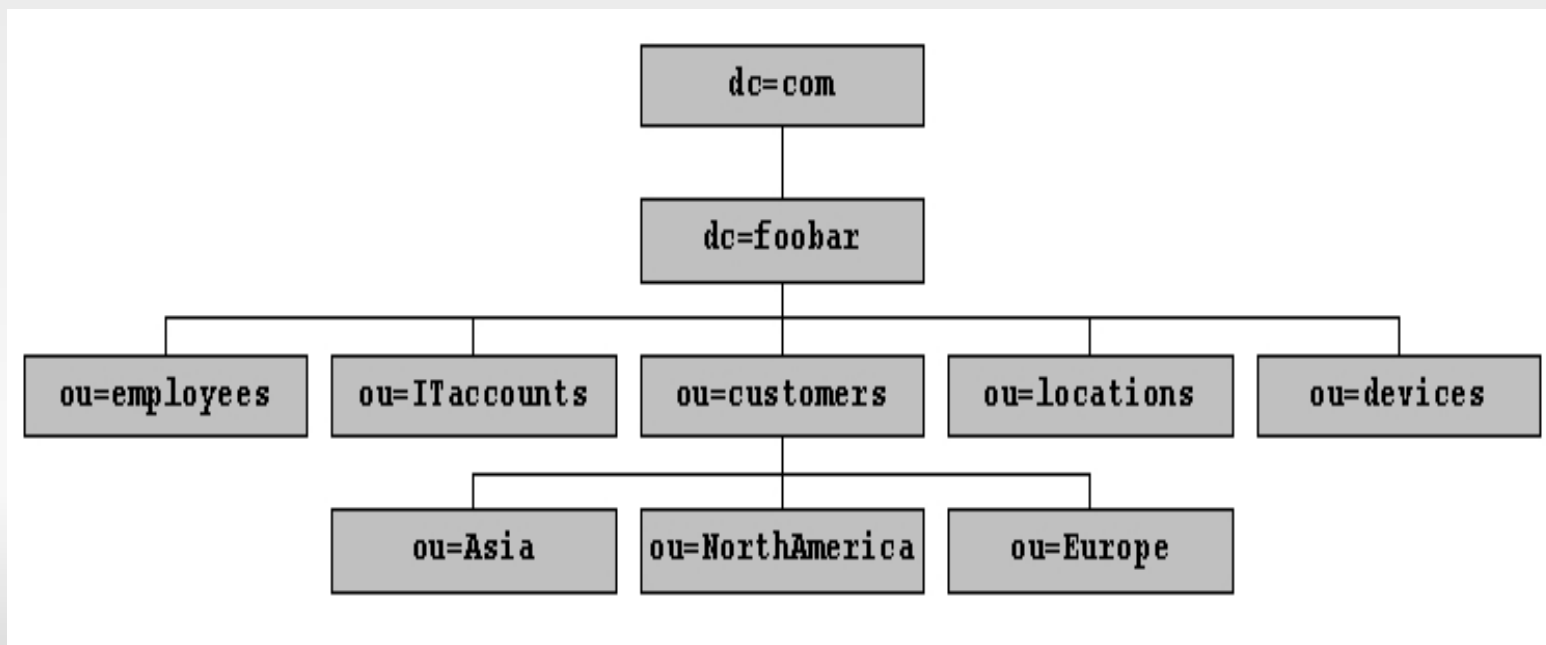
**DN = Distinguished Name**

# Arquitectura LDAP

- **DN Base**

- o="FooBar,Inc.", c=US
- o=foobar.com
- dc=foobar,dc=com

- **Organizational Units (ou)**



# • Arquitectura LDAP

## ■ Entrades individuals

- Per exemple vull afegir una entrada **dins la ou "employees"**, aquesta entrada representa un nou empleat.

- Normalment totes les entrades tenen sempre un **CN (common name)**. Per tant el **DN** d'un nou empleat anomenat "Fran Smith" serà:

**cn=Fran Smith,ou=employees,dc=foobar,dc=com**

- En el cas d'una nova entrada que representa una persona també tinc l'opció de basar el DN a partir d'un atribut anomenat **uid** enlloc de cn.

**uid=fsmith,ou=employees,dc=foobar,dc=com**

# • Exemple entrada LDAP

dn: uid=fsmith, ou=employees, dc=foobar, dc=com

*objectclass: person*

*objectclass: organizationalPerson*

*objectclass: inetOrgPerson*

*objectclass: foobarPerson*

uid: fsmith

givenname: Fran

sn: Smith

cn: Fran Smith

o: Foobar, Inc.

mailRoutingAddress: fsmith@foobar.com

mailhost: mail.foobar.com

userpassword: {crypt}3x1231v76T89N

uidnumber: 1234

gidnumber: 1200

homedirectory: /home/fsmith

loginshell: /usr/local/bin/bashz



# Referències

- <http://es.tldp.org/LinuxFocus/pub/mirror/LinuxFocus/Castellano/July2000/article159.shtml>
- <http://www.openldap.org/>
- [http://www.ldapman.org/ldap\\_rfcs.html](http://www.ldapman.org/ldap_rfcs.html)
- <http://www.zytrax.com/books/ldap/ch2/>
- <http://www.youtube.com/watch?v=LVE3WbakcOE>