Introdución ao LDAP. O servidor OpenLDAP

Sumario

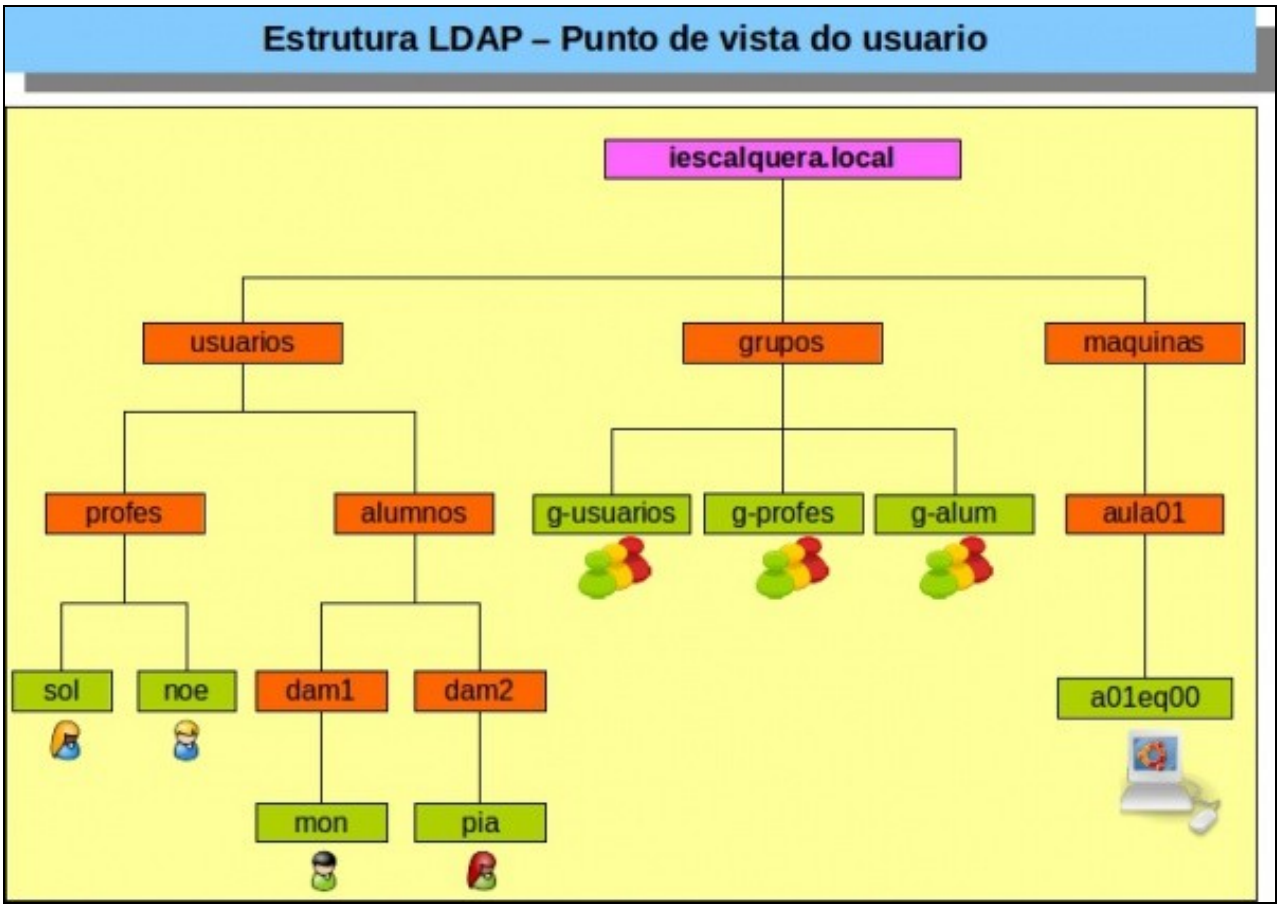
Introdución ao LDAP

Introdución

LDAP (*Lightweight Directory Access Protocol*, Protocolo Lixeiro de Acceso a Directorio) é un protocolo do nivel de aplicación que permite o acceso a un servizo de directorio para buscar diversa información, xa sexan usuarios, grupos, equipos, etc. O directorio é un conxunto de obxectos organizados de forma xerárquica, de forma que o servidor LDAP pode verse como unha base de datos en forma de árbore, que está optimizada para realizar consultas e buscas. O servizo LDAP é moi utilizado para a autenticación de usuarios.

Estrutura do LDAP

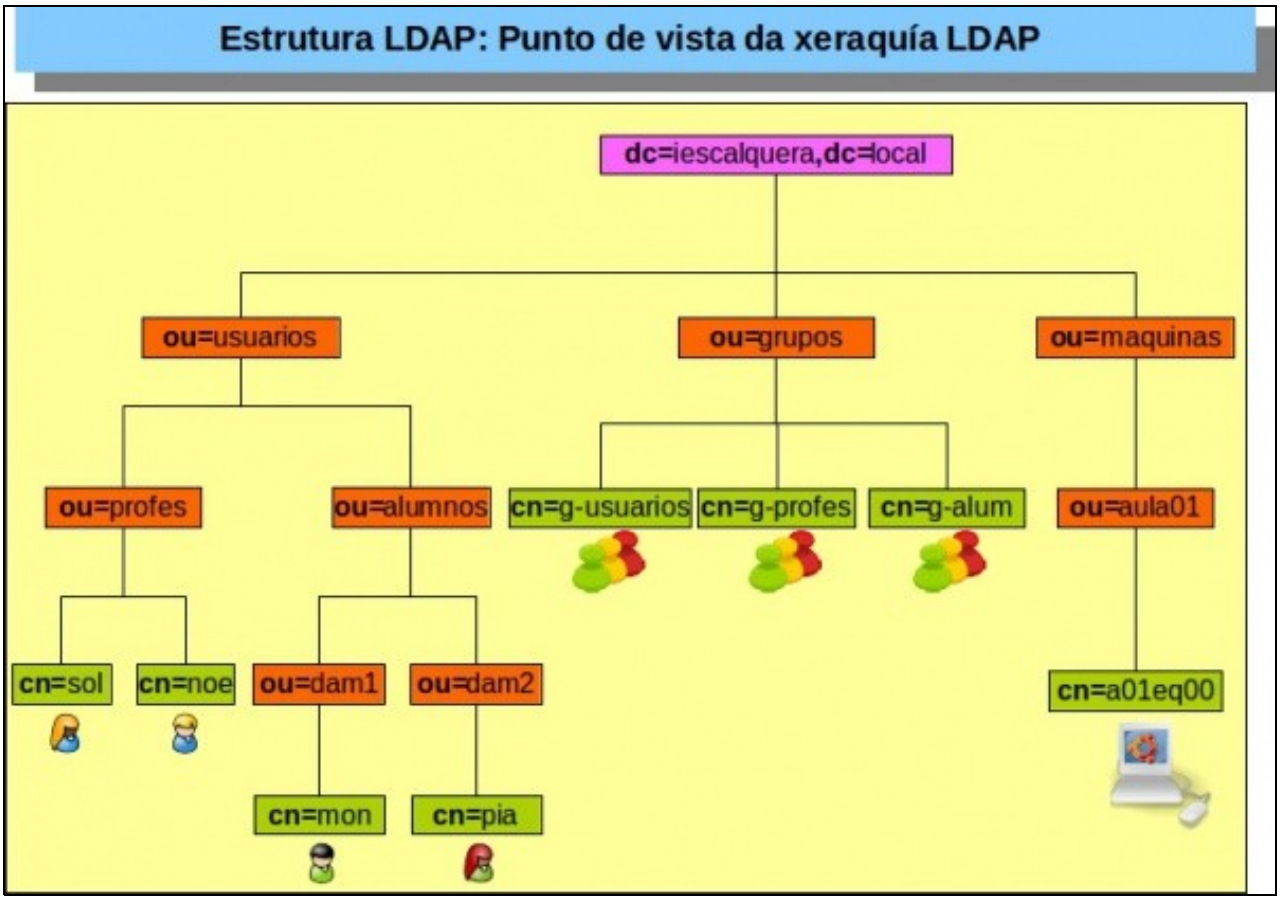
Para explicar a estrutura dun directorio basearémonos na seguinte imaxe:



- Na imaxe obsérvase que hai:
  - Un **dominio**, cor rosa.
  - **Unidades organizativas**, cor laranxa. Notar que hai unidades organizativas para albergar distintos tipos de obxectos: usuarios, grupos, máquinas, ...
  - **Obxectos finais**, cor verde. Tamén hai de distintos tipos, usuarios, grupos, equipos, etc.

- Non confundir a Unidade Organizativa **grupos** cos grupos aos que van pertencer os usuarios. A Unidade Organizativa serve para organizar obxectos, pois poderíamos ter tódolos obxectos finais nunha soa unidade organizativa, pero teríamos un LDAP caótico.

- Na seguinte imaxe amósase como se organiza cada elemento da árbore dentro do directorio LDAP.
- Cada elemento anterior é o valor que toman os distintos atributos que definen un obxecto de LDAP.



- Cada obxecto identifícase inequivocamente usando a notación de cadea de X.500 (http://es.wikipedia.org/wiki/X.500), como se vai amosar a continuación nos seguintes exemplos.
- Pero antes imos indicar o significado dos atributos:
    - **DC** = Compoñente de dominio
    - **OU** = Unidade organizativa
    - **CN** = Nome común
- Ademais imos usar os seguintes atributos:
    - **DN** = Nome distinguido
    - **RDN** = Nome distinguido relativo.

- A continuación imos ver, dunha forma moi resumida, como se almacenaría parte desa árbore nunha base de datos xerárquica de LDAP.
    - dn: dc=iescalquera,dc=local
    - dn: ou=usuarios,dc=iescalquera,dc=local
    - dn: ou=grupos,dc=iescalquera,dc=local
    - dn: ou=equipos,dc=iescalquera,dc=local
    - dn: ou=profes,ou=usuarios,dc=iescalquera,dc=local
    - dn: ou=alum,ou=usuarios,dc=iescalquera,dc=local
    - ...
    - dn: cn=sol,ou=profes,ou=usuarios,dc=iescalquera,dc=local
    - dn: cn=noe,ou=profes,ou=usuarios,dc=iescalquera,dc=local
    - ...
    - dn: ou=dam1,ou=alum,ou=usuarios,dc=iescalquera,dc=local
    - ...

- Observar que cada elemento da árbore ten unha entrada na base de datos. Esas entradas comezan co atributo **DN**.
- Toda entrada debe estar "colgada" de outra entrada "pai" que tamén debe existir na base de datos, salvo a primeira entrada que non colga de ninguén.
- Non pode haber dúas entradas **DN** iguais.
- As entradas do ficheiro pódense organizar nunha árbore como a da figura superior. A esa árbore chámaselle **DIT (Digital Information Tree)**

- Cada entrada ten un identificador único, o seu **Nome Distinguido** (*Distinguished Name*, DN). Este consta do seu Nome Distinguido Relativo (*Relative Distinguished Name*, RDN) formado por algún ou algúns atributos da entrada, seguidos do DN da entrada pai. Por exemplo,
    - **RDN: ou=profes**
    - **ou=usuarios,dc=iescalquera,dc=local** é o nome distinguido da entrada do pai, onde **dc** indica compoñente de dominio (*domain component*).

Atributos

- Imos ver agora, un pequeno exemplo, de como se descompón e almacena unha das entradas anteriores:

```
dn: cn=sol,dc=iescalquera,dc=local
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: Person
objectClass: posixAccount
objectClass: shadowAccount

cn: sol
givenName: Sol
sn: Lúa
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: sol@iescalquera.local
uidNumber: 10000
gidNumber: 10000
userPassword: abc123.
gecos: Sol Lua
loginShell: /bin/bash
homeDirectory: /home/sol
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
initials: SL
```

- Como vemos, neste caso, o obxecto **dn: cn=sol,dc=iescalquera,dc=local** ten unha serie de atributos. Logo veremos de onde saen eses ou outros atributos.
- A orde dos atributos é indiferente, pero sóense poñer os atributos **objectClass** ao principio de todo para saber de que tipo de obxecto estamos a falar: a que clase pertence.
- Segundo o tipo de clase **(objectClass)** o obxecto terá uns atributos ou outros. Como vemos, este obxecto pertence a varias clases, e por tanto terá os atributos de todas esas clases.
- Despois veremos que non teñen os mesmos atributos, por exemplo un usuario e un grupo, aínda que poidan compartir algún.
- Observar, por exemplo:
    - Todos os atributos **shadow*** proveñen da clase **shadowAccount**. Co cal, aquel obxecto que non pertenza a esa clase non pode ter eses atributos.
    - Pódense poñer varios teléfonos. Iso é porque ese atributo permite repeticións.
    - **sn (surname)** serían os apelidos, ese atributo pertence á clase, ... seguro que o usuario é quen de mirar a cal pertence dos ObjectClass. Se non é quen agora, seguro que si o é cando remate este conxunto de apartados introdutorios.
    - **homeDirectory**: seguro que o usuario sabe para que é ese atributo e a que clase pertence.

O formato LDIF

O formato **LDIF (LDAP Data Interchange Format**) permítenos introducir e extraer as entradas do servidor LDAP mediante arquivos de texto (hai que ter en conta que LDAP por si mesmo é un protocolo binario). Aquí pódese ver un exemplo dun ficheiro LDIF coa información dun usuario (o mesmo que vimos antes):

```
dn: cn=sol,dc=iescalquera,dc=local
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: Person
objectClass: posixAccount
objectClass: shadowAccount
```

```
cn: sol
givenName: Sol
sn: Lúa
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: sol@iescalquera.local
uidNumber: 10000
gidNumber: 10000
userPassword: abc123.
gecos: Sol Lua
loginShell: /bin/bash
homeDirectory: /home/sol
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
initials: SL
```

- Este ficheiros pódense facer a man e logo con comandos ser cargados na base de datos de LDAP.
- Cando extraemos información de LDAP imos extraela nese formato.

Esquemas

- Pero de onde saen os atributos de LDAP?. Pois dos **esquemas**
- Un **esquema**:
    - Define unha **clase de obxectos** sobre a que se desexa gardar información, por exemplo *libros*.
    - Define os **atributos** desa clase e o seu tipo, por exemplo: título, subtítulo, autores, clasificación, páxinas, etc.
    - Defínese cales dos atributos son obrigatorios e cales non.
    - Define as subclases que pode haber deses obxectos e os seus atributos, por exemplo: **libros técnicos**.
    - Un esquema pode ser creado por calquera.
    - Xa existen un conxunto de esquemas predefinidos e estandarizados que permiten o intercambio de información entre LDAPs instalados en distintos servidores.
- Por tanto, como xa se indicou, cando se crea un obxecto hai que indicar a que (sub)clase/s pertence e cubrir con valores os atributos obrigatorios de cada una desas (sub)clases.
- A modo de exemplo amosamos o formato dun esquema, máis alá da sintaxe, podemos concluír como se constrúe unha clase, que atributos ten obrigatorios, cales non e como se define un atributo.

```
...
################ Definición de clases
objectclass ( 2.5.6.5 NAME 'organizationalUnit'
        DESC 'RFC2256: an organizational unit'
        SUP top STRUCTURAL
        MUST ou
        MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
                x121Address $ registeredAddress $ destinationIndicator $
                preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
                telephoneNumber $ internationaliSDNNumber $
                facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
                postalAddress $ physicalDeliveryOfficeName $ st $ l $ description ) )
...
objectclass ( 2.5.6.6 NAME 'person'
        DESC 'RFC2256: a person'
        SUP top STRUCTURAL
        MUST ( sn $ cn )
        MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
...

################ Exemplo de definición de atributos
attributetype ( 2.5.4.4 NAME ( 'sn' 'surname' )
        DESC 'RFC2256: last (family) name(s) for which the entity is known by'
        SUP name )

attributetype ( 2.5.4.20 NAME 'telephoneNumber'
        DESC 'RFC2256: Telephone Number'
        EQUALITY telephoneNumberMatch
        SUBSTR telephoneNumberSubstringsMatch
```

```
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )

attributetype ( 2.5.4.9 NAME ( 'street' 'streetAddress' )
        DESC 'RFC2256: street address of this object'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128} )

attributetype ( 2.5.4.17 NAME 'postalCode'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{40} )
...
```

- A modo de exemplo explícanse algunhas das definicións dos atributos e das clases:
    - **MUST**: indica que a clase debe conter eses atributos obrigatoriamente.
    - **MAY**: indica que a clase pode conter os atributos que se relacionan.
    - Observar que hai atributos, como 'telephoneNumber', que están en varias clases.
    - **caseIgnoreMatch**: indica que a cadea pode conter caracteres tanto en maiúsculas como en minúsculas.
    - **1.3.6.1.4.1.1466.115.121.1.15**: String de tipo Unicode (UTF-8).

Características técnicas do servizo LDAP

- A última versión do protocolo LDAP é a versión 3 (LDAPv3), que ofrece como principais vantaxes con respecto á versión anterior (LDAPv2) o uso de conexións seguras con TLS/SSL e autenticación con SASL, uso do xogo de caracteres Unicode, e unha maior estensibilidade, polo que se recomenda utilizar sempre esta última versión.
- O protocolo **LDAP** utiliza o porto **TCP 389**,
- e o protocolo **LDAPS** (versión segura do protocolo que cifra os datos transmitidos) usa o **porto 636**.
- No seguinte enlace está a RFC que define o protocolo LDAPv3 http://tools.ietf.org/html/rfc2251

Características de OpenLDAP

OpenLDAP (http://www.openldap.org) é unha implementación libre do protocolo que soporta múltiples esquemas, polo que pode ser usada para conectarse a calquera outro LDAP. OpenLDAP ten tres compoñentes principais:

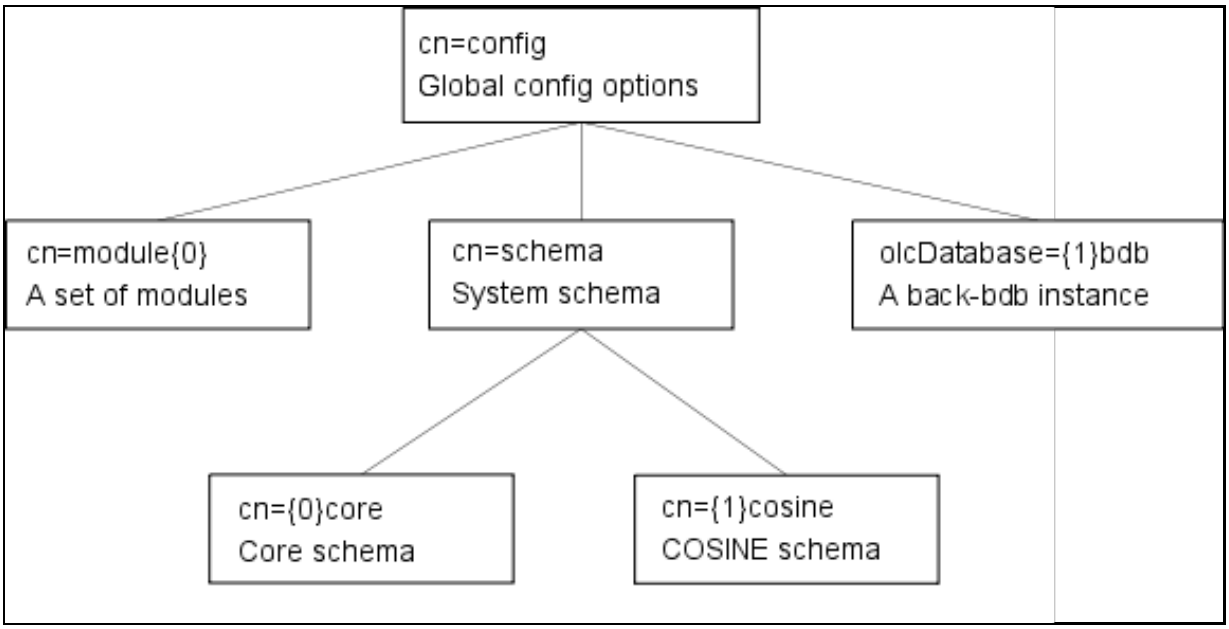
- slapd (Standalone LDAP Daemon): demo de servidor LDAP autónomo.
- Librerías que implantan o protocolo LDAP.
- Utilidades, ferramentas e clientes, como *ldapsearch*, *ldapadd*, *ldapdelete*, etc..

Configuración básica de OpenLDAP

Ata a versión 2.3 de OpenLDAP, a configuración básica do servidor era almacenada no ficheiro de configuración **slapd.conf**.

- En cambio, nas versións actuais a información de configuración do servidor tamén se xestiona co formato LDAP e pode ser modificada usando ficheiros LDIF.
- Esta información de configuración é almacenada no directorio **slapd.d**, que no caso de Ubuntu ou Debian atópase dentro de **/etc/ldap**.

- Desta forma, teremos un directorio ou unha **rama** (se vemos a información almacenada como unha árbore) especial no LDAP cun esquema predefinido para almacenar toda a información de configuración, que inclúe:
    - Opcións globais de configuración do servidor. As entradas de configuración comezan co acrónimo **olc** (OpenLDAP Configuration).
    - Módulos dinámicos que se queren cargar
    - Esquemas
    - Configuración dos distintos *backends* (esquemas de almacenamento) e bases de datos do LDAP.
- Este directorio especial comeza na entrada **cn=config**, e segue a estrutura que se mostra a continuación:



Na páxina do OpenLDAP pódese atopar información detallada sobre as distintas directivas que aquí se poden introducir: http://www.openldap.org/doc/admin24/slapdconf2.html#Configuration%20Directives

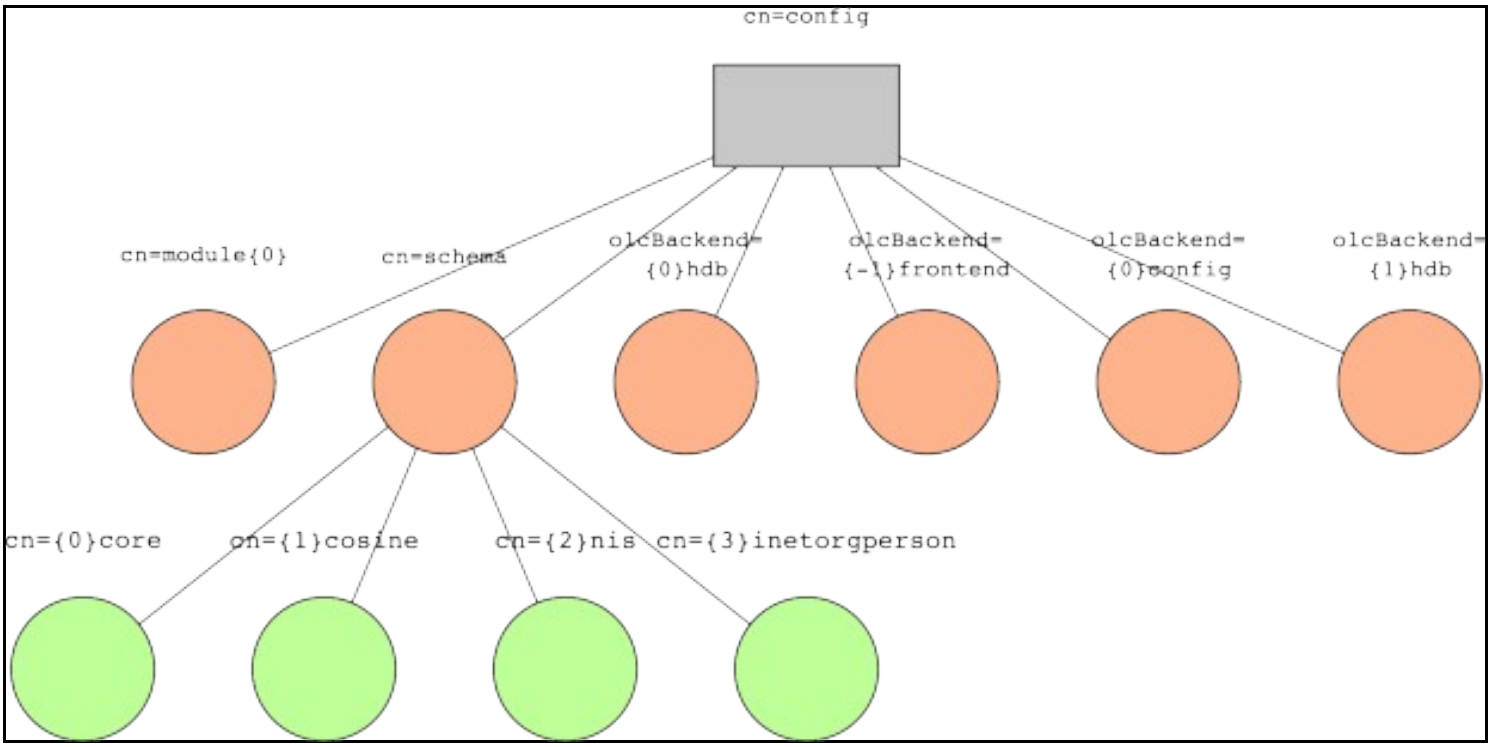
Esquemas de OpenLDAP

- A continuación expóñense os tres esquemas que imos usar en OpenLdap para crear os obxectos (dominios, unidades organizativas, usuarios, grupos, equipos, etc) nesta parte II e III.
- Na parte V introduciremos o esquema para crear obxectos tipo SAMBA, para que clientes Windows poidan facer uso de OpenLdap.
- Os esquemas que se expoñen teñen unha estrutura **enguedellada**, pero recomendamos que se lles adiquen uns minutos para familiarizarse só cos atributos e as clases de obxectos. Non hai que aprendelos...!!! pero si familiarizarse co formato e estrutura.
- No seguinte enlace hai información sobre as especificacións do esquema e como expandilo: http://www.openldap.org/doc/admin23/schema.html
- En **/etc/ldap/schema** hai un conxunto de esquemas predefinidos e estandarizados que poden ser cargados dentro da estrutura LDAP coa instrución:
    - **ldapadd -Y EXTERNAL -H ldapi:/// -f esquema.ldif** (Pronto veremos e explicaremos esta instrución).
- Unha vez que se instale o paquete LDAP (slapd) pódense ver eses esquemas. Non todos eses esquemas están cargados no LDAP (Pronto instalaremos LDAP).

```
root@dserver00:~# ls /etc/ldap/schema/
collective.ldif    cosine.schema         java.ldif      openldap.schema
collective.schema  duaconf.ldif          java.schema    pmi.ldif
corba.ldif         duaconf.schema        misc.ldif      pmi.schema
corba.schema       dyngroup.ldif         misc.schema    ppolicy.ldif
core.ldif          dyngroup.schema       nis.ldif       ppolicy.schema
core.schema        inetorgperson.ldif    nis.schema     README
cosine.ldif        inetorgperson.schema  openldap.ldif
```

- Os ficheiros **.schema** definen os elementos que conforman o esquema.
- Os ficheiros **.ldif** definen eses mesmos elementos pero en formato LDIF para ser cargados no LDAP.
- Deses esquemas hai catro que se instalan por defecto en Debian cando se instala o paquete (slapd): **core**, **cosine**, **nis** e **inetOrgPerson**. Agora pasamos a dar unhas pinceladas de cada un.
- Nos SOs que instalen o ldap sen os esquemas é preciso cargalos coa instrución anterior: **ldapadd -Y EXTERNAL -H ldapi:/// -f esquema.ldif**

- Na imaxe amósase onde colgan os esquemas dentro da xerarquía de LDAP. Imaxe obtida do Blog de Albero Molina Coballes



- Os números entre **chaves {}**, indican a orde na que se cargou cada un dos esquemas.
- Os números serven para organizar un pouco a orde na que se deben cargar os elementos, por se algún depende de outro, aínda que na organización da base de datos a orde na que están as entradas é irrelevante.

Esquema core

- Aparte de poder ver o seu contido nos ficheiros de /etc/ldap/schema/core.*, pódese ver o contido do ficheiro no seguinte enlace: http://www.opensource.apple.com/source/OpenLDAP/OpenLDAP-108.1/OpenLDAP/servers/slapd/schema/core.ldif

- E o esquema principal que contén as seguintes clases:

```
root@dserver00:~# cat /etc/ldap/schema/core.schema | grep objectclass
#objectclass ( 2.5.6.0 NAME 'top'
#objectclass ( 2.5.6.1 NAME 'alias'
objectclass ( 2.5.6.2 NAME 'country'
objectclass ( 2.5.6.3 NAME 'locality'
objectclass ( 2.5.6.4 NAME 'organization'
objectclass ( 2.5.6.5 NAME 'organizationalUnit'
objectclass ( 2.5.6.6 NAME 'person'
objectclass ( 2.5.6.7 NAME 'organizationalPerson'
objectclass ( 2.5.6.8 NAME 'organizationalRole'
objectclass ( 2.5.6.9 NAME 'groupOfNames'
objectclass ( 2.5.6.10 NAME 'residentialPerson'
objectclass ( 2.5.6.11 NAME 'applicationProcess'
objectclass ( 2.5.6.12 NAME 'applicationEntity'
objectclass ( 2.5.6.13 NAME 'dSA'
objectclass ( 2.5.6.14 NAME 'device'
objectclass ( 2.5.6.15 NAME 'strongAuthenticationUser'
objectclass ( 2.5.6.16 NAME 'certificationAuthority'
objectclass ( 2.5.6.17 NAME 'groupOfUniqueNames'
objectclass ( 2.5.6.18 NAME 'userSecurityInformation'
objectclass ( 2.5.6.16.2 NAME 'certificationAuthority-V2'
objectclass ( 2.5.6.19 NAME 'cRLDistributionPoint'
objectclass ( 2.5.6.20 NAME 'dmd'
objectclass ( 2.5.6.21 NAME 'pkiUser'
objectclass ( 2.5.6.22 NAME 'pkiCA'
objectclass ( 2.5.6.23 NAME 'deltaCRL'
objectclass ( 1.3.6.1.4.1.250.3.15 NAME 'labeledURIObject'
objectclass ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject'
objectclass ( 1.3.6.1.4.1.1466.344 NAME 'dcObject'
```

```
objectclass ( 1.3.6.1.1.3.1 NAME 'uidObject'
```

- Por sinalar algunhas: 'organizationalUnit', 'organizationalPerson' e 'person'
- Se se consulta o ficheiro .ldif dese esquema verase que cada entrada anterior comeza con **olc** (OpenLDAP Configuration)

- **Os atributos que define son**:

```
root@dserver00:~# cat /etc/ldap/schema/core.schema | grep attributetype

#attributetype ( 2.5.4.0 NAME 'objectClass'
#attributetype ( 2.5.4.1 NAME ( 'aliasedObjectName' 'aliasedEntryName' )
attributetype ( 2.5.4.2 NAME 'knowledgeInformation'
#attributetype ( 2.5.4.3 NAME ( 'cn' 'commonName' )
attributetype ( 2.5.4.4 NAME ( 'sn' 'surname' )
attributetype ( 2.5.4.5 NAME 'serialNumber'
attributetype ( 2.5.4.6 NAME ( 'c' 'countryName' )
attributetype ( 2.5.4.7 NAME ( 'l' 'localityName' )
attributetype ( 2.5.4.8 NAME ( 'st' 'stateOrProvinceName' )
attributetype ( 2.5.4.9 NAME ( 'street' 'streetAddress' )
attributetype ( 2.5.4.10 NAME ( 'o' 'organizationName' )
attributetype ( 2.5.4.11 NAME ( 'ou' 'organizationalUnitName' )
attributetype ( 2.5.4.12 NAME 'title'
#attributetype ( 2.5.4.13 NAME 'description'
attributetype ( 2.5.4.14 NAME 'searchGuide'
attributetype ( 2.5.4.15 NAME 'businessCategory'
attributetype ( 2.5.4.16 NAME 'postalAddress'
attributetype ( 2.5.4.17 NAME 'postalCode'
attributetype ( 2.5.4.18 NAME 'postOfficeBox'
attributetype ( 2.5.4.19 NAME 'physicalDeliveryOfficeName'
attributetype ( 2.5.4.20 NAME 'telephoneNumber'
attributetype ( 2.5.4.21 NAME 'telexNumber'
attributetype ( 2.5.4.22 NAME 'teletexTerminalIdentifier'
attributetype ( 2.5.4.23 NAME ( 'facsimileTelephoneNumber' 'fax' )
attributetype ( 2.5.4.24 NAME 'x121Address'
attributetype ( 2.5.4.25 NAME 'internationaliSDNNumber'
attributetype ( 2.5.4.26 NAME 'registeredAddress'
attributetype ( 2.5.4.27 NAME 'destinationIndicator'
attributetype ( 2.5.4.28 NAME 'preferredDeliveryMethod'
attributetype ( 2.5.4.29 NAME 'presentationAddress'
attributetype ( 2.5.4.30 NAME 'supportedApplicationContext'
attributetype ( 2.5.4.31 NAME 'member'
attributetype ( 2.5.4.32 NAME 'owner'
attributetype ( 2.5.4.33 NAME 'roleOccupant'
#attributetype ( 2.5.4.34 NAME 'seeAlso'
#attributetype ( 2.5.4.35 NAME 'userPassword'
attributetype ( 2.5.4.36 NAME 'userCertificate'
attributetype ( 2.5.4.37 NAME 'cACertificate'
attributetype ( 2.5.4.38 NAME 'authorityRevocationList'
attributetype ( 2.5.4.39 NAME 'certificateRevocationList'
attributetype ( 2.5.4.40 NAME 'crossCertificatePair'
#attributetype ( 2.5.4.41 NAME 'name'
attributetype ( 2.5.4.42 NAME ( 'givenName' 'gn' )
attributetype ( 2.5.4.43 NAME 'initials'
attributetype ( 2.5.4.44 NAME 'generationQualifier'
attributetype ( 2.5.4.45 NAME 'x500UniqueIdentifier'
attributetype ( 2.5.4.46 NAME 'dnQualifier'
attributetype ( 2.5.4.47 NAME 'enhancedSearchGuide'
attributetype ( 2.5.4.48 NAME 'protocolInformation'
#attributetype ( 2.5.4.49 NAME 'distinguishedName'
attributetype ( 2.5.4.50 NAME 'uniqueMember'
attributetype ( 2.5.4.51 NAME 'houseIdentifier'
attributetype ( 2.5.4.52 NAME 'supportedAlgorithms'
attributetype ( 2.5.4.53 NAME 'deltaRevocationList'
attributetype ( 2.5.4.54 NAME 'dmdName'
attributetype ( 2.5.4.65 NAME 'pseudonym'
#attributetype ( 1.3.6.1.4.1.250.1.57 NAME 'labeledURI'
#attributetype ( 0.9.2342.19200300.100.1.1
attributetype ( 0.9.2342.19200300.100.1.3 NAME ( 'mail' 'rfc822Mailbox' )
attributetype ( 0.9.2342.19200300.100.1.25 NAME ( 'dc' 'domainComponent' )
attributetype ( 0.9.2342.19200300.100.1.37 NAME ( 'dc' 'domainComponent' )
```

```
attributetype ( 1.2.840.113549.1.9.1 NAME ( 'email' 'emailAddress' 'pkcs9email' )
```

- Botarlle un ollo aos distintos atributos, seguro que moitos son familiares.
- Se se consulta o ficheiro .ldif dese esquema verase que cada entrada anterior comeza con **olc** (OpenLDAP Configuration)

Esquema COSINE

- O esquema **COSINE (Co-operation and Open Systems Interconnection in Europe)** define as seguintes clases.
- A versión que instalamos de OpenLDAP implanta a versión RFC 1274 (http://tools.ietf.org/html/rfc1274) que está obsoleta. A versión actual é RFC 4524 (http://tools.ietf.org/html/rfc4524).

```
#objectclass ( 0.9.2342.19200300.100.4.3 NAME 'pilotObject'
objectclass ( 0.9.2342.19200300.100.4.4 NAME ( 'pilotPerson' 'newPilotPerson' )
objectclass ( 0.9.2342.19200300.100.4.5 NAME 'account'
objectclass ( 0.9.2342.19200300.100.4.6 NAME 'document'
objectclass ( 0.9.2342.19200300.100.4.7 NAME 'room'
objectclass ( 0.9.2342.19200300.100.4.9 NAME 'documentSeries'
objectclass ( 0.9.2342.19200300.100.4.13 NAME 'domain'
objectclass ( 0.9.2342.19200300.100.4.14 NAME 'RFC822localPart'
objectclass ( 0.9.2342.19200300.100.4.15 NAME 'dNSDomain'
objectclass ( 0.9.2342.19200300.100.4.17 NAME 'domainRelatedObject'
objectclass ( 0.9.2342.19200300.100.4.18 NAME 'friendlyCountry'
## objectclass ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject'
objectclass ( 0.9.2342.19200300.100.4.20 NAME 'pilotOrganization'
objectclass ( 0.9.2342.19200300.100.4.21 NAME 'pilotDSA'
objectclass ( 0.9.2342.19200300.100.4.22 NAME 'qualityLabelledData'
```

- **Os atributos**, entre eles:
    - **photo**,
    - **favoriteDrink**, hmmmmm!!!.

```
##attributetype ( 0.9.2342.19200300.100.1.1 NAME ( 'uid' 'userid' )
attributetype ( 0.9.2342.19200300.100.1.2 NAME 'textEncodedORAddress'
##attributetype ( 0.9.2342.19200300.100.1.3 NAME ( 'mail' 'rfc822Mailbox' )
attributetype ( 0.9.2342.19200300.100.1.4 NAME 'info'
attributetype ( 0.9.2342.19200300.100.1.5 NAME ( 'drink' 'favouriteDrink' )
attributetype ( 0.9.2342.19200300.100.1.6 NAME 'roomNumber'
attributetype ( 0.9.2342.19200300.100.1.7 NAME 'photo'
attributetype ( 0.9.2342.19200300.100.1.8 NAME 'userClass'
attributetype ( 0.9.2342.19200300.100.1.9 NAME 'host'
attributetype ( 0.9.2342.19200300.100.1.10 NAME 'manager'
attributetype ( 0.9.2342.19200300.100.1.11 NAME 'documentIdentifier'
attributetype ( 0.9.2342.19200300.100.1.12 NAME 'documentTitle'
attributetype ( 0.9.2342.19200300.100.1.13 NAME 'documentVersion'
attributetype ( 0.9.2342.19200300.100.1.14 NAME 'documentAuthor'
attributetype ( 0.9.2342.19200300.100.1.15 NAME 'documentLocation'
attributetype ( 0.9.2342.19200300.100.1.20 NAME ( 'homePhone' 'homeTelephoneNumber' )
attributetype ( 0.9.2342.19200300.100.1.21 NAME 'secretary'
attributetype ( 0.9.2342.19200300.100.1.22 NAME 'otherMailbox'
#attributetype ( 0.9.2342.19200300.100.1.23 NAME 'lastModifiedTime'
#attributetype ( 0.9.2342.1920030http://es.wikipedia.org/wiki/Base640.100.1.24 NAME 'lastModifiedBy'
##attributetype ( 0.9.2342.19200300.100.1.25 NAME ( 'dc' 'domainComponent' )
attributetype ( 0.9.2342.19200300.100.1.26 NAME 'aRecord'
attributetype ( 0.9.2342.19200300.100.1.27 NAME 'mDRecord'
attributetype ( 0.9.2342.19200300.100.1.28 NAME 'mXRecord'
attributetype ( 0.9.2342.19200300.100.1.29 NAME 'nSRecord'
attributetype ( 0.9.2342.19200300.100.1.30 NAME 'sOARecord'
attributetype ( 0.9.2342.19200300.100.1.31 NAME 'cNAMERecord'
#attributetype ( 0.9.2342.19200300.100.1.37 NAME 'associatedDomain'
attributetype ( 0.9.2342.19200300.100.1.38 NAME 'associatedName'
attributetype ( 0.9.2342.19200300.100.1.39 NAME 'homePostalAddress'
attributetype ( 0.9.2342.19200300.100.1.40 NAME 'personalTitle'
attributetype ( 0.9.2342.19200300.100.1.41 NAME ( 'mobile' 'mobileTelephoneNumber' )
attributetype ( 0.9.2342.19200300.100.1.42 NAME ( 'pager' 'pagerTelephoneNumber' )
attributetype ( 0.9.2342.19200300.100.1.43 NAME ( 'co' 'friendlyCountryName' )
attributetype ( 0.9.2342.19200300.100.1.44 NAME 'uniqueIdentifier'
attributetype ( 0.9.2342.19200300.100.1.45 NAME 'organizationalStatus'
attributetype ( 0.9.2342.19200300.100.1.46 NAME 'janetMailbox'
```

```
attributetype ( 0.9.2342.19200300.100.1.47 NAME 'mailPreferenceOption'
attributetype ( 0.9.2342.19200300.100.1.48 NAME 'buildingName'
attributetype ( 0.9.2342.19200300.100.1.49 NAME 'dSAQuality'
attributetype ( 0.9.2342.19200300.100.1.50 NAME 'singleLevelQuality'
attributetype ( 0.9.2342.19200300.100.1.51 NAME 'subtreeMinimumQuality'
attributetype ( 0.9.2342.19200300.100.1.52 NAME 'subtreeMaximumQuality'
attributetype ( 0.9.2342.19200300.100.1.53 NAME 'personalSignature'
attributetype ( 0.9.2342.19200300.100.1.54 NAME 'dITRedirect'
attributetype ( 0.9.2342.19200300.100.1.55 NAME 'audio'
attributetype ( 0.9.2342.19200300.100.1.56 NAME 'documentPublisher'
```

Esquema NIS

- O esquema **NIS (Network Information System** está definido en modo experimental na RFC 2307 (https://tools.ietf.org/html/rfc2307)
- As clases de obxectos que define son:

- Resaltar as tres primeiras clases, pois son as que nos van permitir crear usuarios e grupos cos que poder entrar nos equipos clientes. Usuarios e grupos tipo Unix.

```
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'
objectclass ( 1.3.6.1.1.1.2.1 NAME 'shadowAccount'
objectclass ( 1.3.6.1.1.1.2.2 NAME 'posixGroup'
objectclass ( 1.3.6.1.1.1.2.3 NAME 'ipService'
objectclass ( 1.3.6.1.1.1.2.4 NAME 'ipProtocol'
objectclass ( 1.3.6.1.1.1.2.5 NAME 'oncRpc'
objectclass ( 1.3.6.1.1.1.2.6 NAME 'ipHost'
objectclass ( 1.3.6.1.1.1.2.7 NAME 'ipNetwork'
objectclass ( 1.3.6.1.1.1.2.8 NAME 'nisNetgroup'
objectclass ( 1.3.6.1.1.1.2.9 NAME 'nisMap'
objectclass ( 1.3.6.1.1.1.2.10 NAME 'nisObject'
objectclass ( 1.3.6.1.1.1.2.11 NAME 'ieee802Device'
objectclass ( 1.3.6.1.1.1.2.12 NAME 'bootableDevice'
```

- **Os atributos**: observar até o número 13, pois son familiares para un usuario de Linux.
- **gecos** significa **General Electric Comprehensive Operating System**.
    - ♦ É esa información que se almacena separada por comas cando os usuarios se gardan en local en /**etc**/**passwd**.
    - ♦ Contería a información que se manexaría co comando **chfn** para modificar os subcampos separados por comas que contería este campo: Nome completo usuario/programa, Número de habitación, persoa de contacto, teléfono, etc.
    - ♦ Como se pode ver esa información podémola almacenar en moitos dos atributos vistos en esquemas anteriores.

```
#attributetype ( 1.3.6.1.1.1.1.0 NAME 'uidNumber'
#attributetype ( 1.3.6.1.1.1.1.1 NAME 'gidNumber'
attributetype ( 1.3.6.1.1.1.1.2 NAME 'gecos'
attributetype ( 1.3.6.1.1.1.1.3 NAME 'homeDirectory'
attributetype ( 1.3.6.1.1.1.1.4 NAME 'loginShell'
attributetype ( 1.3.6.1.1.1.1.5 NAME 'shadowLastChange'
attributetype ( 1.3.6.1.1.1.1.6 NAME 'shadowMin'
attributetype ( 1.3.6.1.1.1.1.7 NAME 'shadowMax'
attributetype ( 1.3.6.1.1.1.1.8 NAME 'shadowWarning'
attributetype ( 1.3.6.1.1.1.1.9 NAME 'shadowInactive'
attributetype ( 1.3.6.1.1.1.1.10 NAME 'shadowExpire'
attributetype ( 1.3.6.1.1.1.1.11 NAME 'shadowFlag'
attributetype ( 1.3.6.1.1.1.1.12 NAME 'memberUid'
attributetype ( 1.3.6.1.1.1.1.13 NAME 'memberNisNetgroup'
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
attributetype ( 1.3.6.1.1.1.1.15 NAME 'ipServicePort'
attributetype ( 1.3.6.1.1.1.1.16 NAME 'ipServiceProtocol'
attributetype ( 1.3.6.1.1.1.1.17 NAME 'ipProtocolNumber'
attributetype ( 1.3.6.1.1.1.1.18 NAME 'oncRpcNumber'
attributetype ( 1.3.6.1.1.1.1.19 NAME 'ipHostNumber'
attributetype ( 1.3.6.1.1.1.1.20 NAME 'ipNetworkNumber'
attributetype ( 1.3.6.1.1.1.1.21 NAME 'ipNetmaskNumber'
attributetype ( 1.3.6.1.1.1.1.22 NAME 'macAddress'
attributetype ( 1.3.6.1.1.1.1.23 NAME 'bootParameter'
attributetype ( 1.3.6.1.1.1.1.24 NAME 'bootFile'
attributetype ( 1.3.6.1.1.1.1.26 NAME 'nisMapName'
attributetype ( 1.3.6.1.1.1.1.27 NAME 'nisMapEntry'
```

Esquema InetOrgPerson

- O RFC2798 (https://tools.ietf.org/html/rfc2798) indica que o propósito deste esquema é almacenar información xeral sobre as persoas.

- Posúe un único obxecto de clase

```
objectclass     ( 2.16.840.1.113730.3.2.2  NAME 'inetOrgPerson'
```

- Finalmente **os atributos**, entre eles:
  - **jpegPhoto**: almacénase unha imaxe jpeg en formato base64 (http://es.wikipedia.org/wiki/Base64). Ou sexa o valor dese atributo é un valor binario e non ASCII.

```
( 2.16.840.1.113730.3.1.1 NAME 'carLicense'
( 2.16.840.1.113730.3.1.2 NAME 'departmentNumber'
( 2.16.840.1.113730.3.1.241 NAME 'displayName'
( 2.16.840.1.113730.3.1.3 NAME 'employeeNumber'
( 2.16.840.1.113730.3.1.4 NAME 'employeeType'
( 0.9.2342.19200300.100.1.60 NAME 'jpegPhoto'
( 2.16.840.1.113730.3.1.39 NAME 'preferredLanguage'
( 2.16.840.1.113730.3.1.40 NAME 'userSMIMECertificate'
( 2.16.840.1.113730.3.1.216 NAME 'userPKCS12'
```

TAMÉN PODES VER...

No seguinte documento pódese ver unha introdución ao LDAP e como estenderon o esquema da universidade Carlos III de Madrid:
http://www.rediris.es/ldap/doc/ldap-intro.pdf

-- Antonio de Andrés Lema e Carlos Carrión Álvarez