

GESTIÓN DE USUARIOS, LDAP Y NFS

1. INTRODUCCIÓN

Existen diferentes formas de autenticar clientes en una red *GNU/Linux*, pero una de las más usadas es la combinación de tres herramientas diferentes: *PAM*, *NSS* y *LDAP*.

La idea consiste en disponer de un servidor que facilite la autenticación de los clientes, de modo que éstos recurran al servidor cada vez que un usuario necesite identificarse. De esta forma, la cuenta de usuario no es específica de un equipo cliente, sino que será válida en cualquier equipo de la red que haya sido debidamente configurado.

NSS (Name Service Switch):

Provee una interfaz para la consulta de información del usuario: nombre de usuario, grupo, contraseña, UID, GID, directorio personal, etc. Esta consulta puede ser realizada a bases de datos de usuarios, como pueden ser */etc/passwd*, */etc/shadow* o */etc/groups*, que son ficheros que almacenan las credenciales y nombres de usuario y grupos del sistema o también puede coger la información a partir de otras fuentes como DNS (Domain Name System), NIS(Network Information Service) o LDAP(Lightweight Directory Access Protocol).

Su principal objetivo es que los programas puedan manejar información administrativa de los usuarios de forma transparente, es decir, el programa no tendrá que tener en cuenta contra que base de datos o fichero debemos autenticar al usuario, será el NSS el que se encargue de buscar dichos datos.

En definitiva, NSS guarda la información contra que base de datos se ha de autenticar un usuario.

PAM (Pluggable Authentication Modules):

Genera una interfaz de autenticación entre el programa y el usuario, de forma que el método de autenticación es transparente al programa.

Mientras que NSS se centra en la búsqueda de los usuarios, PAM se encarga de recoger el nombre de usuario y contraseña para autenticarlos en la base de datos que nos señale el NSS.

LDAP (Lightweight Directory Access Protocol):

Un servidor LDAP es un servidor de datos optimizado para la realización rápida de consultas de **lectura** y orientado al **almacenamiento de datos de usuarios**.

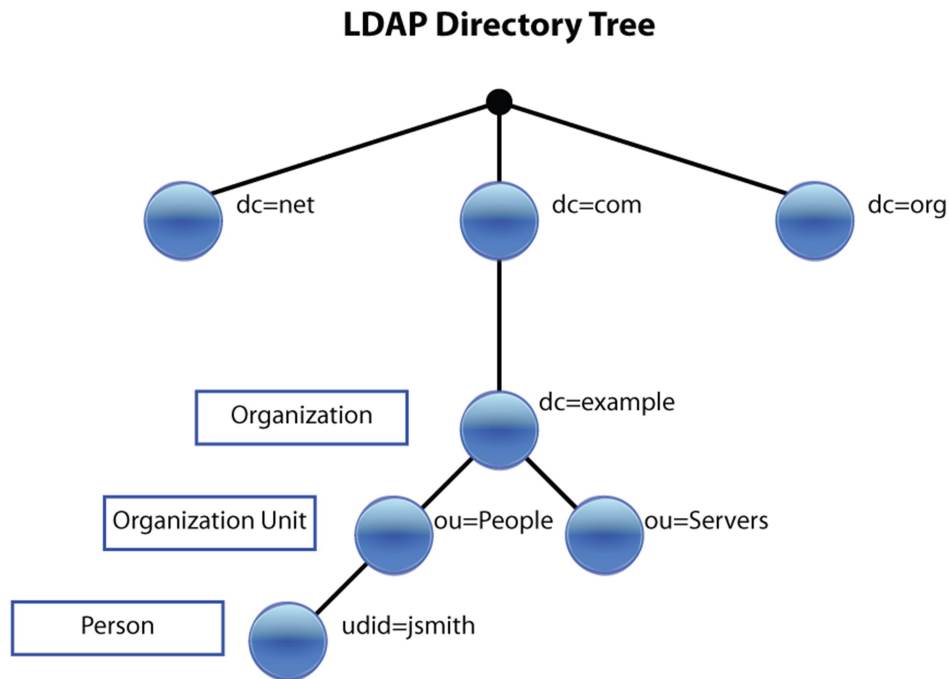
LDAP organiza la información (usuario, contraseña, directorio HOME, nombre y apellidos de la persona, e-mail) en forma de **árbol jerárquico** para asegurar la unicidad, de forma parecida a como trabajan los servicios DNS.

Un servidor LDAP no es más que un gestor de **bases de datos jerárquico** al contrario que MySQL que es un gestor de bases de datos relacional. La realización de consultas o lectura de la base de datos es más rápida que en una BD relacional, en cambio la escritura es más lenta.

La principal utilidad de un directorio LDAP es como servidor de autenticación para los distintos servicios de un sistema informático como puedan ser: autenticación para entrar en un PC, para entrar en una aplicación web, para acceder a un servidor ftp, etc.

Para el desarrollo de ese protocolo usaremos OpenLDAP, el cual es software libre y de código abierto. Podemos encontrar OpenLDAP no solo en distribuciones GNU/Linux, sino también en Windows, Apple o Solaris.

Ejemplo de estructura en árbol:



2. INSTALACIÓN OPENLDAP.

1. Instalar OpenLDAP.

El servidor OpenLDAP está disponible en el paquete **slapd**. También nos conviene instalar el paquete **ldap-utils** que contiene utilidades adicionales:

- `sudo apt-get install slapd ldap-utils`

2. Configurar OpenLDAP.

La configuración de OpenLDAP se almacena en `/etc/ldap/`.

No obstante, podemos lanzar el asistente de configuración:

- `sudo dpkg-reconfigure slapd`

- Crearemos un dominio: "ldapserver.es"
- Esto va a generar dos "dc": dc=ldapserver,dc=es
 - La organización será "SMR"
 - Seleccionar el motor "MDB"
 - No permitir el protocolo LDAP v2

3. Reiniciar servicio y ver estado.

- service slapd {status | restart | start | stop | force-reload}

4. Comprobar arranque automático del servicio.

Cuando Ubuntu arranca tiene 7 modos distintos (del 0 al 6):

- **Nivel 0 (Halt):** Detener o apagar el sistema
- **Nivel 1 (Monousuario):** Modo monousuario, generalmente utilizado para mantenimiento del sistema.
- **Nivel 2 (Multiusuario sin red):** Modo multiusuario pero sin soporte de red.
- **Nivel 3 (Multiusuario completo):** Modo multiusuario con servicios de red.
- **Nivel 4 (No utilizado):** Puede utilizarse para un inicio personalizado
- **Nivel 5 (Multiusuario con inicio gráfico):** Modo multiusuario completo con inicio gráfico.
- **Nivel 6 (Reboot):** Modo de reinicio.

Con el comando "runlevel" nos indica el nivel en el que ha arrancado.

Podemos hacer uso de la herramienta **sysv-rc-conf** para ver y elegir qué servicios arrancan según qué tipo de nivel de arranque.

- Instalar sysv-rc-conf
sudo apt-get install sysv-rc-conf
- Arrancar sysv-rc-conf
sudo sysv-rc-conf

```

salvu@MiniSally: ~
SysV Runlevel Config -: stop service =/+ : start service h: help q: quit

service  1    2    3    4    5    0    6    S
-----
rsyslog  [ ]  [X]  [X]  [X]  [X]  [ ]  [ ]  [ ]
saned    [ ]  [X]  [X]  [X]  [X]  [ ]  [ ]  [ ]
sendmail [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]
single   [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]
slapd    [X]  [X]  [X]  [X]  [X]  [ ]  [ ]  [ ]
speech-dispatcher [ ]  [X]  [X]  [X]  [X]  [ ]  [ ]  [ ]
thermald [ ]  [X]  [X]  [X]  [X]  [ ]  [ ]  [ ]
udev     [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [X]
ufw      [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [X]
umountfs [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]
umountroot [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]
unattended [ ]  [X]  [X]  [X]  [X]  [ ]  [ ]  [ ]
urandom  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [ ]  [X]

Use the arrow keys or mouse to move around.      ^n: next pg      ^p: prev pg
space: toggle service on / off
  
```

5. Comprobar que se ha creado correctamente el servicio LDAP.

Podemos comprobar los parámetros de nuestro servicio ldap ejecutando “slapcat” (necesitaremos credenciales de administrador).

```
alumno@soruserver:~$ sudo slapcat
[sudo] password for alumno:
dn: dc=ldapserver,dc=es
objectClass: top
objectClass: dcObject
objectClass: organization
o: SMR
dc: ldapserver
structuralObjectClass: organization
entryUUID: 4f985f56-904e-1038-8821-75eeaaf5f4dc
creatorsName: cn=admin,dc=ldapserver,dc=es
createTimestamp: 20181209223418Z
entryCSN: 20181209223418.803093Z#000000#000#000000
modifiersName: cn=admin,dc=ldapserver,dc=es
modifyTimestamp: 20181209223418Z

dn: cn=admin,dc=ldapserver,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9LzZlZmVhZSdGoyTzg1a08wcnBIQmlGbEJl
2MHA=
structuralObjectClass: organizationalRole
entryUUID: 4f99f226-904e-1038-8822-75eeaaf5f4dc
```

3. INSTALACIÓN Y USO DE EXPLORADOR DE DIRECTORIOS JXPLORER

Aunque LDAP permite trabajar con comandos y archivos LDIF, para acceder al directorio LDAP y poder crear y modificar elementos en dicho directorio, es más práctico utilizar un explorador de directorios LDAP (LDAP browser). Existen muchos exploradores LDAP tanto de pago como libres. Entre las aplicaciones libres destacamos gq, phpldapadmin (aplicación web) y JXplorer.

3.1. INSTALACIÓN DE JXPLORER

Para realizar la instalación de JXplorer realizaremos los siguientes pasos:

a. Activar repositorios “partner”:

- Son repositorios que incluyen software externo a Ubuntu y que se encuentra desactivado por defecto.
- Para activarlo deberemos editar el siguiente fichero y descomentar las acciones

```
sudo gedit /etc/apt/sources.list
```

Las líneas a descomentar son la 43 y 44:

```
deb http://archive.canonical.com/ubuntu xenial partner
```

```
deb-src http://archive.canonical.com/ubuntu xenial partner
```

b. Actualizar apt-get:

```
sudo apt-get update
```

c. Instalar JXplorer:

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

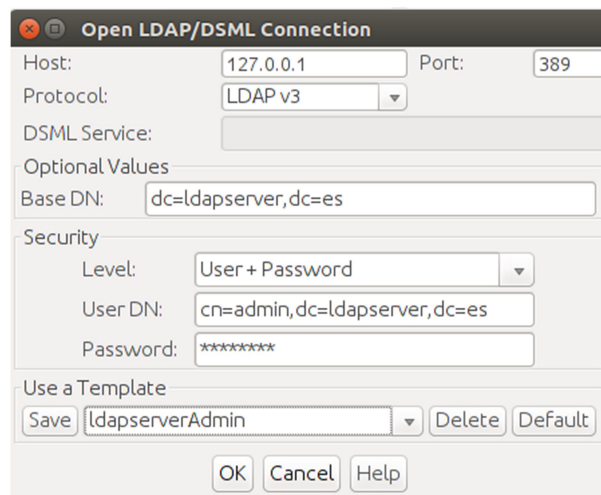
d. Ejecutar JXplorer.

```
jxplorer
```

3.2. CONEXIÓN AL SERVIDOR LDAP

La conexión con el servidor LDAP podemos hacerla como usuario anónimo o como usuario administrador. Si conectamos de forma **anónima** solo podremos visualizar los elementos pero no podremos hacer cambios. Si conectamos como **administrador**, podremos crear, modificar y eliminar elementos de cualquier tipo.

Como hemos visto anteriormente existe un usuario por defecto “admin” que incorpora la contraseña por defecto que hemos insertado durante la instalación del servidor LDAP. Por lo que podemos entrar con estas credenciales para poder modificar los valores del servidor.



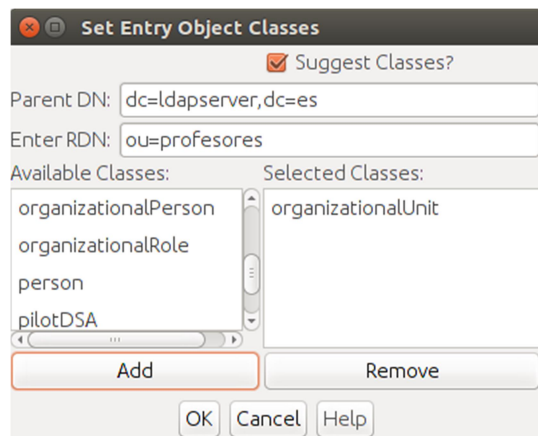
3.3. AÑADIR NUEVOS ELEMENTOS MEDIANTE JXPLORER

Para añadir nuevos elementos haremos clic derecho sobre el nodo padre al que pertenecerá el nuevo objeto y pulsaremos sobre “Nuevo”. Nos mostrará una ventana donde podremos incluir los datos del nuevo elemento a crear:

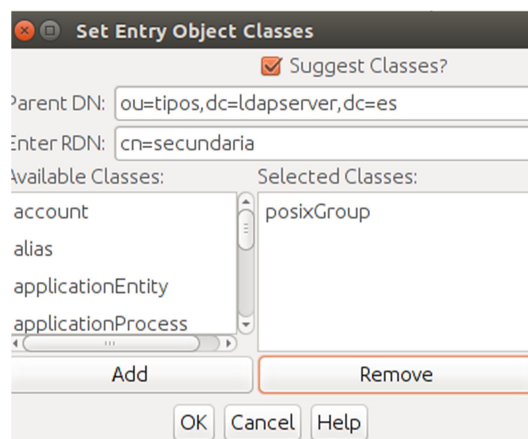
- Parent DN: hace referencia al Distinguished Name del nodo padre al que pertenecerá el objeto. Si hemos pulsado “Nuevo” habiendo hecho clic derecho sobre un nodo, ya nos aparecerá rellenado.
- RDN (Relative Distinguished Name): en este campo incluiremos el nombre del nuevo objeto.
- SelectedClasses: en función del tipo de objeto que vayamos a incluir indicaremos a qué clases pertenece.
-

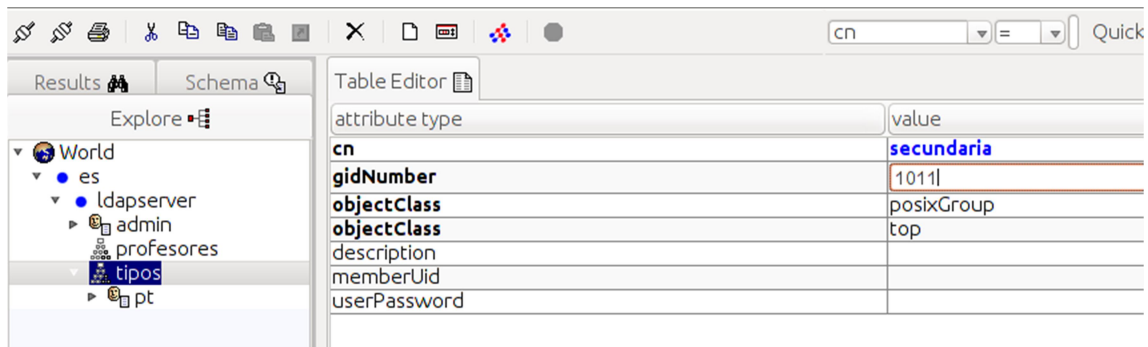
1. Crea una unidad organizativa.

El nombre del objeto se introducirá en el segmento de RDN (Relative Distinguished Name). Como en este caso es una unidad organizativa escribiremos ou=[nombre del objeto] y como clases del objeto seleccionaremos “organizationalUnit”.

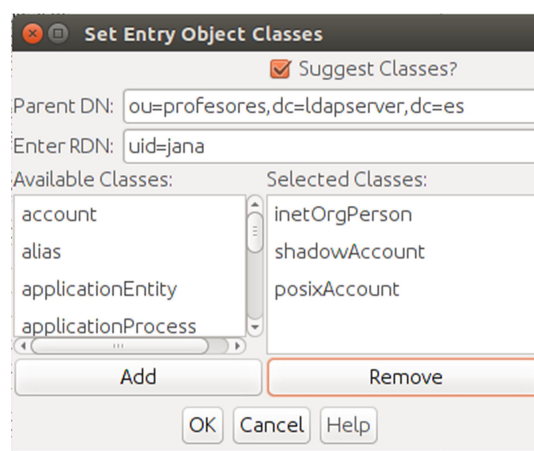


2. Crear grupos.





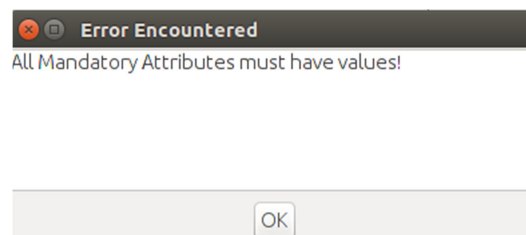
3. Insertar usuarios.



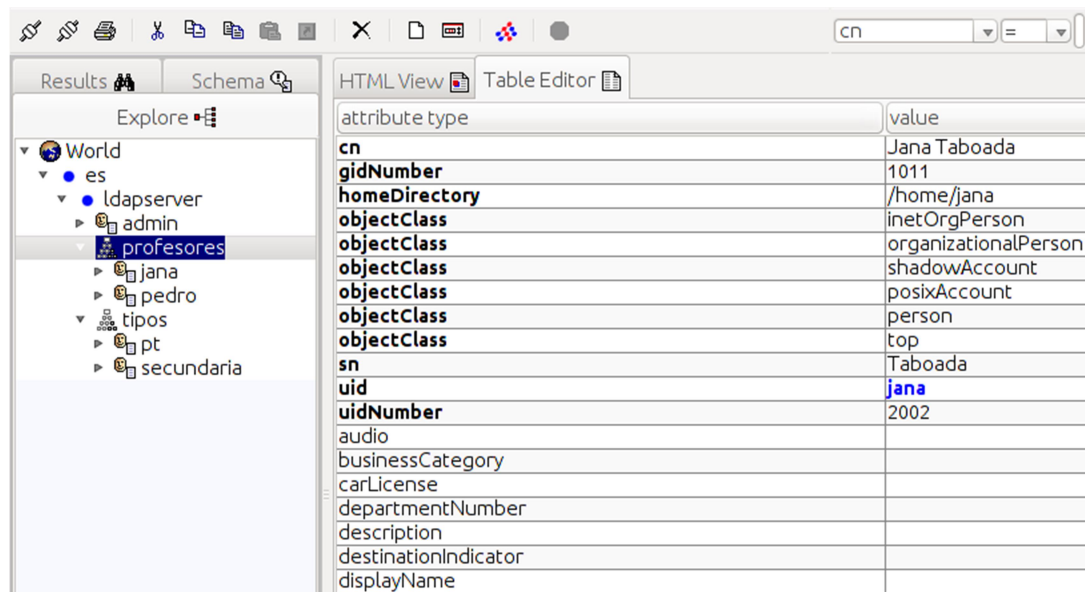
En el caso de los usuarios será obligatorio rellenar al menos los siguientes campos:

- uidNumber
- gidNumber
- homeDirectory
- uid
- cn
- sn

Como podéis comprobar dichos campos requeridos se encuentran en negrita en el propio JXplorer. En caso de intentar rellenar un usuario sin alguno de estos campos JXplorer nos mostrará un error como el siguiente:

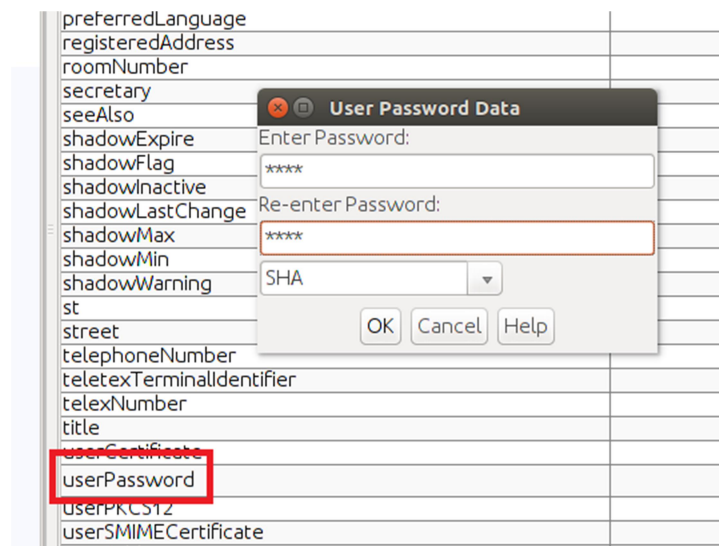


****Importante:** No hagáis uso de acentos ya que no son interpretados correctamente por la aplicación JXplorer.



attribute type	value
cn	Jana Taboada
gidNumber	1011
homeDirectory	/home/jana
objectClass	inetOrgPerson
objectClass	organizationalPerson
objectClass	shadowAccount
objectClass	posixAccount
objectClass	person
objectClass	top
sn	Taboada
uid	jana
uidNumber	2002
audio	
businessCategory	
carLicense	
departmentNumber	
description	
destinationIndicator	
displayName	

También podemos escribir la contraseña del usuario, con el tipo de encriptación que queramos utilizando el campo UserPassword:



preferredLanguage	
registeredAddress	
roomNumber	
secretary	
seeAlso	
shadowExpire	
shadowFlag	*****
shadowInactive	
shadowLastChange	
shadowMax	*****
shadowMin	
shadowWarning	SHA
st	
street	
telephoneNumber	
teletexTerminalIdentifier	
telexNumber	
title	
userCertificate	
userPassword	
UserPKCS12	
userSMIMECertificate	