Administración dos usuarios e grupos do LDAP

Sumario

 LEMBRAR EN UBUNTU DESKTOP

Antes de comezar con esta sección é aconsellable que o usuario domine a xestión de usuarios en GNU/Linux.

Recoméndase que se revisen as seccións

- Usuarios e grupos en Ubuntu

do curso Curso Platega 08-09: Sistema operativo GNU-LINUX: UBUNTU 8.10.

Administración mediante scripts

O paquete **ldapscripts** inclúe unha serie de scripts para administrar de forma sinxela os usuarios e grupos almacenados no servidor LDAP. En primeiro lugar teremos que instalar o paquete:

```
sudo apt-get install ldapscripts
```

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

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

Para rematar a configuración do paquete, introduciremos no ficheiro **/etc/ldapscripts/ldapscripts.passwd** o contrasinal para conectarse ao servidor LDAP:

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

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:

```
sudo ldapaddgroup alumnos
Successfully added group alumnos to LDAP
```

```
sudo ldapadduser pepe alumnos
Successfully added user pepe to LDAP
Successfully created home directory for user pepe
sudo 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
sudo ldapaddusertogroup pepe profes
Successfully added user pepe to group profes
```

NOTAS:

- En /**home** do servidor creouse unha carpeta persoal para pepe, pero non nos clientes, iso verase na parte III do curso.
- Para comprobar o resultado, agora podemos 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:

```
$ id
uid=10001(pepe) gid=10001(alumnos) grupos=10000(profes),10001(alumnos)
```

Imos agora a ver como borrar o usuario e grupo creados:

```
sudo ldapdeleteuserfromgroup pepe profes
Successfully deleted user pepe from group profes
sudo ldapdeleteuser pepe
Successfully deleted user uid=pepe,ou=usuarios,dc=iescalquera,dc=local from LDAP
sudo ldapdeletegroup alumnos
Successfully deleted group cn=alumnos,ou=grupos,dc=iescalquera,dc=local from LDAP
```

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

Unha opción que pode ser moi útil con estes scripts é o 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).

Administración con webmin

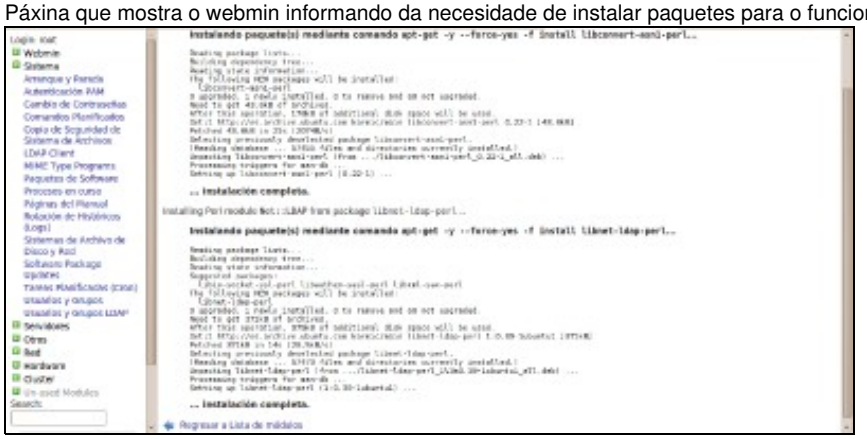
O webmin inclúe un módulo moi cómodo para facer a xestión de usuarios e grupos do LDAP. Atoparémolo na categoría de **Sistema**, como nome de **Usuarios y Grupos LDAP**. Se non aparecese aquí, teremos que picar na opción de **Refresh Modules** para que detecte agora que o serivdor LDAP está instalado e que este módulo xa ten utilidade.

Configuración inicial do módulo de Usuarios e grupos LDAP

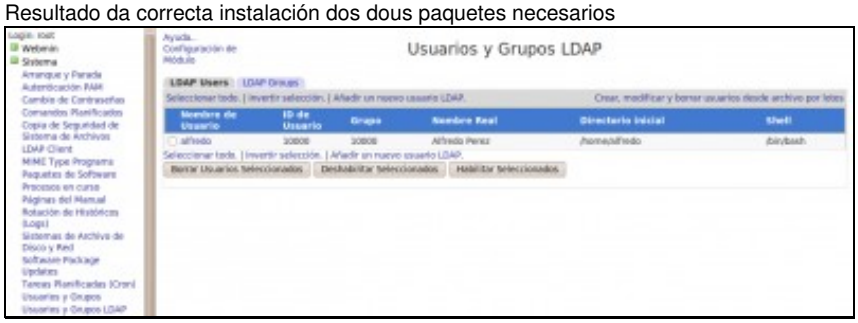
Se accedemos ao módulo, veremos que hai un software para o uso do protocolo LDAP con scripts en PERL (que é a linguaxe de programación na que está escrito o webmin) que non está instalado. Picando no enlace **Pulse aquí** o webmin instalará usando o comando *apt-get* os paquetes necesarios:

- 

Páxina que mostra o webmin informando da necesidade de instalar paquetes para o funcionamento do módulo

- 

Resultado da correcta instalación dos dous paquetes necesarios

- 

Unha vez instalados os paquetes, xa podemos acceder ao módulo e visualizar os usuarios e grupos do LDAP

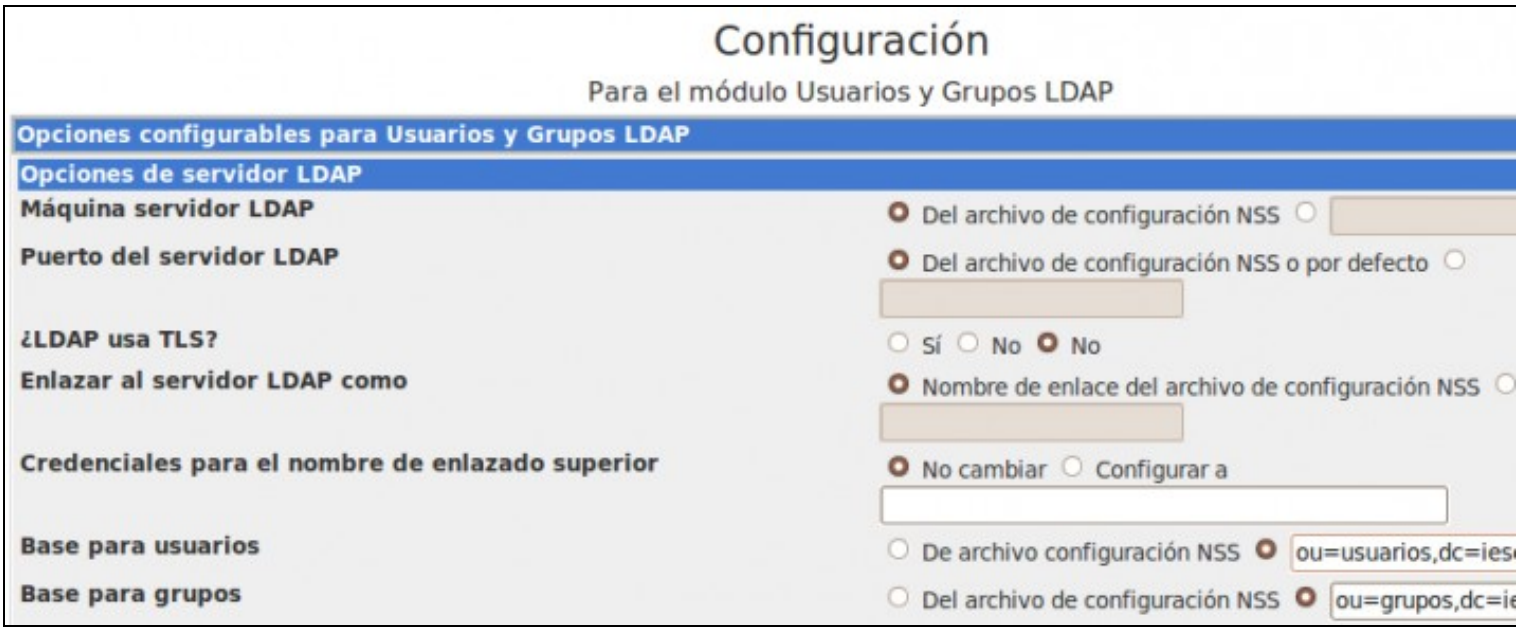
Neste momento o módulo de xestión de usuarios e grupos LDAP do webmin xa é totalmente operativo e podemos agregar, editar e borrar usuarios e grupos no noso servidor LDAP. Pero imos realizar un par de cambios na configuración do módulo para afinar o seu funcionamento. Vexamos cales son os problemas...

É moi habitual que as distribucións de Linux comecen a asignar os identificadores de usuario para os novos usuarios locais no número 500 ou 1000 (este é o caso de Ubuntu). Por iso, é conveniente que os usuarios do LDAP non coincidan no seu identificador de usuario con estes usuarios, xa que entón cando iniciemos sesión no equipo cliente asignaranse os permisos e privilexios do usuario local ao usuario do dominio (téñase en conta que a xestión de permisos faise en Linux en base ao *uid* do usuario); e o mesmo poderíamos dicir dos grupos. Polo tanto o que faremos é configurar o módulo do webmin para que os novos usuarios e grupos que se creen no LDAP se lles asignen identificadores a partir do número 10000, e non haberá coincidencia de *ids* entre os usuarios locais dos equipos e os do dominio (se nos fixamos no ficheiro de configuración de *ldapscripts*, este é o identificador mínimo para usuarios e grupos que se establece por defecto).

Por outra banda, o módulo toma a rama do LDAP base para usuarios e a rama base para grupos do ficheiro de configuración do cliente LDAP, que será no noso caso *dc=iescalquera,dc=local*, cando nós queremos almacenar os usuarios e os grupos en subramas distintas do LDAP (*ou=usuarios,dc=iescalquera,dc=local* e *ou=grupos,dc=iescalquera,dc=local*). Hai que dicir que isto non é obrigatorio e poderiamos traballar perfectamente almacenando os usuarios e os grupos directamente na rama raíz do LDAP, pero para ter un pouco máis ordenado o directorio estruturarémolo deste xeito.

Así que picaremos no enlace de **Configuración de módulo** que atopamos na parte superior da páxina e accedemos á unha páxina na que podemos establecer un bo número de parámetros acerca do comportamento do módulo. En concreto, imos modificar os seguintes:

- No apartado de **Opciones de servidor LDAP**, a **Base para usuarios** e a **Base para grupos**:

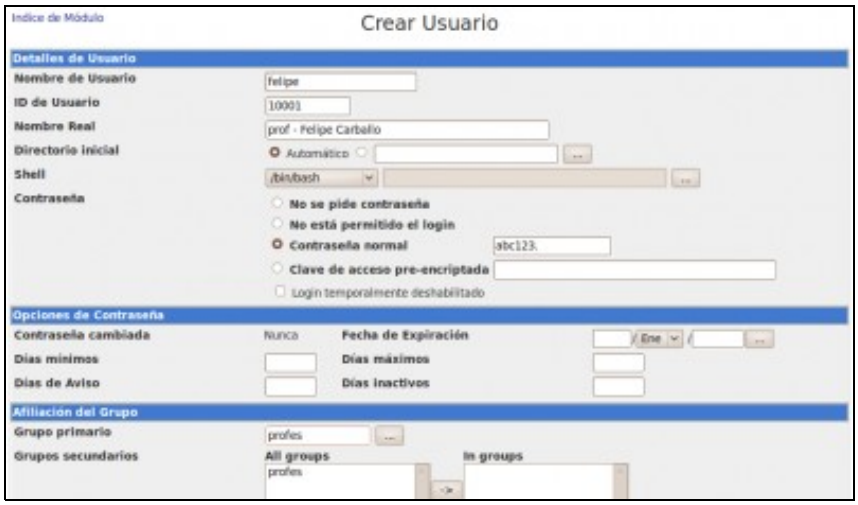


- Dentro do apartado de **Opciones para usuario nuevo** o **UID menor para nuevos usuarios** e o **GID menor para nuevos grupos**:

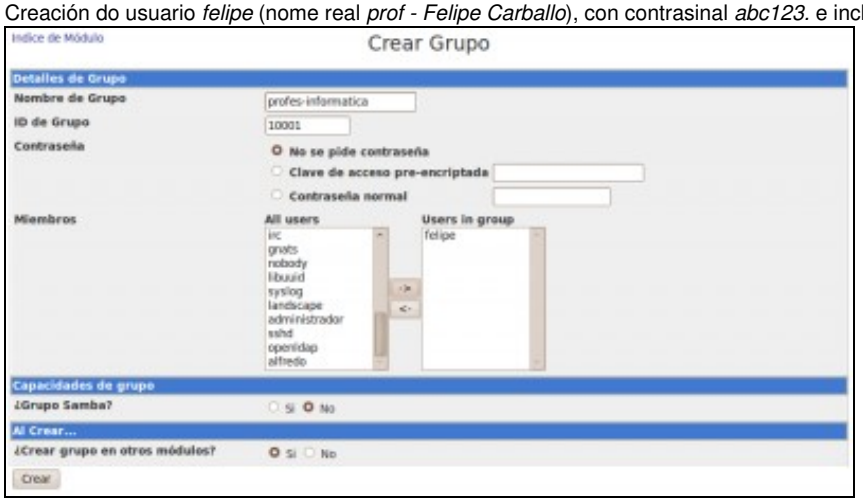
- Picamos no botón de **Salvar** para gardar esta configuración.

Administración de usuarios e grupos do LDAP con webmin

A administración de usuarios e grupos do LDAP con este módulo é moi simple, e só teremos que usar os enlaces para a creación de novos usuarios e grupos, e picar sobre o nome dun usuario ou un grupo para editar as súas propiedades ou eliminalo. A continuación móstranse un par de exemplos da creación dun usuario e dun grupo:

- 

Creación do usuario *felipe* (nome real *prof - Felipe Carballo*), con contrasinal *abc123.* e incluído no grupo *profes*

- 

Creación do grupo *profes-informatica*, e inclusión do usuario *felipe* neste grupo

Creación masiva de usuarios

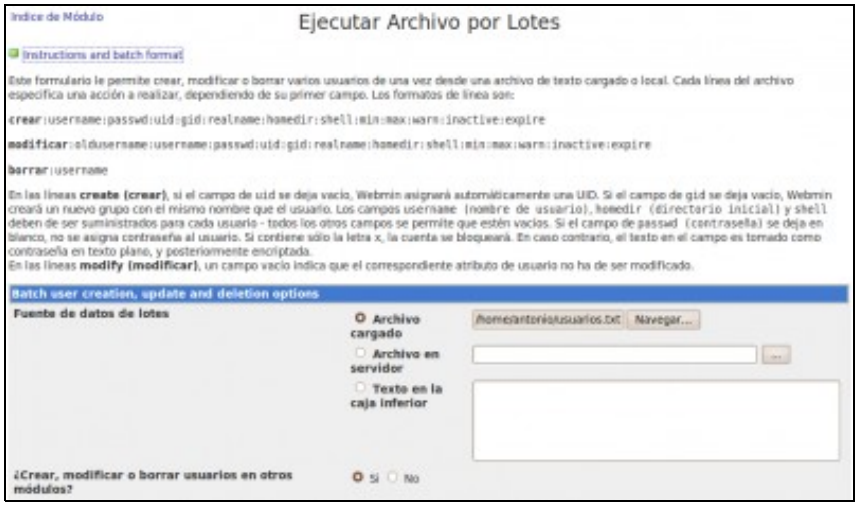
O módulo de usuarios e grupos LDAP do webmin ofrece a opción de **Crear, modificar e borrar usuarios dende un arquivo por lotes**. Con ela podemos subir ao servidor un ficheiro de texto dos datos dunha serie de usuarios (unha liña por cada usuario) e automatizar a creación e modificación masiva no LDAP. Isto é enormemente útil cando o número de usuarios que hai que manexar é grande, e pode aforrar moito tempo de administración.

Por exemplo, un ficheiro para a creación de dous usuarios podería ter o seguinte contido (ollo, as liñas deben comezar por *create*, *modify* ou *delete*, e non por *crear*, *modificar* e *borrar* como aparece nas instrucións traducidas ao castelán):

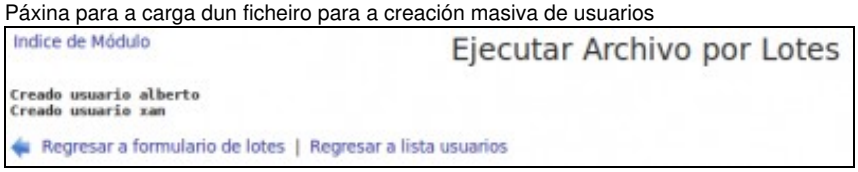
```
create:alberto:abc123.::10000:prof - Alberto Miguez:/home/alberto:/bin/bash:::::
create:xan:abc123.::10000:prof - Xan Pereira:/home/xan:/bin/bash:::::
```

Nas instrucións da páxina explícase que campos son necesarios e cales se poden deixar en branco, como se fai con algúns campos neste exemplo. Por suposto, en cada caso concreto e dependendo do formato do ficheiro que se nos proporcione para a creación de usuarios, haberá que buscar o método máis ou menos automatizado de crear un ficheiro con este formato, ou ben escribindo algún script ou simplemente con algún programa de folla de cálculo gardando o ficheiro resultante en formato *CSV* (ficheiro de texto separado por comas) establecendo como separado de campo o carácter **:** en lugar da **,**.

Podemos ver a continuación un exemplo se carga do ficheiro *usuarios.txt* con este contido, e o resultado da súa execución:

- 

Páxina para a carga dun ficheiro para a creación masiva de usuarios

- 

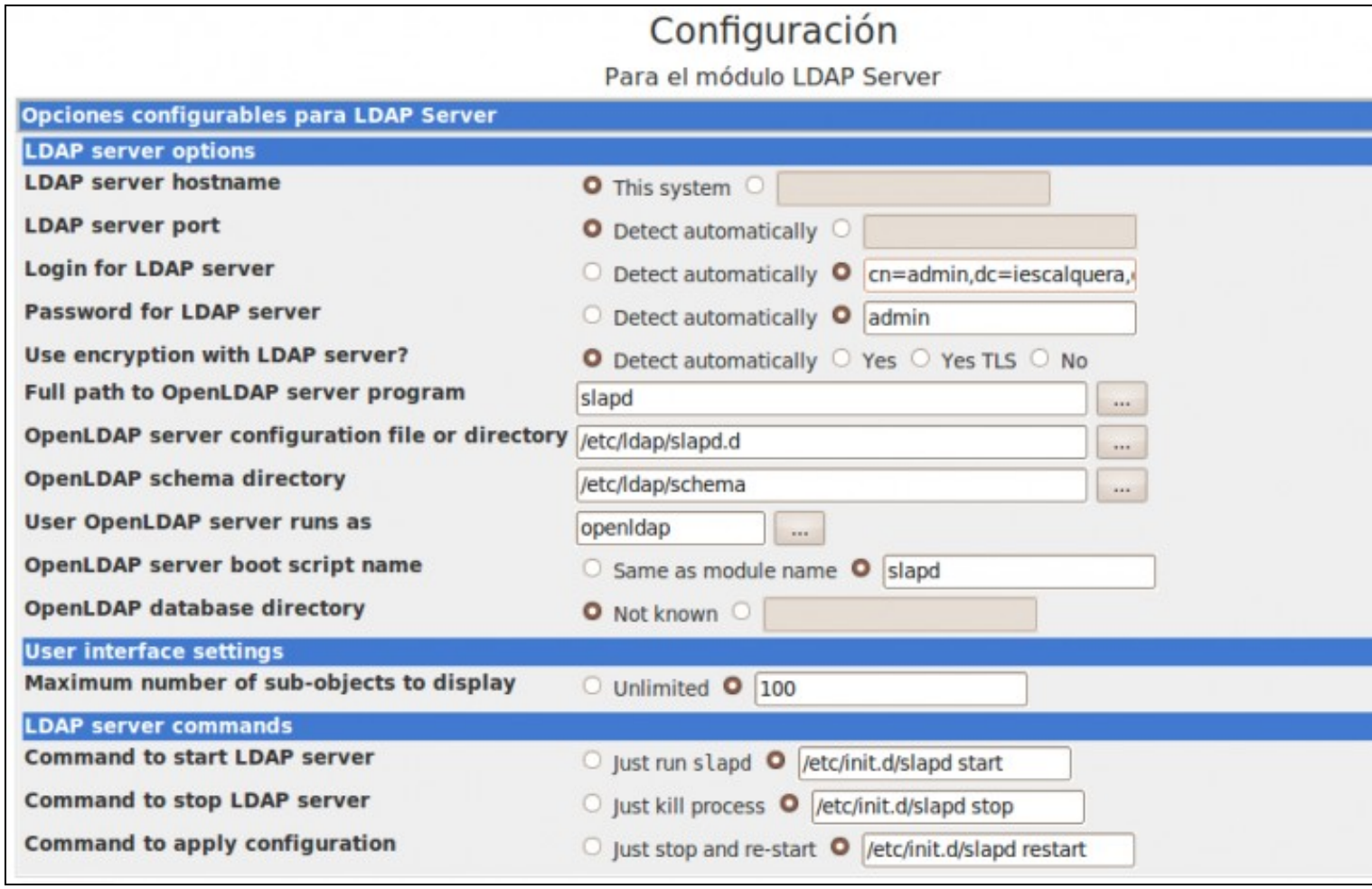
Resultado do proceso de creación dos usuarios. Observar como en /**home** están as carpetas persoais dos usuarios creados. Estas usaranse na parte III do curso.

- 

Lista de usuarios do LDAP despois de cargado o ficheiro

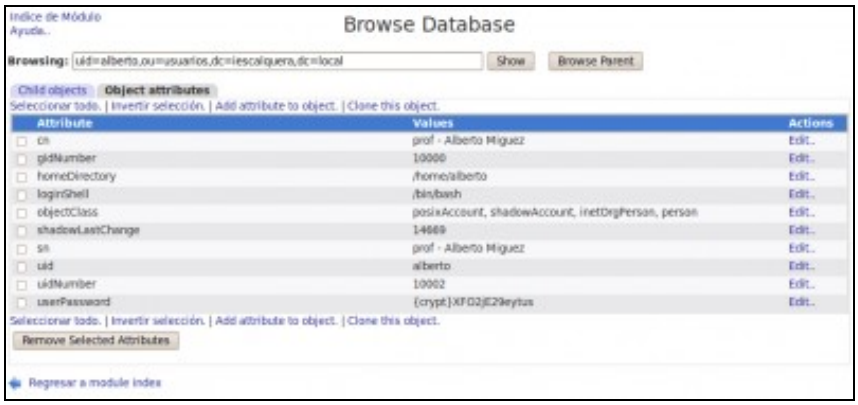
O módulo de servidor LDAP

O webmin tamén inclúe o módulo **LDAP Server** (dentro da categoría de **Servidores**), que aínda que non o usaremos para configurar o servidor LDAP no noso caso, si pode ser útil para poder navegar polos datos almacenados nel. Antes de usalo, teremos que entrar na configuración do módulo para introducir o usuario e contrasinal que usará para conectarse ao servidor LDAP, que poderá ser un usuario normal se só queremos visualizar os datos almacenados ou o administrador se queremos tamén poder realizar modificacións dos datos de calquera usuario ou grupo:



Unha vez gardados estes datos, picamos na opción **Browse Database**, introducimos a rama do LDAP que queremos explorar e picamos no botón de **Show**. A continuación pódense ver algunhas páxinas de exploración do LDAP:

- 

Vista do contido da rama base do LDAP
- 

Vista das propiedades do usuario *alberto*

LDAP Account Manager

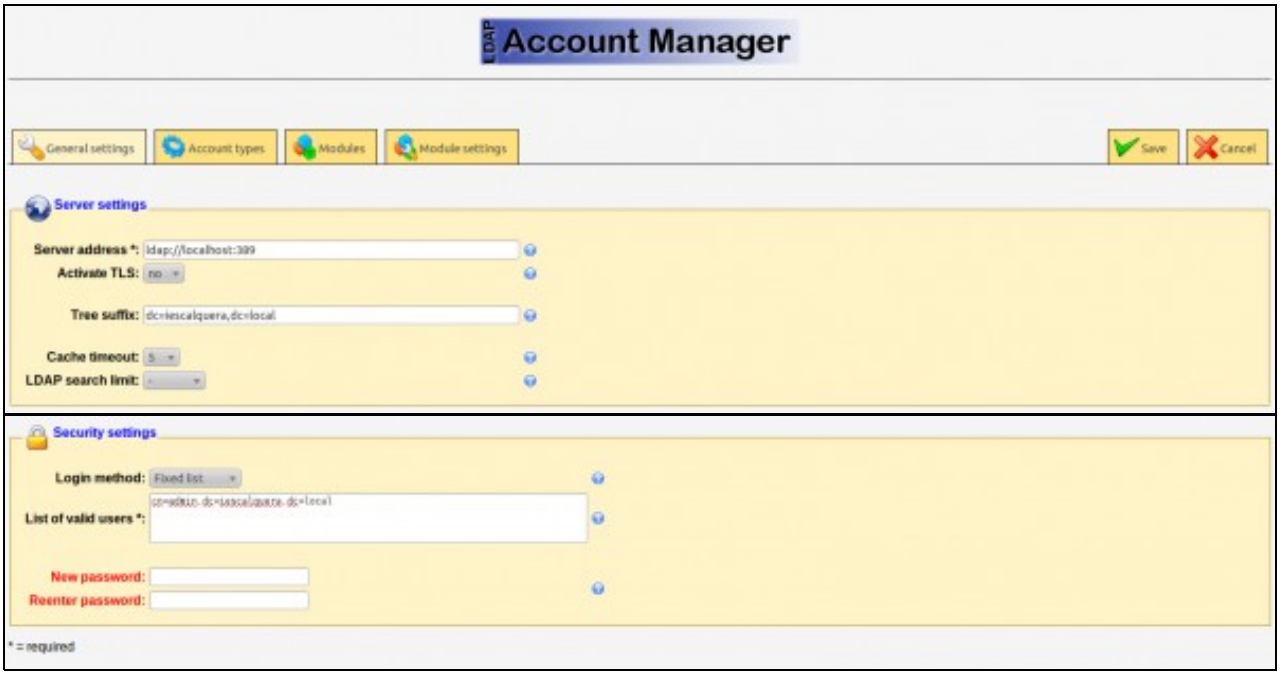
Aínda que non a utilizaremos no curso, outra ferramenta que podemos utilizar para administrar os usuarios e grupos do servidor LDAP é LDAP Account Manager. En Ubuntu Server, instálase co paquete **ldap-account-manager**, así que introduciríamos o comando:

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

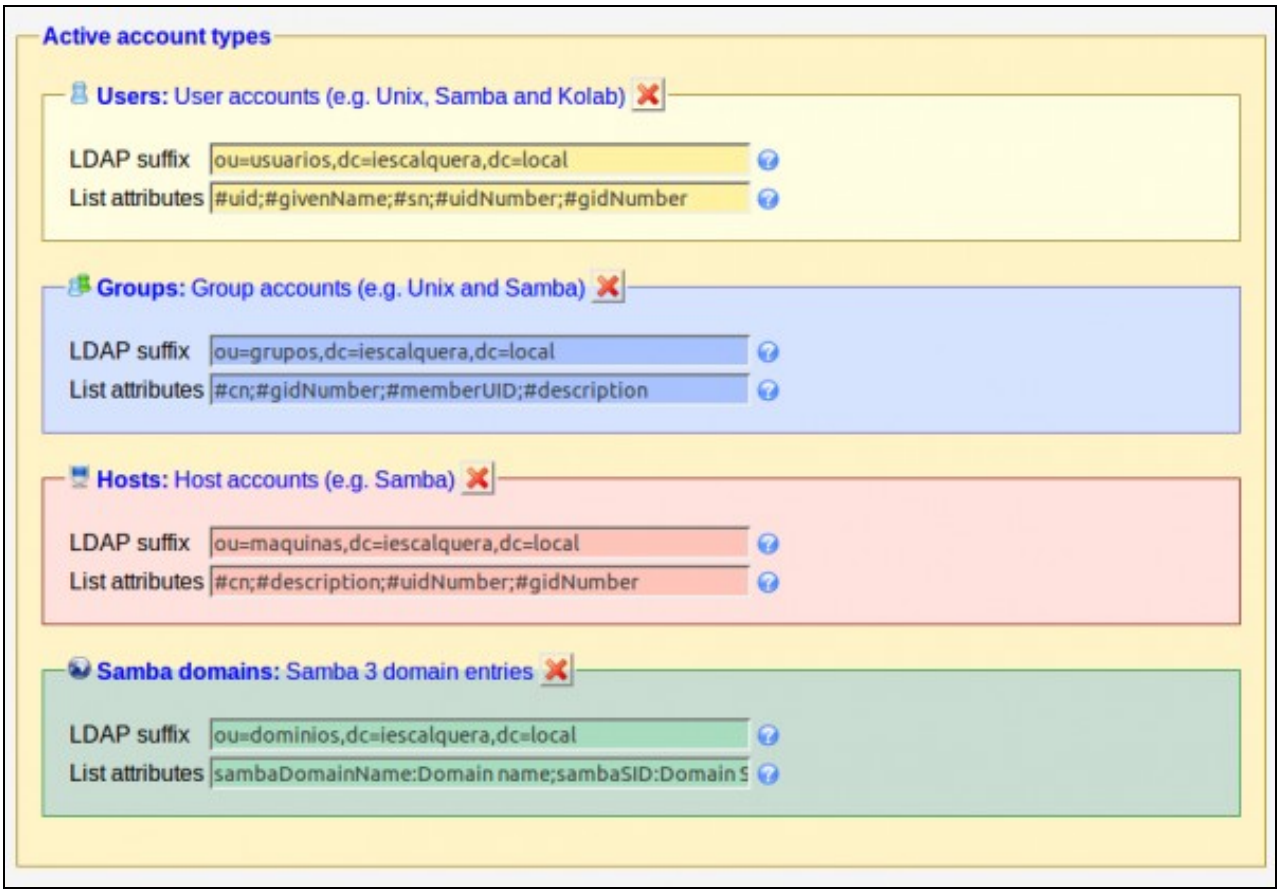
Con isto xa nos podemos conectar con un navegador dende un cliente introducindo a dirección *http://direcciónIPServidor/lam* (Nun servidor real, sería moi recomendable configurar o servidor apache para recibir conexións seguras e usar **https** en lugar de **http**):

Picamos no enlace de **LAM configuration** e logo en **Edit server profiles** para configurar os parámetros de conexión ao noso servidor LDAP. Introduciremos o contrasinal por defecto (*lam*) e entramos na páxina de configuración na que modificaremos os parámetros:

- Na pestana **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.



- Na pestana **Account Types**, dentro do apartado **Active account types**:
    - **Users -> LDAP suffix**: ou=usuarios,dc=iescalquera,dc=local
    - **Groups -> LDAP suffix**: ou=grupos,dc=iescalquera,dc=local
    - **Hosts -> LDAP suffix**: ou=maquinas,dc=iescalquera,dc=local
    - **Samba domains -> LDAP suffix**: ou=dominios,dc=iescalquera,dc=local



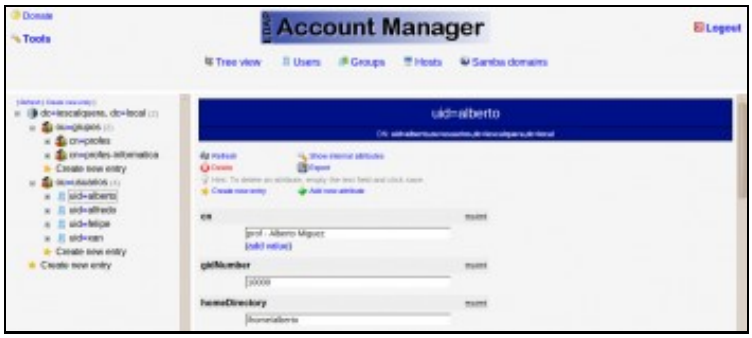
Picamos no botón **Save** para gardar os cambios. Todos estes parámetros introducidos almacénanse no ficheiro de configuración de lam (*/usr/share/ldap-account-manager/config/lam.conf*).

Agora xa podemos entrar na ferramenta introducindo o contrasinal do administrador do LDAP (*admin*):

- 

Inicio de sesión.
- 

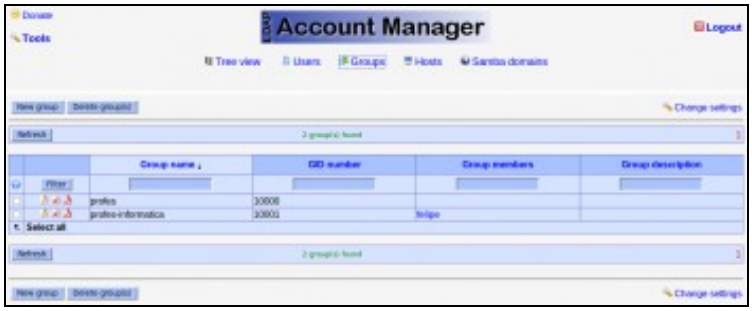
Pregúntanos se queremos crear as ramas para almacenar as máquinas e os dominios no directorio, xa que detecta que non existen aínda.

- 

Vista da árbore do LDAP

- 

Vista dos usuarios

- 

Vista dos grupos

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

-- Antonio de Andrés Lema e Carlos Carrión Álvarez