

Administración dos usuarios e grupos do LDAP

Sumario

- 1 **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 Ubuntudo curso [Curso Platega 08-09: Sistema operativo GNU-LINUX: UBUNTU 8.10.](#)
- 2 Administración mediante scripts
- 3 Administración con webmin
 - ◆ 3.1 Configuración inicial do módulo de Usuarios e grupos LDAP
 - ◆ 3.2 Administración de usuarios e grupos do LDAP con webmin
 - ◆ 3.3 Creación masiva de usuarios
 - ◆ 3.4 O módulo de servidor LDAP
- 4 LDAP Account Manager



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
```

NOTAS:

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

```

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

```

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 extensión `.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

## Configuración inicial do módulo de Usuarios e grupos LDAP

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <ul style="list-style-type: none"> <li>● Login: root</li> <li>■ Sistema</li> <li>■ Autenticación PAM</li> <li>Cambio de Contraseñas</li> <li>Contraseñas Plurales</li> <li>Copia de Seguridad de Sistema de Archivos</li> <li>LDAP Client</li> <li>MIME Type Programs</li> <li>Paquetes de Software</li> <li>Procesos en Curso</li> <li>Páginas del Manual</li> <li>Resolución de Problemas</li> <li>Log(s)</li> <li>Sistemas de Archivo de Disco y Red</li> <li>Software Package</li> <li>Virtuales</li> <li>Tareas Programadas (Cron)</li> <li>Usuarios y Grupos</li> <li>Usuarios y Grupos LDAP</li> </ul> | <p>Ayuda...<br/>Configuración de módulos</p> <p>El módulo de Perl Convert(UNIX)AGREGU(Bien)(UNIX)LDAP que es necesario para este módulo no está instalado o bien no funciona bien. Pulse aquí para descargarlo e instalarlo.</p> <p>El error que muestra Perl al intentar cargar el módulo es:</p> <pre>(perl) % perl -MLDAP -e "use LDAP; require '/usr/lib/perl5/vendor_perl/convert_unix2ldap.so'; use LDAP;"</pre> <p>Module failed: compilation aborted at /usr/lib/perl5/...</p> | <h2>Usuarios y Grupos LDAP</h2> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|

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 asignaríanse 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 *Idapscripts*, 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 poderíamos 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**:

# Configuración

Para el módulo Usuarios y Grupos LDAP

## Opciones configurables para Usuarios y Grupos LDAP

### Opciones de servidor LDAP

Máquina servidor LDAP

☒ Del archivo de configuración NSS ☐

Puerto del servidor LDAP

☒ Del archivo de configuración NSS o por defecto ☐

¿LDAP usa TLS?

☐ Sí ☐ No ☒ No

Enlazar al servidor LDAP como

☒ Nombre de enlace del archivo de configuración NSS ☐

Credenciales para el nombre de enlazado superior

☒ No cambiar ☐ Configurar a

Base para usuarios

☐ De archivo configuración NSS ☒ ou=usuarios,dc=ies

Base para grupos

☐ Del archivo de configuración NSS ☒ ou=grupos,dc=ies

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

### Opciones de usuario nuevo

UID menor para nuevos usuarios

☐ Del módulo de Usuarios y Grupos ☒ 10000

GID menor para nuevos grupos

☐ Del módulo de Usuarios y Grupos ☒ 10000

Método de encriptación de contraseñas

☐ LDAP MD5 ☐ Unix MD5 ☒ crypt ☐ Texto plano ☐

Construir lista de shells desde

☐ Lista original ☒ Usuarios de sistema ☒ /etc/shells

Conf. por defecto de nuevo usuario

- 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:

• Índice de Módulo

### Crear Usuario

|                               |                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Detalles de Usuario</b>    |                                                                                                                                                                                                                                                                                                                                   |
| Nombre de Usuario             | <input type="text" value="felipe"/>                                                                                                                                                                                                                                                                                               |
| ID de Usuario                 | <input type="text" value="10001"/>                                                                                                                                                                                                                                                                                                |
| Nombre Real                   | <input type="text" value="prof - Felipe Carballo"/>                                                                                                                                                                                                                                                                               |
| Directorio inicial            | <input checked="" type="radio"/> Automático <input type="radio"/> <input type="text"/>                                                                                                                                                                                                                                            |
| Shell                         | <input type="text" value="/bin/bash"/>                                                                                                                                                                                                                                                                                            |
| Contraseña                    | <input type="radio"/> No se pide contraseña<br><input type="radio"/> No está permitido el login<br><input checked="" type="radio"/> Contraseña normal <input type="text" value="abc123"/><br><input type="radio"/> Clave de acceso pre-encriptada <input type="text"/><br><input type="radio"/> Login temporalmente deshabilitado |
| <b>Opciones de Contraseña</b> |                                                                                                                                                                                                                                                                                                                                   |
| Contraseña cambiada           | Nunca                                                                                                                                                                                                                                                                                                                             |
| Días mínimos                  | <input type="text"/>                                                                                                                                                                                                                                                                                                              |
| Días de Aviso                 | <input type="text"/>                                                                                                                                                                                                                                                                                                              |
| Fecha de Expiración           | <input type="text" value="Ene"/> <input type="text"/>                                                                                                                                                                                                                                                                             |
| Días máximos                  | <input type="text"/>                                                                                                                                                                                                                                                                                                              |
| Días inactivos                | <input type="text"/>                                                                                                                                                                                                                                                                                                              |
| <b>Afiliación del Grupo</b>   |                                                                                                                                                                                                                                                                                                                                   |
| Grupo primario                | <input type="text" value="profes"/>                                                                                                                                                                                                                                                                                               |
| Grupos secundarios            | <input type="text" value="All groups"/><br><input type="text" value="profes"/>                                                                                                                                                                                                                                                    |

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

• Índice de Módulo

### Crear Grupo

**Detalles de Grupo**

Nombre de Grupo:

ID de Grupo:

Contrasena:

☒ No se pide contraseña

☐ Clave de acceso pre-encryptada

☐ Contraseña normal

**Miembros**

All users:

Users in group:

**Capacidades de grupo**

¿Grupo Samba? ☐ Si ☒ No

**Al Crear...**

¿Crear grupo en otros módulos? ☒ Si ☐ No

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 folia 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:

• Índice de Módulo

### Ejecutar Archivo por Lotes

[Instructions and batch format](#)

Este formulario le permite crear, modificar o borrar varios usuarios de una vez desde un archivo de texto cargado o local. Cada línea del archivo especifica una acción a realizar, dependiendo de su primer campo. Los formatos de línea son:

```
crear:username:passwd:uid:gid:realname:homedir:shell:min:max:warn:inactive:expire
modificar:oldusername:username:passwd:uid:gid:realname:homedir:shell:min:max:warn:inactive:expire
borrar:username
```

En las líneas **create (crear)**, si el campo de uid se deja vacío, Webmin asignará automáticamente una UID. Si el campo de gid se deja vacío, Webmin creará un nuevo grupo con el mismo nombre que el usuario. Los campos username (nombre de usuario), homedir (directorio inicial) y shell deben de ser suministrados para cada usuario - todos los otros campos se permite que estén vacíos. Si el campo de passwd (contraseña) se deja en blanco, no se asigna contraseña al usuario. Si contiene sólo la letra x, la cuenta se bloqueará. En caso contrario, el texto en el campo es tomado como contraseña en texto plano, y posteriormente encriptada.

En las líneas **modify (modificar)**, un campo vacío indica que el correspondiente atributo de usuario no ha de ser modificado.

**Batch user creation, update and deletion options**

Fuente de datos de lotes

☒ Archivo cargado

☐ Archivo en servidor

☐ Texto en la caja inferior

¿Crear, modificar o borrar usuarios en otros módulos? ☒ Si ☐ No

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

- Indice de Módulo

## Ejecutar Archivo por Lotes

Creado usuario alberto  
Creado usuario xan

[Regresar a formulario de lotes](#) | [Regresar a lista 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.

- Ayuda - Configuración de Módulo

## Usuarios y Grupos LDAP

LDAP Users | LDAP Groups

Seleccionar todo | Invertir selección | Añadir un nuevo usuario LDAP

Crear, modificar y borrar usuarios desde archivo por lotes

| Nombre de Usuario                | ID de Usuario | Grupo | Nombre Real            | Directorio Inicial | Shell     |
|----------------------------------|---------------|-------|------------------------|--------------------|-----------|
| <input type="checkbox"/> alfredo | 10000         | 10000 | Alfredo Perez          | /home/alfredo      | /bin/bash |
| <input type="checkbox"/> felipe  | 10001         | 10000 | prof - Felipe Carballo | /home/felipe       | /bin/bash |
| <input type="checkbox"/> alberto | 10002         | 10000 | prof - Alberto Miguez  | /home/alberto      | /bin/bash |
| <input type="checkbox"/> xan     | 10003         | 10000 | prof - Xan Pereira     | /home/xan          | /bin/bash |

Seleccionar todo | Invertir selección | Añadir un nuevo usuario LDAP

[Borrar Usuarios Seleccionados](#) [Deshabilitar Seleccionados](#) [Habilitar Seleccionados](#)

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:

## Configuración

### Para el módulo LDAP Server

#### Opciones configurables para LDAP Server

##### LDAP server options

**LDAP server hostname** ☒ This system ☐

**LDAP server port** ☒ Detect automatically ☐

**Login for LDAP server** ☐ Detect automatically ☒

**Password for LDAP server** ☐ Detect automatically ☒

**Use encryption with LDAP server?** ☒ Detect automatically ☐ Yes ☐ Yes TLS ☐ No

**Full path to OpenLDAP server program**

**OpenLDAP server configuration file or directory**

**OpenLDAP schema directory**

**User OpenLDAP server runs as**

**OpenLDAP server boot script name** ☐ Same as module name ☒

**OpenLDAP database directory** ☒ Not known ☐

##### User interface settings

**Maximum number of sub-objects to display** ☐ Unlimited ☒

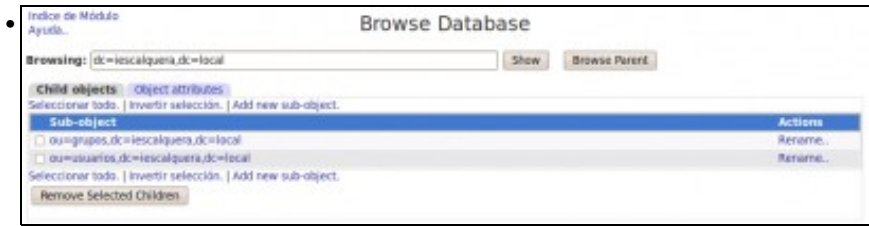
##### LDAP server commands

**Command to start LDAP server** ☐ Just run slapd ☒

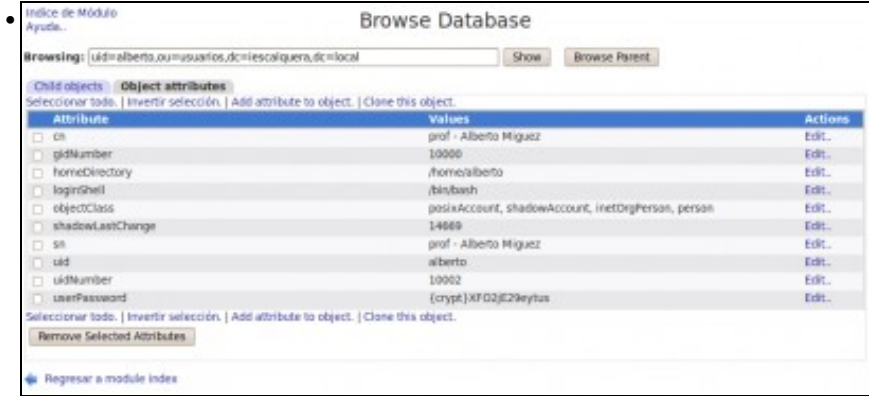
**Command to stop LDAP server** ☐ Just kill process ☒

**Command to apply configuration** ☐ Just stop and re-start ☒

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.

The screenshot shows the 'LDAP Account Manager' web interface. At the top, there's a navigation bar with tabs: 'General settings' (selected), 'Account types', 'Modules', and 'Module settings'. To the right of these tabs are 'Save' and 'Cancel' buttons. Below the tabs, the 'Server settings' section is visible. It contains the following fields: 'Server address \*' with the value 'ldap://localhost:389', 'Activate TLS' set to 'no', 'Tree suffix' with the value 'dc=iescalquera,dc=local', 'Cache timeout' set to '5', and 'LDAP search limit' set to '1'. Below this, the 'Security settings' section is visible. It contains: 'Login method' set to 'Fixed list', 'List of valid users \*' with the value 'cn=admin,dc=iescalquera,dc=local', and two empty password fields labeled 'New password' and 'Reenter password'. A footnote at the bottom left states '\* = required'.

- 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

**Active account types**

**Users:** User accounts (e.g. Unix, Samba and Kolab)

LDAP suffix

List attributes

**Groups:** Group accounts (e.g. Unix and Samba)

LDAP suffix

List attributes

**Hosts:** Host accounts (e.g. Samba)

LDAP suffix

List attributes

**Samba domains:** Samba 3 domain entries

LDAP suffix

List attributes

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`).

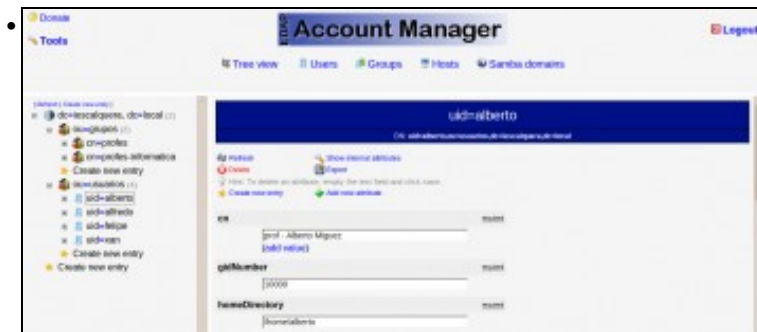
Agora xa podemos entrar na ferramenta introducindo o contrasinal do administrador do LDAP (*admin*):

- 

Inicio de sesión.

- 

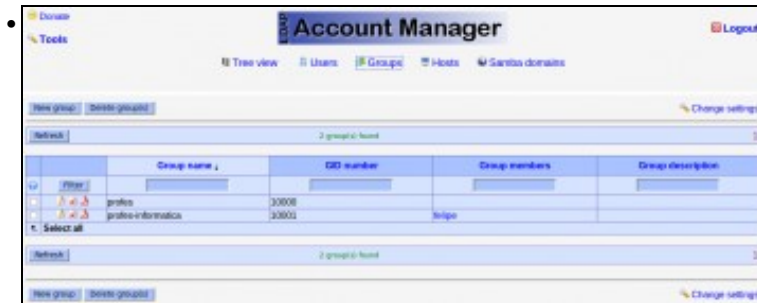
Pregúntanos se queremos crear as ramas para almacenar as máquinas e os dominios no directorio, xa que detecta que non existen aínda.



Vista da árvore 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