Ferramentas para administración do LDAP: ldapscripts, LDAP Account Manager (LAM) e JXplorer

Sumario

Introdución

- Como vimos no apartado anterior traballar con ficheiros LDIF é un chisco enguedellado.
- Neste apartado imos facer unha breve reseña sobre algunhas ferramentas que podemos utilizar para administrar o servidor LDAP de forma xenérica, para introducir, buscar e extraer información, mantelo en óptimo funcionamento, etc.

Administración mediante scripts

- O paquete **ldapscripts** inclúe unha serie de scripts para administrar de forma sinxela os usuarios e grupos almacenados no servidor LDAP.
- Este paquete proporciona scripts para xestionar contas tipo POSIX (usuarios, grupos e máquinas) no directorio activo.

Instalación do paquete ldapscripts

En primeiro lugar teremos que instalar en **dserver00** o paquete:

```
apt-get install ldapscripts
```

- A continuación temos que editar o ficheiro de configuración /**etc/ldapscripts/ldapscripts.conf** de acordo ás preferencias do noso servidor LDAP, descomentando e modificando os seguintes parámetros:

```
SERVER="ldap://localhost"
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
SUFFIX="dc=iescalquera,dc=local"
GSUFFIX="ou=grupos"
USUFFIX="ou=usuarios"
MSUFFIX="ou=maquinas"
...
BINDDN="cn=admin,dc=iescalquera,dc=local"
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
...
CREATEHOMES="yes"
```

- Para rematar a configuración do paquete
  - introduciremos no ficheiro **/etc/ldapscripts/ldapscripts.passwd** o contrasinal para conectarse ao servidor LDAP
  - Configuramos que so root poida acceder ao ficheiro:

```
sh -c "echo -n 'abc123.' > /etc/ldapscripts/ldapscripts.passwd"
chmod 400 /etc/ldapscripts/ldapscripts.passwd
```

- Agora temos moitos comandos que comezan por ldap (Lembrar premer TAB 2 veces).

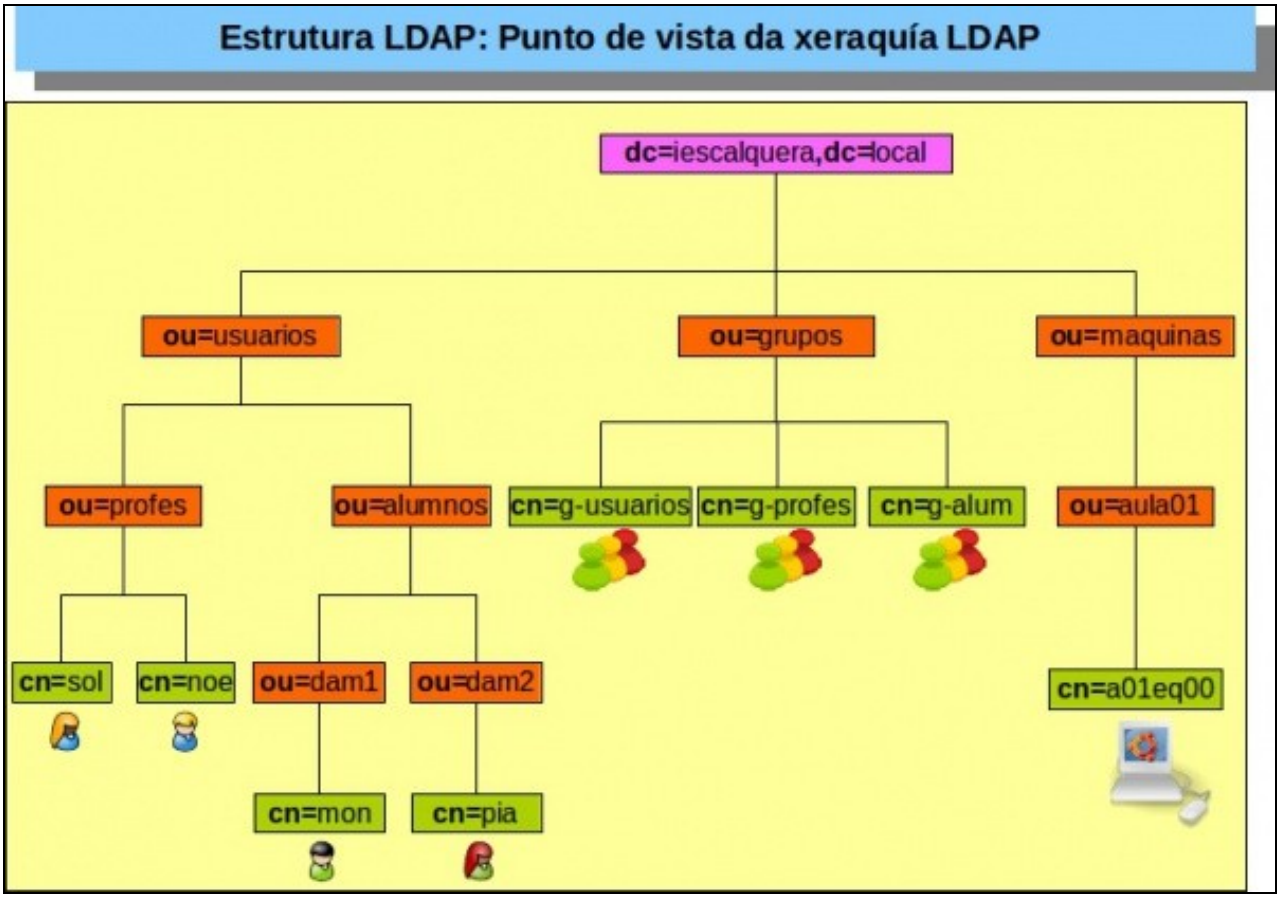
- Pararse un minuto a mirar os seus nomes, onde se pode comprobar que son bastante intuitivos.
- Lembrar que algúns son do paquete *ldap-utils*:

```
root@dserver00:~# ldap
ldapadd                 ldapdeleteuserfromgroup  ldapmodrdn
ldapaddgroup            ldapexop                 ldappasswd
ldapaddmachine          ldapfinger               ldaprenamegroup
ldapadduser             ldapgid                  ldaprenamemachine
ldapaddusertogroup      ldapid                   ldaprenameuser
ldapcompare             ldapinit                 ldapsearch
ldapdelete              ldapmodify               ldapsetpasswd
ldapdeletegroup         ldapmodifygroup          ldapsetprimarygroup
ldapdeletemachine       ldapmodifymachine        ldapurl
ldapdeleteuser          ldapmodifyuser           ldapwhoami
```

Xestión de usuarios e grupos

- A continuación móstrase o uso dos scripts do paquete para crear, cambiar o contrasinal e borrar un usuario, así como crear e borrar un grupo e engadir e eliminar usuarios a un grupo:

- Pero temos un problema:
  - Os scripts traballan directamente con tres OUs específicas: usuarios, grupos e maquinas.
  - Eses scripts non traballan cos obxectos que estean contidos en fillos desas OUs.
  - Por exemplo se observamos o noso DIT:



- Vemos que non podemos dar usuarios de alta nas OUs profes, dam1 e dam2, só os podemos dar de alta con estes scripts na OU usuarios.
- Estes scripts veñen ben cando se trata de organizacións pequenas que non teñen clasificados os usuarios e todos están xuntos na OU usuarios.
- O mesmo pasa coas máquinas.
- En cambio cos grupos, neste caso, si que podemos dar de alta. Neste caso o grupo **g-alum**. Non confuncir coa OU alumnos.

```
ldapaddgroup g-alum
Successfully added group g-alum to LDAP
```

- A continuación ponse a modo de exemplo unha ficticia xestión de usuarios, que vai traballar coa OU usuarios (supoñendo que previamente creamos no LDAP os grupos *grupo1-ficticio* e *grupo2-ficticio* con *ldapaddgroup*):

```
ldapadduser pepe grupo1-ficticio
Successfully added user pepe to LDAP
Successfully set password for user pepe
Successfully created home directory for user pepe

ldapsetpasswd pepe
Changing password for user uid=pepe,ou=usuarios,dc=iescalquera,dc=local
New Password:
Retype New Password:
Successfully set password for user uid=pepe,ou=usuarios,dc=iescalquera,dc=local

ldapaddusertogroup pepe grupo2-ficticio
Successfully added user pepe to group grupo2-ficticio
```

NOTAS:

- En /**home** do servidor crearíase unha carpeta persoal para *pepe*, pero non nos clientes, iso verase na parte III do curso.
- Para comprobar o resultado, agora poderiamos iniciar sesión, en modo consola, non en modo gráfico, que se verá na parte III do curso, co usuario *pepe* dende un equipo configurado para tomar os usuarios do LDAP e utilizar o comando *id* para ver os grupos aos que pertence.

Imos ver agora como borrar o usuario e grupo creados:

```
ldapdeleteuserfromgroup pepe grupo2-ficticio
Successfully deleted user pepe from group grupo2-ficiticio

ldapdeleteuser pepe
Successfully deleted user uid=pepe,ou=usuarios,dc=iescalquera,dc=local from LDAP

ldapdeletegroup grupo1-ficiticio
Successfully deleted group cn=grupo1-ficiticio,ou=grupos,dc=iescalquera,dc=local from LDAP
```

NOTA: Observar como se eliminaría o usuario *pepe*, pero a súa carpeta carpeta persoal seguiría no servidor en /**home**. No cliente xa non tiña carpeta.

Unha opción que pode ser moi útil con estes scripts é a de definir un modelo para os valores por defecto que terán os novos usuarios, grupos e máquinas. Estes modelos deben ser almacenados en ficheiros con formato LDIF (en */usr/share/doc/ldapscripts/examples* hai exemplos destes ficheiros coa estensión *.template.sample*). No ficheiro de configuración */etc/ldapscripts/ldapscripts.conf* podemos indicar os ficheiros de modelos que queiramos utilizar nos parámetros **UTEMPLATE** (usuarios), **GTEMPLATE** (grupos) e **MTEMPLATE** (máquinas).

LDAP Account Manager (LAM)

Instalación de LAM

- Outra ferramenta que podemos utilizar para administrar os usuarios e grupos do servidor LDAP é LDAP Account Manager.
- Instálase en calquera equipo o paquete **ldap-account-manager**, neste caso imos instalalo no servidor *dserver00*. Así que, introducimos o comando:

```
apt-get install ldap-account-manager

Lendo as listas de paquetes... Feito
Construindo a árbore de dependencias
Lendo a información do estado... Feito
Instalaranse os seguintes paquetes extra:
```

```
 apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common
 libapache2-mod-php5 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
 libaprutil1-ldap libonig2 libqdbm14 php-fpdf php5 php5-cli php5-common
 php5-gd php5-ldap
Paquetes suxeridos:
 apache2-doc apache2-suexec apache2-suexec-custom php5-mcrypt
 ldap-account-manager-lamdaemon php-pear ttf2pt1
Os seguintes paquetes NOVOS hanse instalar:
 apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common
 ldap-account-manager libapache2-mod-php5 libapr1 libaprutil1
 libaprutil1-dbd-sqlite3 libaprutil1-ldap libonig2 libqdbm14 php-fpdf php5
 php5-cli php5-common php5-gd php5-ldap
0 anovados, 18 instalados, Vanse retirar 0 e deixar 0 sen anovar.
Ten que recibir 16,8 MB de arquivos.
Despois desta operación ocuparanse 57,0 MB de disco adicionais.
Quere continuar [S/n]?
```

- Observar que vai instalar o servidor web apache.

Por se non estiveran instaladas as extensións XML e ZIP de PHP no servidor:

```
apt-get install php-xml
apt-get install php-zip
```

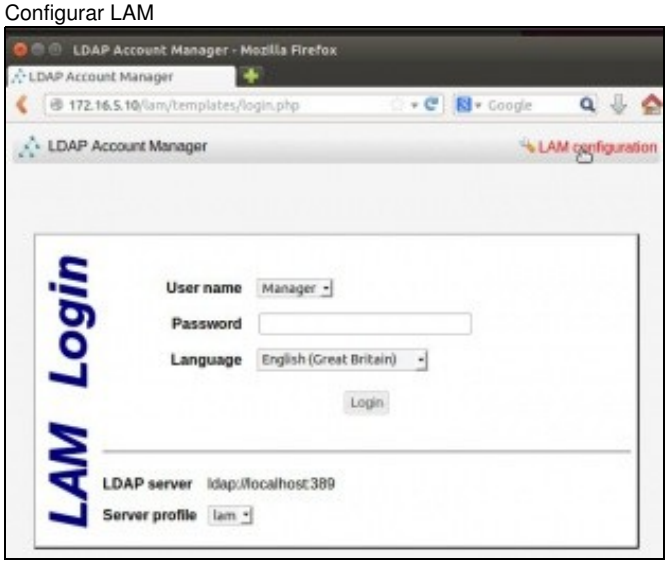
Reiniciamos o servizo

```
service apache2 restart
```

Configuración de LAM

- Agora toca configurar a utilidade lam para que manexe o noso directorio LDAP.

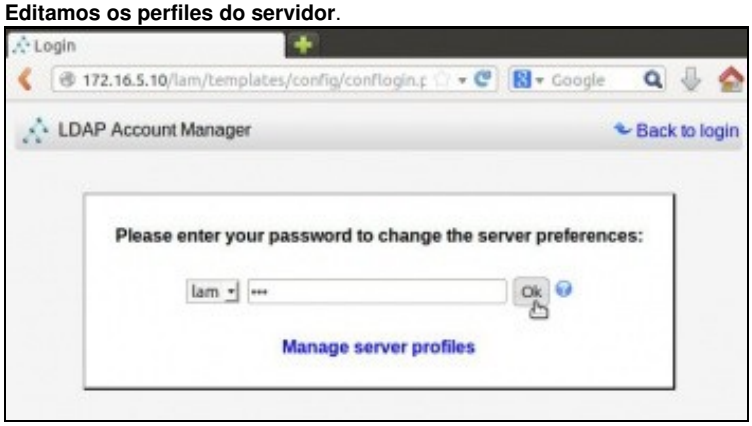
- Ao rematar a instalación podemos conectarnos a el dende calquera equipo cun navegador web.
  - Podemos facelo dende **uclient01**: **http://ip_ou_nomeservidor/lam**
  - Se temos Rede NAT de VirtualBox, podemos redirixir un porto, por exemplo 8080, ao porto 80 da IP do servidor
  - Para conectarse dende o exterior sería, neste caso: **http://ip_do_equipo_real:8080/lam**
  - Nun servidor real, sería moi recomendable configurar o servidor apache para recibir conexións seguras e usar **https** en lugar de **http**

- Configurar LAM
- 

Unha vez conectados á utilidade, prememos en **LAM configuration**.

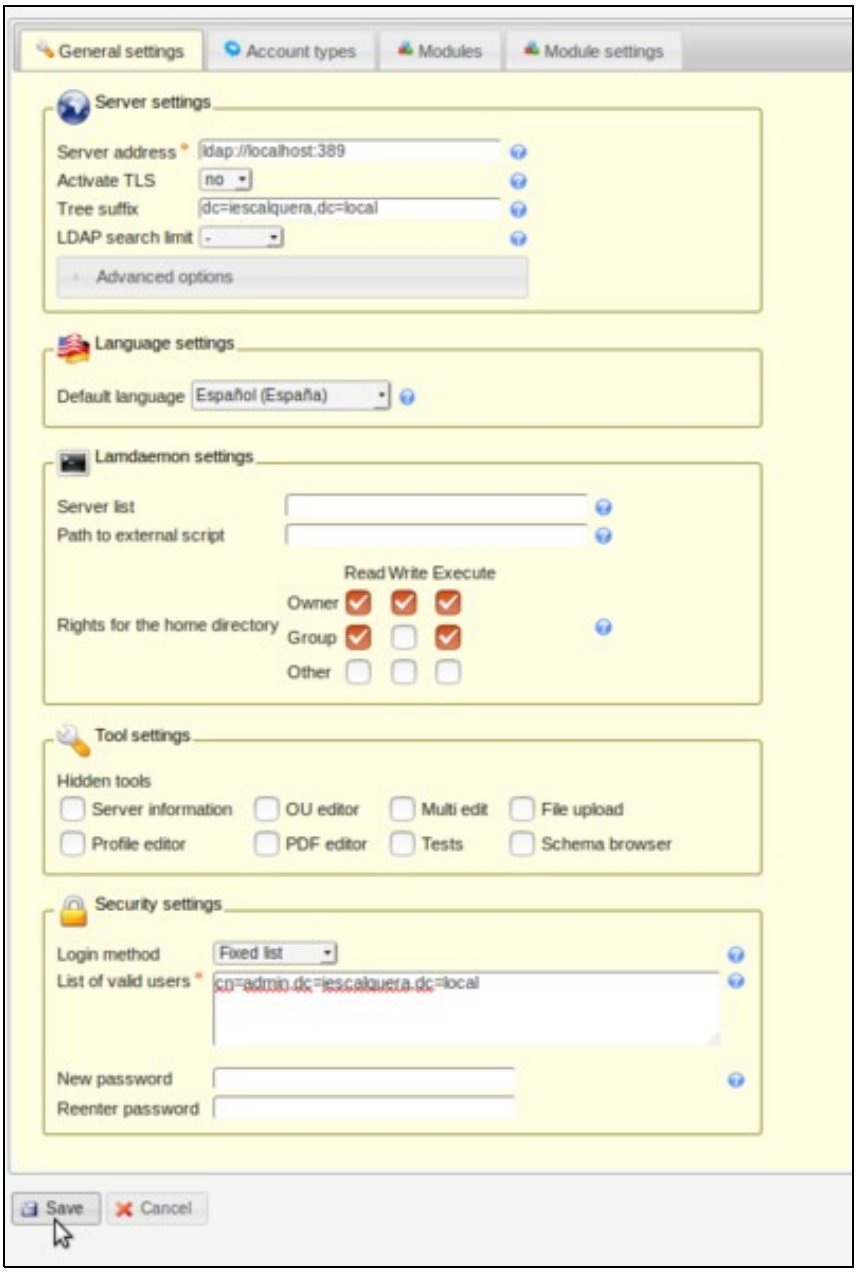
- 

Editamos os perfiles do servidor.

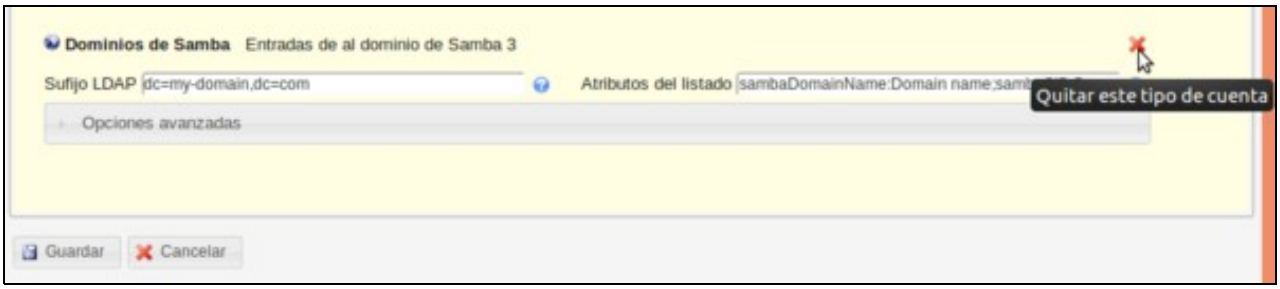
- 

O contrasinal por defecto da utilidade LAM é: **lam**. Pódese cambiar.

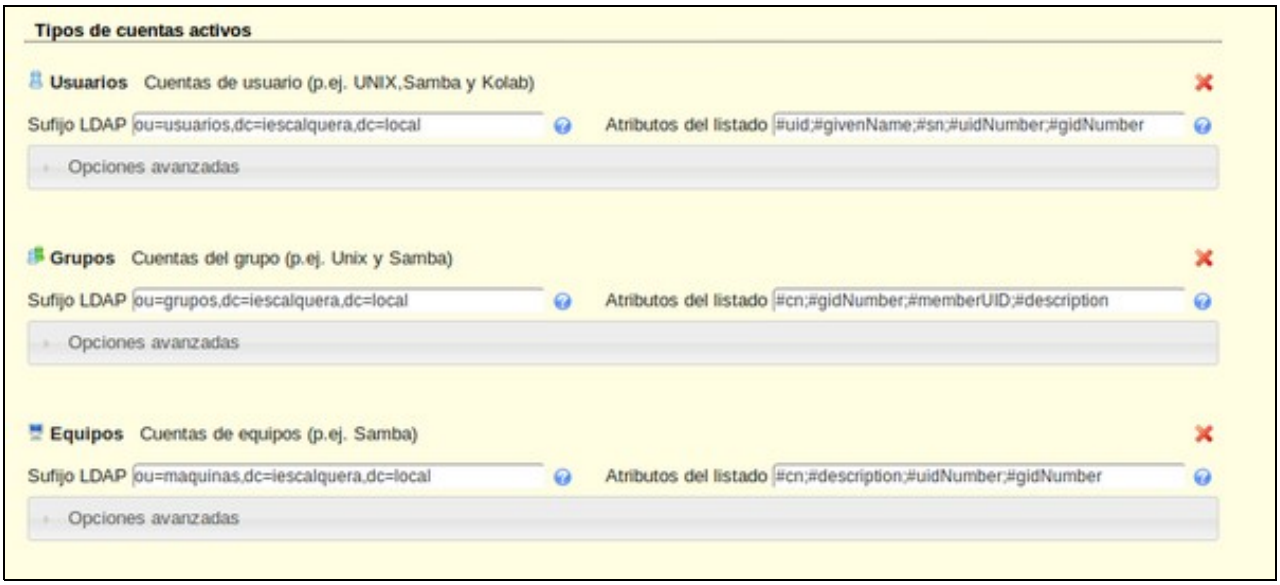
- Na lapela **General Settings**:
    - **Tree suffix**: Para introducir o sufixo do noso directorio (**dc=iescalquera,dc=local**).
    - **Default language**: Español.
    - **List of valid users**: Poremos o DN do usuario administrador do LDAP (**cn=admin,dc=iescalquera,dc=local**)
    - Podemos cambiar o contrasinal para acceder a esta páxina de configuración introducindo nas dúas últimas caixas de texto un novo.


General settings
Account types
Modules
Module settings
Server settings
Server address *
ldap://localhost:389
Activate TLS
no
Tree suffix
dc=iescalquera,dc=local
LDAP search limit
-
Advanced options
Language settings
Default language
Español (España)
Lamdaemon settings
Server list
Path to external script
Read Write Execute
Rights for the home directory
Owner
Group
Other
Tool settings
Hidden tools
Server information
OU editor
Multi edit
File upload
Profile editor
PDF editor
Tests
Schema browser
Security settings
Login method
Fixed list
List of valid users *
cn=admin,dc=iescalquera,dc=local
New password
Reenter password
Save
Cancel

- Se gardamos os cambios, agora xa podemos ver a páxina de configuración en castelán.
- Na lapela **Tipos de cuentas**, dentro do apartado **Tipos de cuentas activos**:
    - Borramos ao final da páxina o tipo de conta: **Dominios de Samba** que usaremos na parte V do curso, se é que ese tipo de conta estivese activo.

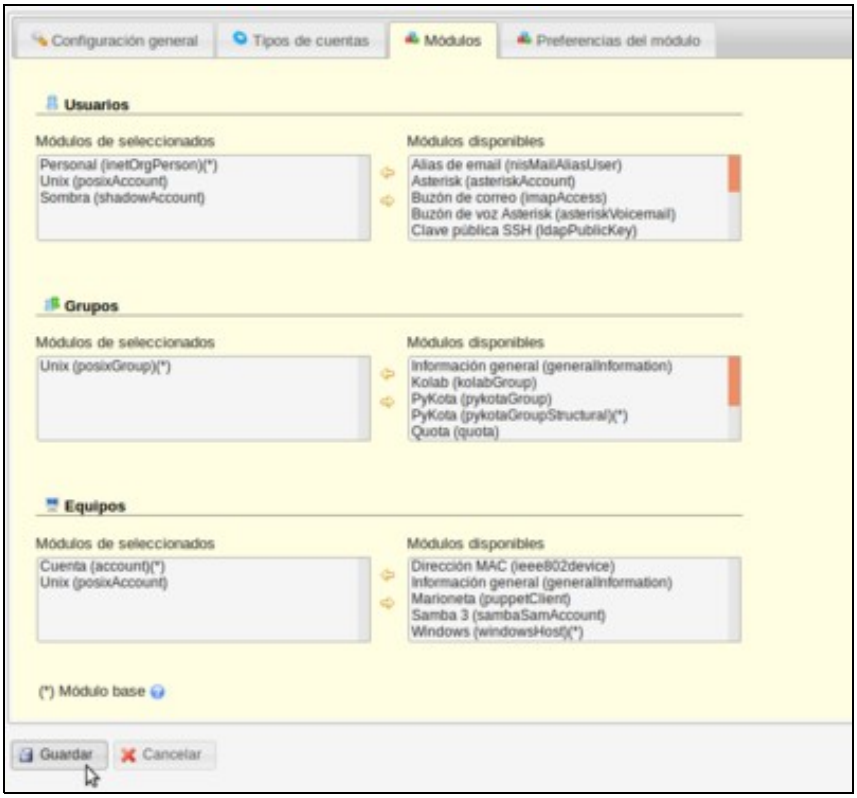


- Na mesma lapela **Tipos de cuenta**, dentro do apartado **Tipos de cuentas activos**:
    - **Usuarios -> Sufijo LDAP**: ou=usuarios,dc=iescalquera,dc=local
    - **Grupos -> Sufijo LDAP**: ou=grupos,dc=iescalquera,dc=local
    - **Equipos (hosts) -> Sufijo LDAP**: ou=maquinas,dc=iescalquera,dc=local
        - ◊ Esta última non a imos usar por agora, pero deixámola configurada.
        - ◊ Esta última non a imos usar por agora, pero deixámola configurada.
        - ◊ Se non está activa, engadila a "Tipos de conta activas"



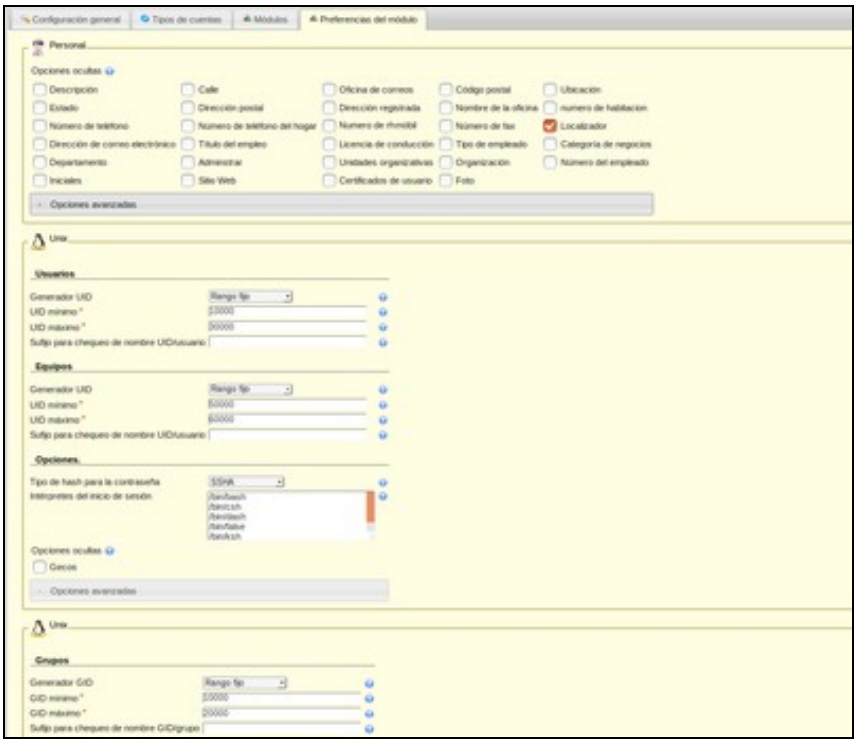
- Na lapela **Módulos**, en Usuarios, Grupos e Equipos retiramos, se estivera presente, o módulo Samba 3:

- A seguinte imaxe amosa Usuarios, Grupos e Equipos sen o módulo SAMBA 3. No caso dos Equipos asegurarse de que stean presentes os módulos Account e Unix.



- **Prememos en salvar agora, ou cando vexamos a seguinte lapela**.

- Na lapela **Preferencias del módulo** podemos ver que opcións podemos ocultar, en UID e GID podemos ver en que números se comeza para ser asignados a usuarios e grupos.

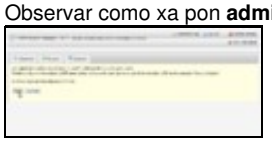
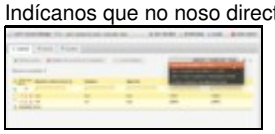


- Podemos revisar a configuración sempre que o desexemos.

Iniciar sesión por primeira vez

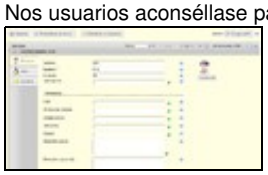
- Imos revisar todo o realizado até agora con *ldap-utils* e *ldapscript* no directorio LDAP.

- Revisión do realizado
- 

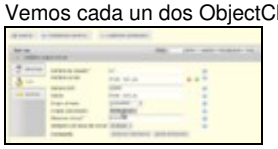
Observar como xa pon **admin** como nome de usuario para conectarse ao directorio LDAP.
- 
Indícanos que no noso directorio LDAP non hai unha rama **máquinas** e se desexamos que sexa creada. Indicamos que si.
- 
Observamos os usuarios creados até agora. Observar que podemos seleccionar dentro de que OU desexamos velos/crealos.
- 
Os grupos creados até agora e os seus usuarios que os teñen como grupos secundarios.

- 

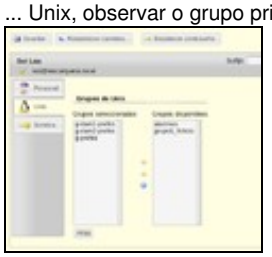
Nos usuarios aconséllase pararse a analizar os campos. Se editamos un usuario.

- 

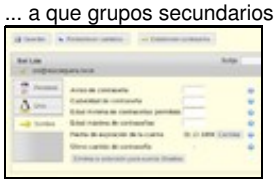
Vemos cada un dos ObjectClass: Personal ...

- 

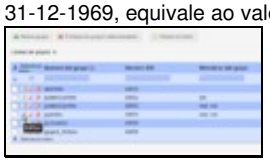
... Unix, observar o grupo primario. Podemos editar os grupos para ver ...

- 

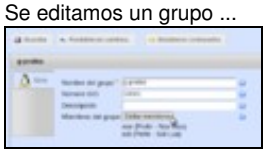
... a que grupos secundarios pertence ese usuario.

- 

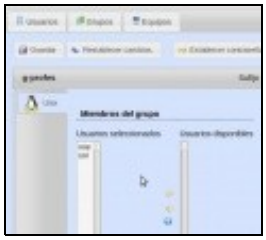
En **Sombra** pódese bloquear o contrasinal, cambiar, poñer data caducidade. Observar como indica LAM que o contrasinal nunca caduca: 31-12-1969, equivale ao valor **shadowExpire: -1** que poñíamos nos ficheiros LDIF.

- 

Se editamos un grupo ...

- 

... vemos os seus atributos e valores. Se editamos os usuarios ...

- 

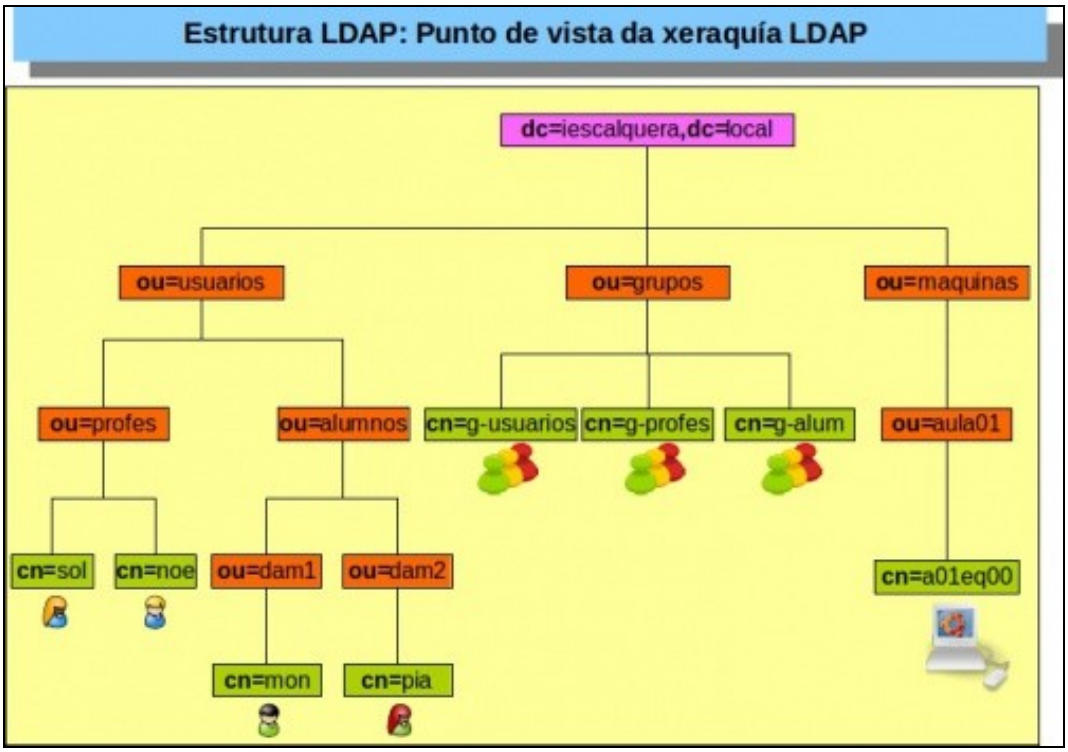
... vemos os seus membros.

- 

Se prememos en **Visor del árbol** vemos toda a estrutura en formato DIT.

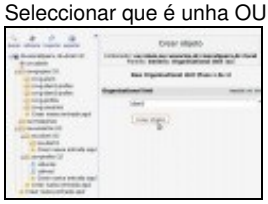
Crear OUs en LAM

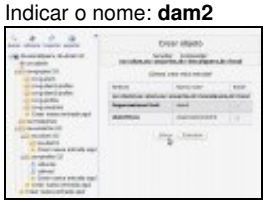
- Imos crear unha das OUs que nos falta: **dam2**.



- Crear OU dam2
- 

  Premer en **Crear nueva entrada aquí** dentro da OU=alum.
- 

  Seleccionar que é unha OU xenérica.
- 

  Indicar o nome: **dam2**
- 

  Gardar
- 

OU creada e á dereita amósase todo o que se pode facer nesa OU.

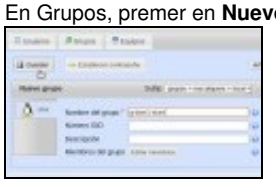
Crear grupos en LAM. Exercicio

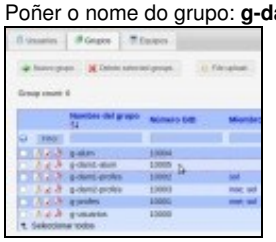
- Imos agora crear os grupos que faltan por crear: *g-dam1-alum* e *g-dam2-alum*

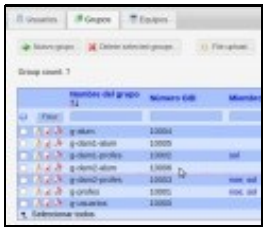
USUARIOS E GRUPOS

Grupos Usuarios	Nome Completo	g-usarios (10000)	g-profes (10001)	g-dam1-profes (10002)	g-dam2-profes (10003)	g-alum (10004)	g-dam1-alum (10005)	g-dam2-alum (10006)
Descric.		Tódolos usuarios de LDAP	Todo o profesorado	Profesorado de 1º da DAM	Profesorado de 2º DAM	Todo o alumnado	Alumnado de 1º da DAM	Alumnado de 2º da DAM
sol (10000)	Profe - Sol Lúa	✔(1º)	✔	✔	✔			
noe (10001)	Profe - Noé Ras	✔(1º)	✔		✔			
mon (10002)	Dam1 - Mon Mon	✔(1º)				✔	✔	
tom (10003)	Dam1 - Tom Tom	✔(1º)				✔	✔	
pia (10004)	Dam2 - Pía Glez	✔(1º)				✔		✔
paz (10005)	Dam2 - Paz Fdez	✔(1º)				✔		✔

- Crear grupos
- 

  En Grupos, premer en **Nuevo grupo**.
- 

  Poñer o nome do grupo: **g-dam1-alum**. Observar que non se puxo o GID, porque ...
- 

  ... LAM créao automaticamente, observar que lle asignou o seguinte número libre: **10005**
- 

Exercicio: agora o/a lector/a debe agora crear o grupo **g-dam2-alum**.

Crear usuarios en LAM

- Lembrar como estaba organizados os usuarios:

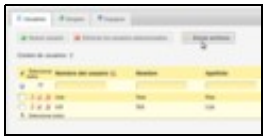
USUARIOS E GRUPOS

Grupos Usuarios	Nome Completo	g-usarios (10000)	g-profes (10001)	g-dam1-profes (10002)	g-dam2-profes (10003)	g-alum (10004)	g-dam1-alum (10005)	g-dam2-alum (10006)
Descric.		Tódolos usuarios de LDAP	Todo o profesorado	Profesorado de 1º da DAM	Profesorado de 2º DAM	Todo o alumnado	Alumnado de 1º da DAM	Alumnado de 2º da DAM
sol (10000)	Profe - Sol Lúa	✔(1º)	✔	✔	✔			
noe (10001)	Profe - Noé Ras	✔(1º)	✔		✔			
mon (10002)	Dam1 - Mon Mon	✔(1º)				✔	✔	
tom (10003)	Dam1 - Tom Tom	✔(1º)				✔	✔	
pia (10004)	Dam2 - Pía Glez	✔(1º)				✔		✔
paz (10005)	Dam2 - Paz Fdez	✔(1º)				✔		✔

- Podemos crear usuarios en modo gráfico como se fixo cos grupos, pero imos crealos cun ficheiro CSV.
- Un ficheiro **CSV** é, en modo resumido, un ficheiro onde cada liña representa un obxecto do directorio e os seus campos están separados por comas.
- Este tipo de ficheiros son moi cómodos cando se desexan crear usuarios de forma masiva.
- So hai que poñer unha liña na cabeceira cos campos (separados por comas) que vai conter o ficheiro.
- E debaixo unha liña por cada obxecto, cos valores dos campos separados por comas.

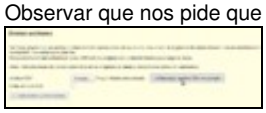
- Aconséllase traballar nunha folla de cálculo, pois logo podemos exportar o ficheiro a formato CSV, que é un documento de texto, onde cada campo da folla se converterá nun campo separado por comas no ficheiro CSV.
- É moi recomendable que se conserven os dous ficheiros: o da folla de cálculo (xls ou ods) e o CSV. O primeiro sobre todo porque pode conter fórmulas para construír os valores dos distintos campos.
- No seguinte enlace está un ficheiro en formato **ods** (Folla de cálculo de LibreOffice) que se pode usar como base para crear os usuarios:
  - Formato ods: usuarios.ods
  - Formato Google Drive

- Dos usuarios que faltan por crear, crearemos a *Mon*, *Tom* e *Pía*. Imos deixar polo momento sen crear a *Paz*.

- Crear usuarios con CSV
- 

  En **Usuarios** premer en **File upload**.
- 

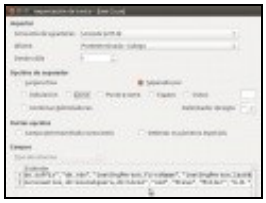
Observar que nos pide que tipo de conta e módulos. Premer en **Aceptar**.

- 

Se prememos en **Descargar archivo csv de ejemplo** podemos ver como se constrúe o ficheiro.

- 

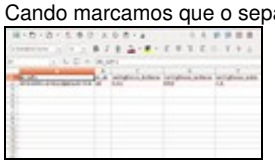
Abrímolo con LibreOffice ou Excel.

- 

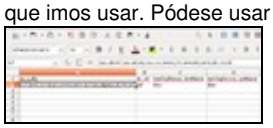
Observar que dentro dun campo pode haber comas, nese caso o campo vai entre comillas.

- 

Cando marcamos que o separador é a coma, vemos como se van construír as columnas.

- 

E aí temos o ficheiro exemplo, do que imos eliminar varias columnas/campos por non usalas. O ficheiro que está arriba amosa os campos que imos usar. Pódese usar ese ficheiro de base.

- 

Unha vez que configuremos a folla de cálculo como desexemos (exemplo o ficheiro de arriba). Imos crear o usuario *Mon*.

- 

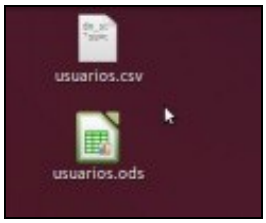
Gardamos a folla como formato Excel ou Calc e tamén en formato CSV. Marcar editar a configuración do filtro.

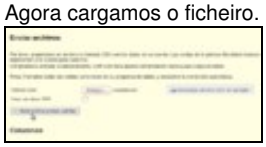
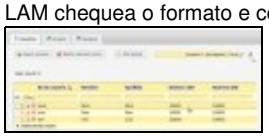
- 

Advertencia de LibreOffice de que non imos usar o seu formato.

- 

Vemos que o delimitador de campo é coma e o texto vai ir entre comillas naqueles casos nos que conteña comas.

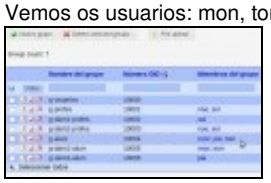
- 

Os dous ficheiros creados. A folla de cálculo será sempre para crear os nosos usuarios e unha vez composta gardámola como CSV.
- 
Editamos cun editor de texto o ficheiro CSV para ver o seu contido.
- 
Agora cargamos o ficheiro. Navegamos até el ...
- 
... e subímolo. Antes se se quere pódese ver o ficheiro ldif asociado.
- 
LAM chequea o formato e contido do ficheiro e se todo vai ben esa é mensaxe. Subímolo.
- 
E aí vemos a Mon co seu UID (10002), que non se lle indicou no ficheiro.
- 
E vémolo dentro da súa OU ...
- 
... e do seu grupo secundario.

Exercicio para o/a lector/a

- Agora o/a lector/a, baseándose no ficheiro **usuarios.ods** de arriba debe ser quen de crear os usuarios:
    - mon (dam1)
    - tom (*dam1*)
    - pia (*dam2*)

- Unha vez creados este debe ser o resultado.

- Resultado final
- 
Vemos os usuarios: mon, tom e pia. (Premeuse no campo Número UID, para ordenar o listado)
- 

Vemos os grupos cos seus usuarios. (Premeuse no campo Número UID, para ordenar o listado)

- 

Resultado de executar nun cliente LDAP: **getent passwd**

- 

Resultado de executar nun cliente LDAP: **getent group**

IMPORTANTE: Con **LAM** pódense crear usuario e grupos, pero non vai crear no servidor as carpetas persoais asociadas a cada usuario.

JXplorer

- Existen moitas máis ferramentas gráficas para conectarse a un servidor LDAP e manexar a información almacenada nel, e **JXplorer** é un dos máis usados. Está implementado en Java, polo que pode usado tanto dende unha máquina Windows como Linux.
- Só hai que instalala no cliente e non se precisa realizar nada no servidor.
- No noso caso ímola instalar no cliente Ubuntu Desktop (**uclient01**), e teremos que ter instalada no equipo a máquina virtual de java.
- Dende a páxina de descargas (http://jxplorer.org/downloads/users.html) pódese descargar JXplorer para distintas plataformas.
- No noso caso se alguén a instala no equipo real que lembre que precisa redirixir portos se usa Rede NAT de VirtualBox para a IP de dserver00, porto 389.

- No noso caso en **uclient01**:

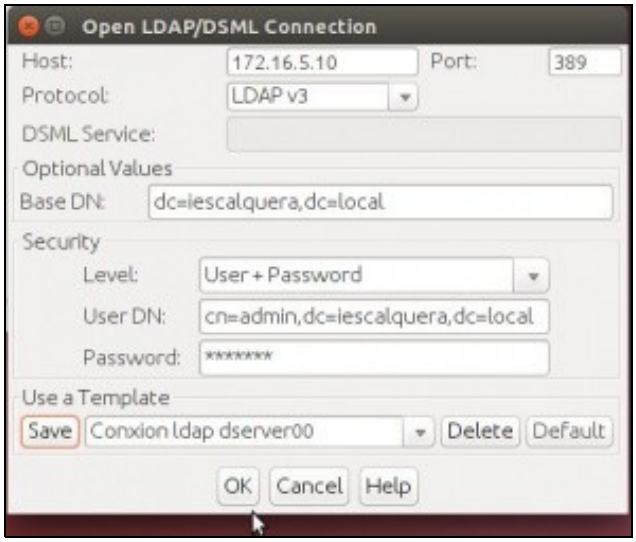
```
sudo apt-get install jxplorer
```

- Observar que xa instala os paquetes Java que precisa, se non estiveran instalados xa.

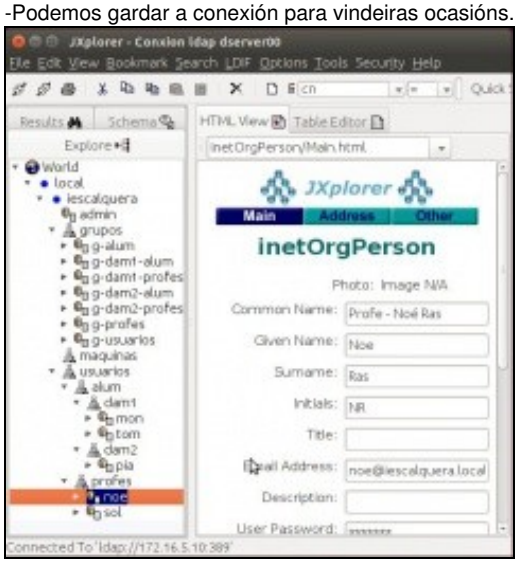
A continuación móstranse algunhas opcións do programa:

- 

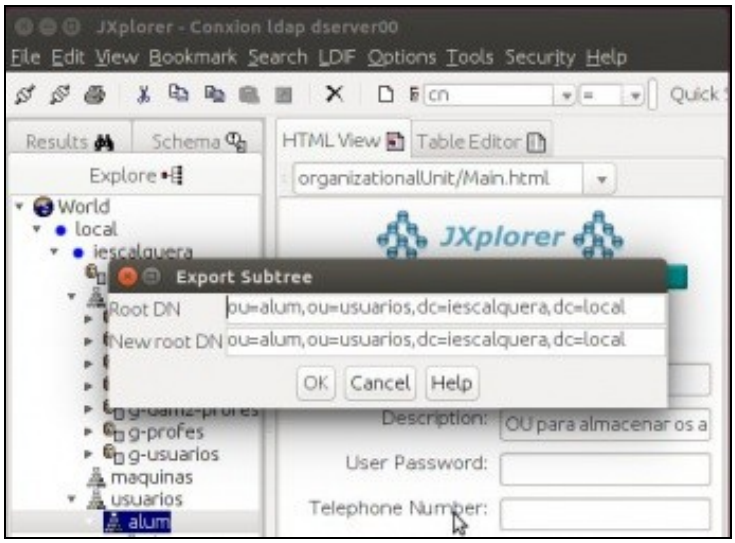
Ventá do programa antes de conectarse a ningún servidor LDAP. O primeiro botón da barra de ferramentas permítenos conectarnos a un servidor.

- 

Ventá de conexión ao servidor LDAP. Teremos que indicar
-Os datos do servidor (dirección IP, porto)
-A rama base do LDAP (no noso caso **dc=iescalquera,dc=local**)
-As credenciais para conectarnos (podemos seleccionar anónimo, pero se queremos facer modificacións no noso caso nos conectaremos como *admin*).
-Podemos gardar a conexión para vindeiras ocasións.

- 

Visualización da árbore LDAP unha vez conectados ao servidor LDAP. Podemos mover elementos dun lugar a outro arrastrándoos na visualización na árbore.

- 

O menú **LDIF** ofrece opcións como exportar todo ou unha rama do directorio a un ficheiro LDIF ou importar un ficheiro LDIF.

Instantáneas do escenario 1.E

- Ao igual que se fixo nos escenarios anteriores, convén crear a instantánea do escenario 1.E tanto no servidor *dserver00* como nos clientes *uclient01* e *uclient02*.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez