# Configuración do cliente LDAP

## Sumario



## Introdución

- Neste apartado veremos os pasos que temos que seguir para configurar un equipo como cliente LDAP, de forma que o equipo tomará os usuarios e grupos do LDAP como usuarios e grupo do propio sistema, e autenticará os usuarios que inicien sesión validándose contra o servidor LDAP.

- Polo tanto, teremos que realizar esta configuración en todos os equipos que pertenzan ao noso dominio, **incluíndo (e moi especialmente) o servidor de dominio** (no que se executa o servidor LDAP), xa que senón os usuarios e grupos do LDAP non serán válidos para el mesmo, aínda que sexa el quen almacena a información do directorio.

## Instalar os paquetes necesarios

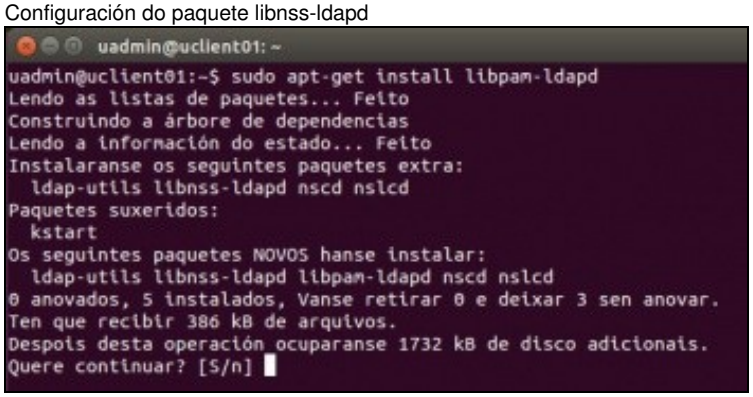
- En moitos manuais vese que se instala o seguinte paquete **libnss-ldap**. E funciona para autenticar os usuarios, pero cos contrasinais hoxe en día hai que configurar varias cousas para que os usuarios os poidan cambiar.

- O paquete máis moderno e sinxelo é **nslcd** (ollo coa "d" final). Para instalalo imos instalar outro paquete que necesitamos: **libpam-ldapd** e que depende de nslcd.

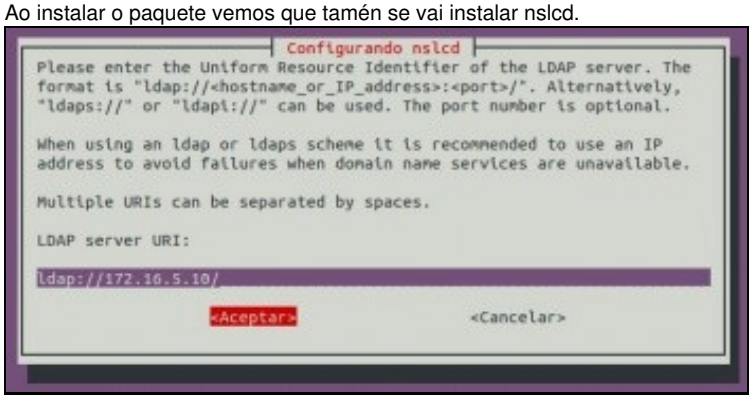
```
sudo apt-get install libpam-ldapd
```

- Este novo paquete fai toda a configuración dun modo moi sinxelo por nós, con moitos menos pasos que o paquete que se menciona ao principio.

A instalación deste paquete obrigará tamén a instalación do paquete **ldap-auth-config**, que permite configurar a autenticación do equipo contra un servidor LDAP. Lanzarase automaticamente un asistente para configurar a conexión co servidor LDAP:

- Configuración do paquete libnss-ldapd
- 

Ao instalar o paquete vemos que tamén se vai instalar nslcd.

- 

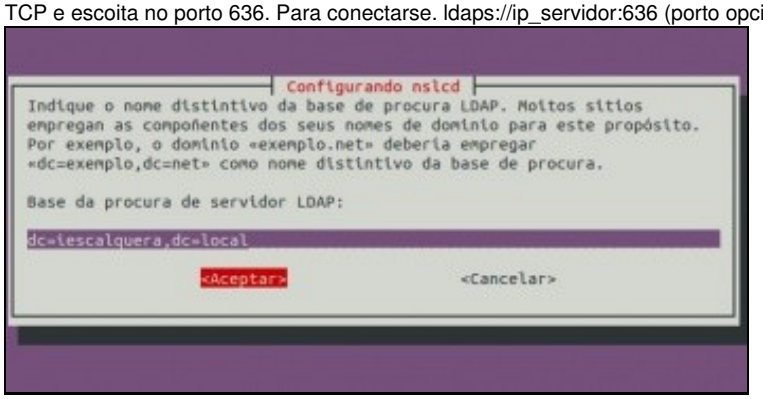

Introducimos a URL da conexión do servidor LDAP (ldap://IPServidor). Se funciona o servidor DNS podemos usar o seu FQDN (http://es.wikipedia.org/wiki/FQDN) ou o seu nome se temos configurado o dominio de busca.

Os protocolos polos que se pode conectar un cliente ao servidor son:

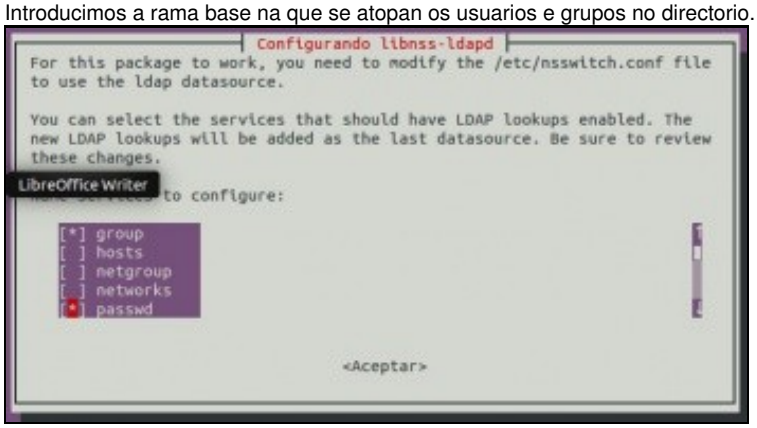
**-ldap**: que usa o protocolo TCP e escoita no porto 389, podemos conectarnos dende calquera sitio coa sintaxe: ldap://ip_do_servidor

**-ldapi**: que se usa para conectarse dende o cliente **dentro do mesmo servidor** ao demo slapd usando **Sockets de Unix** (http://es.wikipedia.org/wiki/Socket_Unix) e non a pila de protocolos TCP/IP. Para conectarse so precisamos poñer o nome do protocolo: ldapi:/// (Ollo coas tres barras).

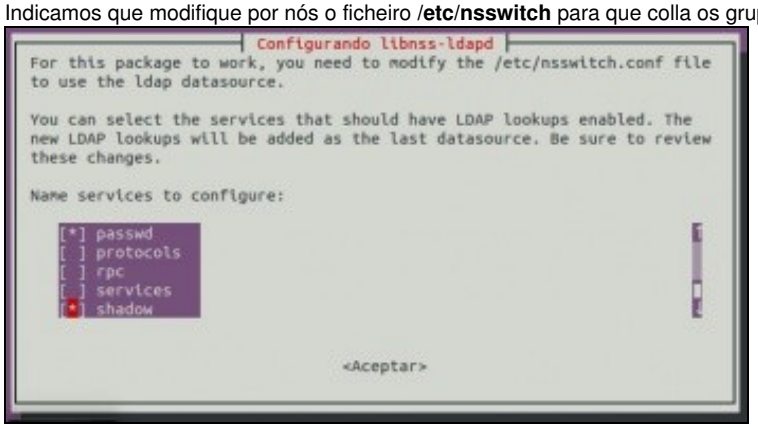
**- ldaps**: permite realizar conexións cifradas (seguras) entre os clientes e o servidor como veremos no escenario 1.F. Usa tamén o protocolo TCP e escoita no porto 636. Para conectarse. ldaps://ip_servidor:636 (porto opcional).

- 

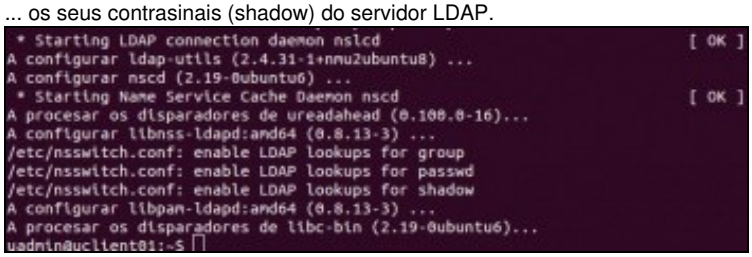

Introducimos a rama base na que se atopan os usuarios e grupos no directorio.

- 

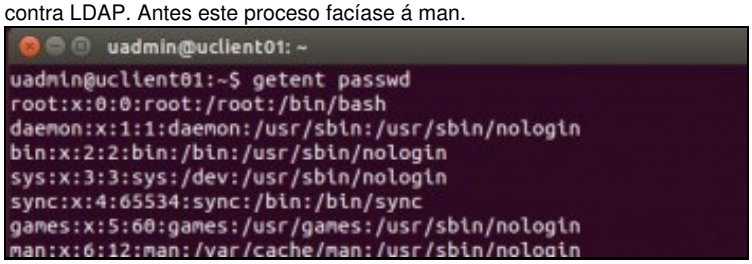

Indicamos que modifique por nós o ficheiro /**etc**/**nsswitch** para que colla os grupos (**group**), os usuarios (**passwd**) e ...

- 

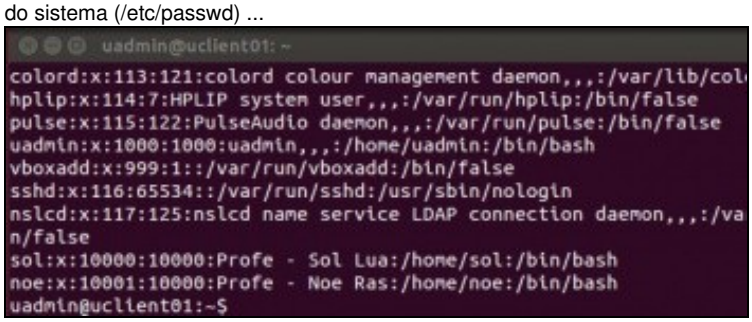
... os seus contrasinais (shadow) do servidor LDAP.

- 


Vemos que ao final do proceso de instalación, este xa configura nslcd, /etc/nsswitch.conf e os módulos PAM que se precisan para autenticar contra LDAP. Antes este proceso facíase á man.

- 

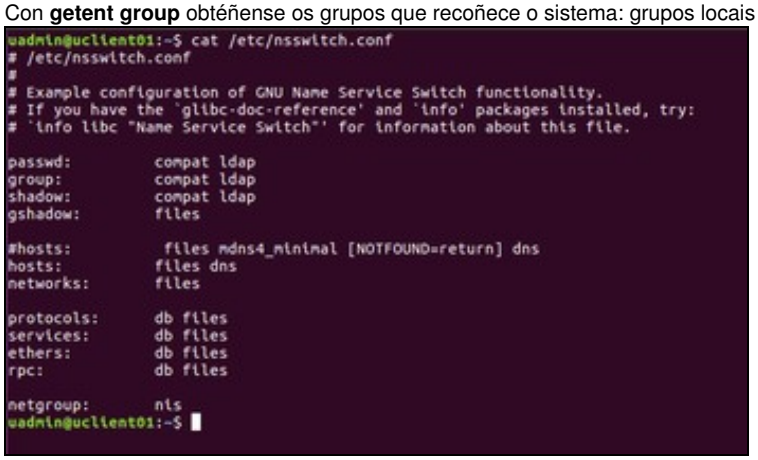

Co comando **getent passwd** obtemos a lista de tódolos usuarios que poden iniciar sesión no equipo local. Os primeiros usuario son os locais do sistema (/etc/passwd) ...

- 


... e ao final amosa os usuarios que obtén do LDAP.

- 

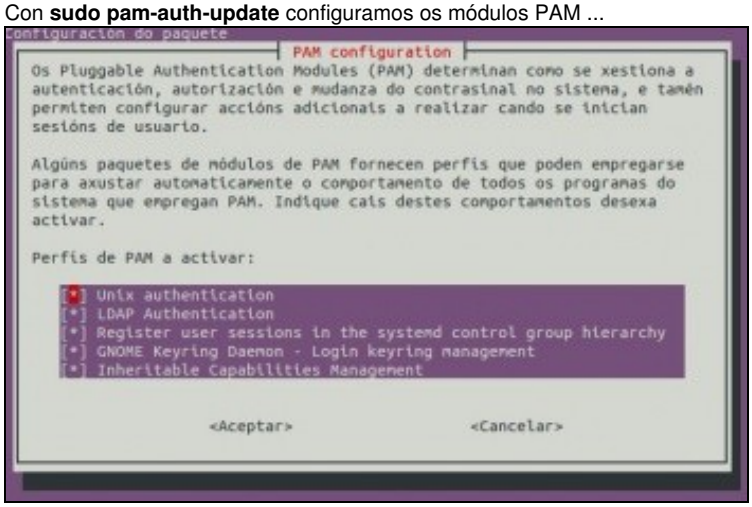

Con **getent group** obtéñense os grupos que recoñece o sistema: grupos locais + grupos do LDAP.

- 

Se observamos o ficheiro **/etc/nsswitch.conf** vemos que os usuarios, grupos e contrasinais son obtidos primeiro dos ficheiros locais (compact ou files) e logo de ldap.

- 


Con **sudo pam-auth-update** configuramos os módulos PAM ...

- 


..., pero xa están configurados polo programa de instalación. Podemos ver que a autenticación LDAP xa está marcada por defecto.

Se cometésemos algún erro introducindo os datos de conexión pódese reconfigurar o paquete "nslcd" co mesmo asistente introducindo o seguinte comando:

```
sudo dpkg-reconfigure nslcd
```

## Ficheiro de configuración /etc/nslcd.conf

- O proceso anterior configurou ademais de todo o anterior o ficheiro **/etc/nslcd.conf**.
- No ficheiro **/etc/nslcd.conf** pódese ver e modificar a configuración do cliente ldap.
- Observar as seguintes entradas:
    - uri
    - base

```
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.

# The user and group nslcd should run as.
uid nslcd
gid nslcd

# The location at which the LDAP server(s) should be reachable.
uri ldap://172.16.5.10/

# The search base that will be used for all queries.
base dc=iescalquera,dc=local

# The LDAP protocol version to use.
#ldap_version 3

# The DN to bind with for normal lookups.
#binddn cn=annonymous,dc=example,dc=net
#bindpw secret

# The DN used for password modifications by root.
```

```
#rootpwmoddn cn=admin,dc=example,dc=com

# SSL options
#ssl off
#tls_reqcert never

# The search scope.
#scope sub
```

## Probar o funcionamento do cliente

- Recoméndase reiniciar o ordenador cliente para asegurarase que se aplican os cambios.

- Temos dúas formas sinxelas de comprobar que a configuración do cliente é correcta e toma realmente os usuarios do servidor:
- A primeira xa a vimos con **getent passwd**:
    - Como se indicou, este comando mostra pola pantalla todos os usuarios do sistema, tomándoos das diversas fontes que pode ter configuradas. No noso caso, deberían aparecer ao final os usuarios LDAP. A continuación pódese ver a última parte do resultado deste comando, no que aparecen os usuarios do LDAP:

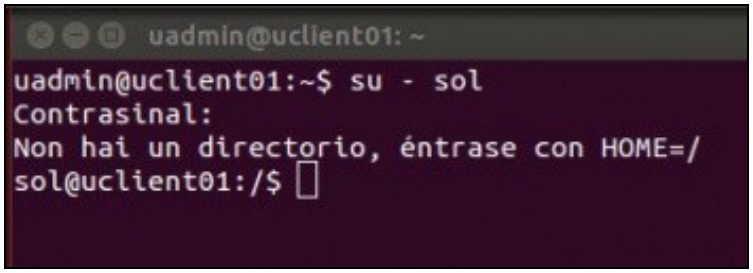
```
...
sol:x:10000:10000:Profe - Sol Lua:/home/sol:/bin/bash
noe:x:10001:10000:Profe - Noe Ras:/home/noe:/bin/bash
```

- Tamén con **getent group**, observamos os grupos que usuarios os teñen como grupos secundarios.

```
...
g-usuarios:*:10000:
g-profes:*:10001:noe,sol
g-dam1-profes:*:10002:sol
g-dam2-profes:*:10003:noe,sol
```

- A segunda forma é iniciar sesión no equipo cliente con un usuario do LDAP:
    - Deberemos iniciar a sesión en **modo de texto**, **non en modo gráfico, iso verase na parte III do curso.**
    - Utilizando por exemplo unha consola virtual, premendo nas teclas Control+Alt+F1 (En VirtualBox CTRL_DEREITA+F1), e poderemos volver ao contorno gráfico premendo Control+Alt+F7), xa que ao non existir no equipo cliente a carpeta persoal do usuario (/home/usuario), se intentamos iniciar unha sesión en modo gráfico produciranse unha serie de erros impedirán o inicio de sesión (Solucionaremos este problema con *NFS* máis adiante).
    - Tamén o podemos facer dende o contorno gráfico entrando como **uadmin** e pasándonos a un dos usuarios de LDAP.
- Antes de nada imos reiniciar os sevizos cliente de ldap:

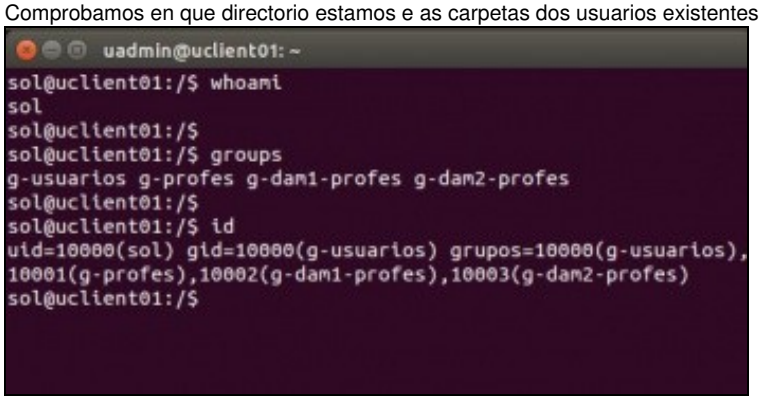
```
sudo service nslcd restart
sudo service nscd restart
```

- Dende un terminal de Ubuntu
- 

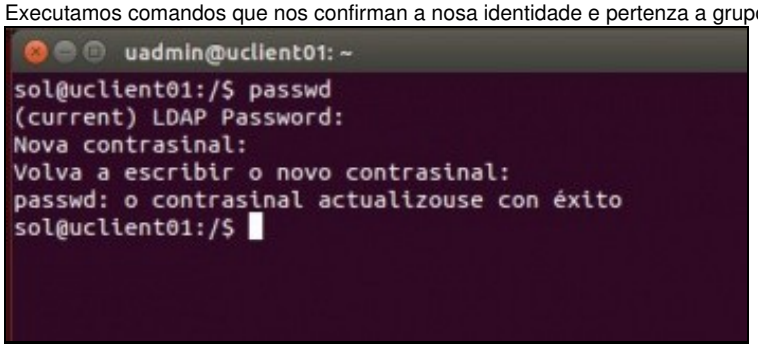
Pasámonos a usuaria sol: **su - sol**. Vemos que non temos directorio home e que se asigna o directorio raíz como directorio home da usuaria. Na parte III resolveremos este problema.

- 

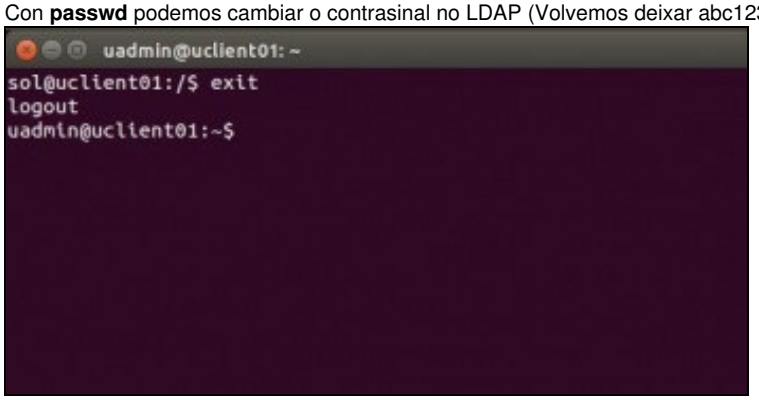

Comprobamos en que directorio estamos e as carpetas dos usuarios existentes no cliente, non está a de sol!!!. Na parte III resolverase

- 


Executamos comandos que nos confirman a nosa identidade e pertenza a grupos.

- 


Con **passwd** podemos cambiar o contrasinal no LDAP (Volvemos deixar abc123.).

- 


Con **exit** ou **logout** pechamos a sesión de sol.

## Configuración cliente LDAP en dserver00 e uclient02

- Queda para o/a lector/a configurar o cliente LDAP nos seguintes equipos:
    - **dserver00** (Ollo que servidor dserver00, por agora só é servidor de LDAP, pero aínda non é cliente de si mesmo).
    - **uclient02**

-- Antonio de Andrés Lema e Carlos Carrión Álvarez