

Configuración do cliente LDAP

Sumario

- 1 Introducción
- 2 Instalar os paquetes necesarios
- 3 Ficheiro de configuración /etc/nslcd.conf
- 4 Probar o funcionamento do cliente
- 5 Configuración cliente LDAP en dserver00 e uclient02

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 pertencen 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
```

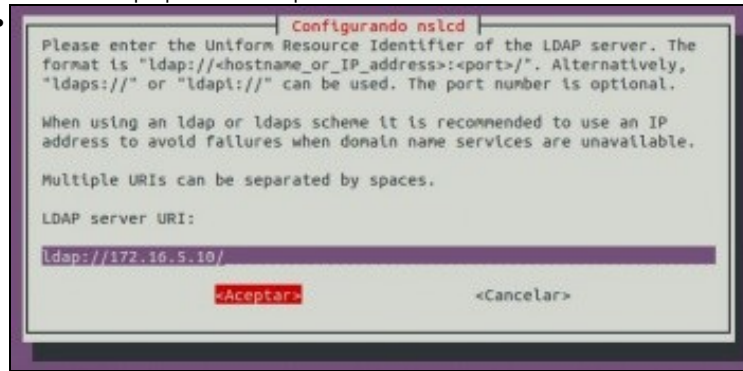
- Este novo paquete fai toda a configuración dun modo moi sinxelo por nós, con moitos menos pasos que o paquete que se menciona ao principio.

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

```
uadmin@uclient01: ~  
uadmin@uclient01:~$ sudo apt-get install libpam-ldapd  
Lendo as listas de paquetes... Feito  
Construindo a árbore de dependencias  
Lendo a información do estado... Feito  
Instalaranse os seguintes paquetes extra:  
  ldap-utils libnss-ldapd nscd nslcd  
Paquetes suxeridos:  
  kstart  
Os seguintes paquetes NOVOS hanse instalar:  
  ldap-utils libnss-ldapd libpam-ldapd nscd nslcd  
0 anovados, 5 instalados, Vanse retirar 0 e deixar 3 sen anovar.  
Ten que recibir 386 kB de arquivos.  
Despois desta operación ocuparanse 1732 kB de disco adicionais.  
Quere continuar? [S/n]
```

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:

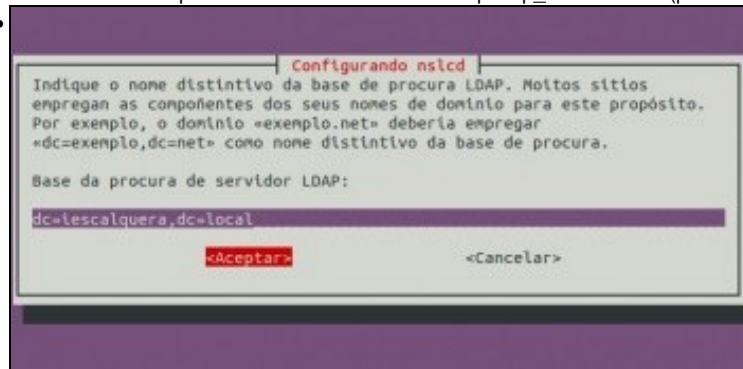
-**ldap**: que usa o protocolo TCP e escoita no porto 389, podemos conectarnos dende calquera sitio coa sintaxe: ldap://ip_do_servidor

-**ldapi**: que se usa para conectarse dende o cliente **dentro do mesmo servidor** ao demo slapd usando **Sockets de Unix**

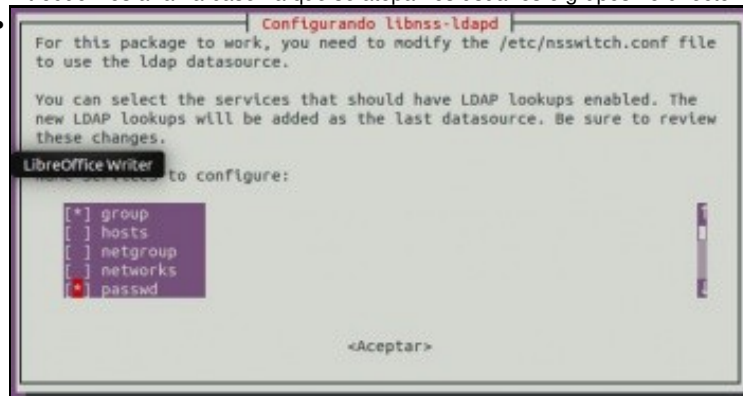
(http://es.wikipedia.org/wiki/Socket_Unix) e non a pila de protocolos TCP/IP. Para conectarse so precisamos poñer o nome do protocolo:

ldapi:/// (Olla coas tres barras).

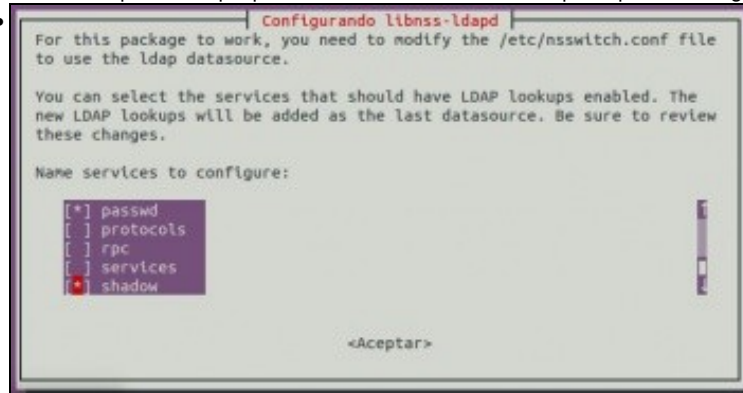
- **ldaps**: permite realizar conexións cifradas (seguras) entre os clientes e o servidor como veremos no escenario 1.F. Usa tamén o protocolo TCP e escoita no porto 636. Para conectarse. ldaps://ip_servidor:636 (porto opcional).



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.

```
* Starting LDAP connection daemon nslcd [ OK ]
A configurar ldap-utils (2.4.31-1+nmu2ubuntu8) ...
A configurar nscd (2.19-0ubuntu6) ...
* Starting Name Service Cache Daemon nscd [ OK ]
A procesar os disparadores de ureadahead (0.100.0-16)...
A configurar libnss-ldapd:amd64 (0.8.13-3) ...
/etc/nsswitch.conf: enable LDAP lookups for group
/etc/nsswitch.conf: enable LDAP lookups for passwd
/etc/nsswitch.conf: enable LDAP lookups for shadow
A configurar libpam-ldapd:amd64 (0.8.13-3) ...
A procesar os disparadores de libc-bin (2.19-0ubuntu6)...
uadmin@uclient01:~$
```

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.

```
uadmin@uclient01:~$ getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

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) ...

```
uadmin@uclient01:~$ getent passwd
colord:x:113:121:colord colour management daemon,,,:/var/lib/col
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
uadmin:x:1000:1000:uadmin,,,:/home/uadmin:/bin/bash
vboxadd:x:999:1:/:/var/run/vboxadd:/bin/false
sshd:x:116:65534:/:/var/run/ssh:/usr/sbin/nologin
nslcd:x:117:125:nslcd name service LDAP connection daemon,,,:/va
n/false
sol:x:10000:10000:Profe - Sol Lua:/home/sol:/bin/bash
noe:x:10001:10000:Profe - Noe Ras:/home/noe:/bin/bash
uadmin@uclient01:~$
```

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

```
lightdm:x:118:
nopasswdlogin:x:119:
bluetooth:x:120:
colord:x:121:
pulse:x:122:
pulse-access:x:123:
uadmin:x:1000:
sambashare:x:124:uadmin
vboxsf:x:999:
nslcd:x:125:
g-usuarios:*:10000:
g-profes:*:10001:noe,sol
g-dam1-profes:*:10002:sol
g-dam2-profes:*:10003:noe,sol
uadmin@uclient01:~$
```

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

```
uadmin@uclient01:~$ cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

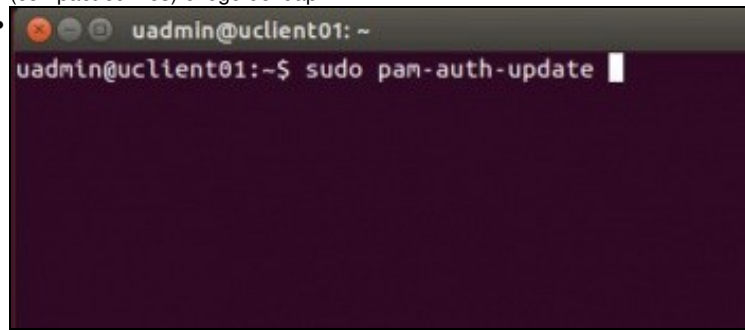
passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
gshadow:        files

#hosts:         files mdns4_minimal [NOTFOUND=return] dns
hosts:          files dns
networks:       files

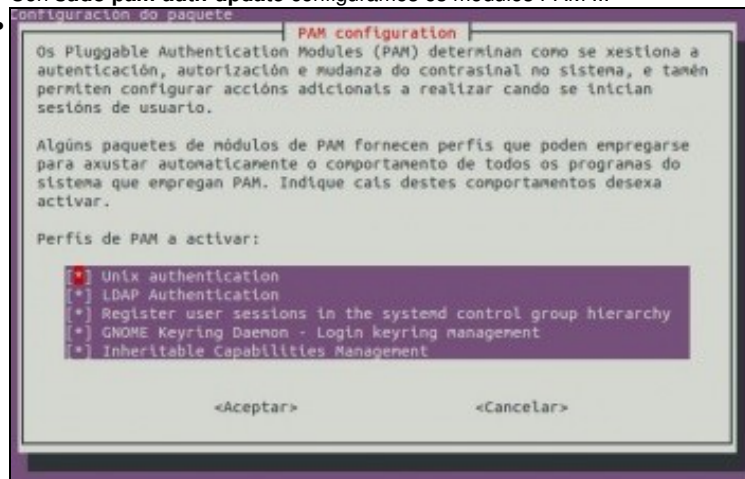
protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
uadmin@uclient01:~$
```

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 autentificación 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=anonymous,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 asegurarse 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 servizos cliente de ldap:

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

- Dende un terminal de Ubuntu

```
uadmin@uclient01: ~
uadmin@uclient01:~$ su - sol
Contrasinal:
Non hai un directorio, éntrese con HOME=/
sol@uclient01:/$
```

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.

```
uadmin@uclient01: ~
uadmin@uclient01:~$ su - sol
Contrasinal:
Non hai un directorio, éntrese con HOME=/
sol@uclient01:/$
sol@uclient01:/$ pwd
/
sol@uclient01:/$ ls /home
uadmin
sol@uclient01:/$
```

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

```
uadmin@uclient01: ~
sol@uclient01:/$ whoami
sol
sol@uclient01:/$
sol@uclient01:/$ groups
g-usuarios g-profes g-dam1-profes g-dam2-profes
sol@uclient01:/$
sol@uclient01:/$ id
uid=10000(sol) gid=10000(g-usuarios) grupos=10000(g-usuarios),
10001(g-profes),10002(g-dam1-profes),10003(g-dam2-profes)
sol@uclient01:/$
```

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

```
uadmin@uclient01: ~
sol@uclient01:/$ passwd
(current) LDAP Password:
Nova contrasinal:
Volva a escribir o novo contrasinal:
passwd: o contrasinal actualizouse con éxito
sol@uclient01:/$
```

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

```
uadmin@uclient01: ~
sol@uclient01:/$ exit
logout
uadmin@uclient01:~$
```

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** (Olla que servidor dserver00, por agora só é servidor de LDAP, pero aínda non é cliente de si mesmo).
 - ♦ **uclient02**