



Treball fi de carrera

**ENGINYERIA TÈCNICA EN
INFORMÀTICA DE SISTEMES**

**Facultat de Matemàtiques
Universitat de Barcelona**

**LDAP PER A ENTORNS MIXTES
WINDOWS/LINUX**

Iván Hidalgo Caballero

Director: Jaume Timoneda Salat
Realitzat a: Departament de
Matemàtica
Aplicada i Anàlisi.
UB

Barcelona, 4 de juliol de 2005

Índex

1. Resum del projecte.....	Pàg.3
2. Introducció	Pàg.5
3. Objectius del projecte	Pàg.7
4. NIS i NFS	Pàg.9
4.1. <i>Conceptes Teòrics</i>	Pàg.9
5 . LDAP.....	Pàg.13
5.1. <i>Conceptes Teòrics</i>	Pàg.13
5.2. <i>LDAP Servidor</i>	Pàg.18
5.2.1. <i>Conceptes Teòrics</i>	Pàg.18
5.3. <i>LDAP Client.....</i>	Pàg.21
5.3.1. <i>Conceptes Teòrics</i>	Pàg.21
5.4. <i>LDAP Segur</i>	Pàg.22
5.4.1. <i>Conceptes Teòrics</i>	Pàg.22
5.4.2. <i>SSL i TLS.....</i>	Pàg.22
6. Samba	Pàg.25
6.1. <i>Conceptes Teòrics</i>	Pàg.25
6.2. <i>smbldap-tools</i>	Pàg.30
6.2.1. <i>Conceptes Teòrics.....</i>	Pàg.30
7. CUPS.....	Pàg.31
7.1. <i>Conceptes teòrics</i>	Pàg.31
8. Configuració LDAP.....	Pàg.37
8.1. <i>Instal·lació LDAP.....</i>	Pàg.38
8.2. <i>LDAP</i>	Pàg.42
8.2.1. <i>Configuració.....</i>	Pàg.42
8.3. <i>LDAP Segur.....</i>	Pàg.56
8.3.1. <i>Creació certificats</i>	Pàg.56
8.3.2. <i>Configuració.....</i>	Pàg.61
8.4. <i>Eines de migració clients Linux a LDAP</i>	Pàg.63
8.5. <i>Compartir directori personal home.....</i>	Pàg.66
8.6. <i>Problemes.....</i>	Pàg.70

9. Configuració Samba.....	Pàg.77
9.1. Instal·lació.....	Pàg.77
9.2. Configuració Samba-LDAP.....	Pàg.80
9.3. Configuració Samba-LDAP-Segur.....	Pàg.101
9.4. smbldap-tools.....	Pàg.102
9.5. Clients Samba a Unix.....	Pàg.107
9.6. Afegir clients Windows al domini.....	Pàg.109
9.6.1. Microsoft Windows2000.....	Pàg.109
9.6.2. Microsoft Windows XP Professional.....	Pàg.110
9.7. Problemes.....	Pàg.111
10. Creació d'usuaris al directori LDAP.....	Pàg.113
10.1. Manualment.....	Pàg.113
10.2. Interfície web.....	Pàg.115
10.2.1. LDAP-Account-Manager.....	Pàg.115
10.2.2. phpLDAPadmin.....	Pàg.127
11. CUPS.....	Pàg.133
11.1. Instal·lació.....	Pàg.133
11.2. Configuració.....	Pàg.136
11.3. Instal·lació impressores en xarxa.....	Pàg.138
11.3.1. Instal·lació a sistemes operatius Linux.....	Pàg.142
11.3.2. Instal·lació a sistemes operatius Windows.....	Pàg.143
12. Temps implantació Sistemes LDAP-Samba.....	Pàg.149
13. Annexos.....	Pàg.151
13.1. Fitxer implementació servidor Samba-LDAP.....	Pàg.151
13.2. Fitxer implementació servidor Samba-LDAP Segur.....	Pàg.167
14. Bibliografia.....	Pàg.169
15. Glossari.....	Pàg. 175
16. Agraïments.....	Pàg.178

1. Resum del projecte

Amb la realització d'aquest projecte configurarem i instal·larem un servidor *LDAP*, que ens permetrà, amb l'ajuda de Samba, autenticar usuaris a entorns mixtes *Windows/Linux*.

El projecte vol servir de guia per tal d'implementar *LDAP* a les aules d'informàtica de la Universitat, fent que l'utilització de les màquines sigui més intuïtiva i fàcil per als alumnes. Cada alumne podrà fer ús del seu directori personal sigui quin sigui el sistema operatiu que utilitzi, i només li caldrà un nom d'usuari i clau per tal d'accedir tant a sistemes operatius *Windows* com *Unix*.

Inicialment explicarem els conceptes teòrics de les eines utilitzades per la implementació del nostre projecte, veurem detalladament que és *LDAP*, *Samba* i *CUPS*, les tres eines principals del nostre projecte, així com diferents eines que ens facilitaran l'administració del nostre servidor *LDAP*, eines que ens permetran migrar usuaris implementats a un sistema *NIS*, facilitar la compatibilitat entre *Samba* i *LDAP*, etc.

Posteriorment veurem com instal·lar i configurar tots els paquets necessaris per posar en marxa el projecte, veient els diferents modes de seguretat per tal d'implementar *LDAP* i les seves configuracions respectives. Explicarem pas a pas les modificacions necessàries als arxius de configuració de cada paquet instal·lat per tal de tenir un servidor *LDAP* treballant perfectament per autenticar usuaris en entorn mixtes *Windows/Linux*.

També tindrem en compte els problemes que ens han sorgit durant el transcurs de la realització d'aquest projecte, intentant que en el cas que aquest errors surtin a l'hora d'implementar el servidor *LDAP*, puguin ser solucionats ràpida i efectivament.

2. Introducció

Fa molt de temps les sales d'ordinadors, eren petites i amb pocs usuaris i recursos que manegar. L'entorn de computació era senzill i la seva era una tasca relativament senzilla. Tots treballaven al mateix lloc i no importava molt el perdre espai amb informació duplicada.

Però la situació va canviar ràpidament. Amb l'arribada de les xarxes de computadores la quantitat d'usuaris va augmentar de manera exponencial i els llocs de treball cada cop es varen fer més allunyats. També la quantitat d'informació emmagatzemada va fer que l'aprofitament dels recursos es convertís en una tasca vital.

Es va fer precís l'aparició de mecanismes que permetessin sincronitzar Aquests recursos de manera eficient. Es va buscar que els usuaris poguessin treballar en qualsevol màquina amb el seu compte, tenint a mà el seus arxius, el procés hauria de ser transparent per l'usuari. Es va pensar que seria idoni que l'administració de comptes i recursos fossin centralitzats, cosa que evitaria inconsistències. L'ús d'aquestes eines hauria ser consistent entre les diferents màquines per facilitar l'administració.

Els sistemes d'arxius de xarxa (*NFS*, Network File System) i el sistema d'informació de xarxes (*NIS*, Network Information Service) donen mecanismes per resoldre el problema de que qualsevol usuari, amb el seu identificador pogués entrar a qualsevol ordinador de la xarxa i tenir a mà els seus arxius. Això si parlem del Sistema Operatiu *Unix*.

Windows també va crear el seu sistema d'arxius de xarxa, a dia d'avui el que coneixem per *Active Directory* s'encarrega de l'administració d'usuaris dins d'un domini de la xarxa, fent que qualsevol usuari pugui entrar a qualsevol ordinador dins d'una xarxa *Windows*.

El problema el tenim quan intentem posar en marxa una xarxa que contingui diferents sistemes operatius. Cada fabricant de Sistemes Operatius té els seus propis protocols de xarxa, i això fa que la tasca de crear aquesta xarxa sigui si més no inviable.

Per solucionar aquests problemes tenim dues implementacions que ens permetran portar a terme les implementacions d'aquestes xarxes.

Per un costat tenim *LDAP* per l'administració d'usuaris i per un altre *Samba* que ens permetrà que amb màquines *Unix* i *Windows* puguem crear una xarxa consistent.

Més endavant parlarem més detingudament de totes dues implementacions.

3. Objectius del projecte

Aquest projecte intentarà facilitar les labors d'administració en sistemes heterogenis, en les quals existeixen múltiples clients, i cadascun d'aquests puguin tenir un sistema operatiu diferent, en els quals poden operar una infinitat d'usuaris el que fa l'administració d'aquests sistemes molt complicades. Posant un exemple, si no tinguessin una base de dades d'usuaris comú a tots els clients, s'hauria de donar d'alta a cada nou client en cada màquina que hagi d'utilitzar, i imaginem que per un canvi de política a la empresa, universitat, ... s'hagi de modificar algun aspecte a tots els comptes d'usuari existents, això faria que el temps d'implementació d'aquest canvi de política creixi exponencialment quan més usuaris tinguem.

Imaginem també l'aspecte de la compartició d'arxius entre els diferents usuaris, o el magatzem de documents i fitxers d'un determinat usuari, que poden utilitzar diferents clients, la cosa es complica. Per exemple en el cas de la nostra universitat, un usuari no pot utilitzar el seu *home* a *Windows* per desar els fitxers i documents fets en aquesta plataforma, la qual cosa l'obliga a utilitzar altres tipus de *software* o hardware per emmagatzemar la seva informació. Si aquest usuari tingués el seu *home* compartit, i el pogués utilitzar tan a *Linux* com a les plataformes de *Microsoft*, facilitaria molt la seva labor.

Un altre tema que reforçarà aquest projecte és el poder autenticar-se amb el mateix nom d'usuari i contrasenya en diferents sistemes operatius. Això permetrà privacitat a cada ordinador, ja que quan entris al teu compte saps que ningú més hi pot entrar.

Per poder portar a terme els objectius d'aquest projecte, per facilitar la integració en xarxes heterogènies, la principal idea és utilitzar un directori *LDAP* com a base de dades comú per utilitzar la informació relativa als usuaris (pot ser informació personal, relativa a comptes *Unix*, relativa a comptes *Samba/Windows* o gestor de correu).

Samba proveirà la integració de xarxes *Unix/Windows* per tal de simplificar l'intercanvi i emmagatzemament d'informació dels usuaris, i s'integrarà amb *LDAP* per tal de poder entrar a cadascun del sistemes operatius amb el mateix nom d'usuari i contrasenya. *Samba* permetrà per exemple, tenir un únic *home* per usuari, independentment del sistema operatiu que utilitzi. *Samba* actuarà també com a *PDC* (Controlador Primari de Domini) de la xarxa. *Samba* també ens permetrà la integració d'impressores i control d'aquestes per possibilitar la impressió a qualsevol usuari i qualsevol plataforma.

4. NIS i NFS

4.1. Conceptes Teòrics

Els protocols *NFS* i *NIS* van ser desenvolupats per Sun Microsystems i són pràcticament un estàndard alhora de resoldre aquests tipus de problemes.

NIS és un sistema de base de dades distribuïdes que permet compartir la informació del sistema en entorns basats en *Unix*. Alguns exemples d'aquesta informació són el fitxers `/etc/paswd`, `/etc/group`, `/etc/hosts`.

NIS aporta les següents avantatges:

- Proporciona un espai de noms consistent per als identificadors d'usuari i grup a un elevat nombre de sistemes.
- Redueix el temps i esforç per part de l'usuari per la gestió d'IDs d'usuari i grups.
- Redueix el temps i esforç dels administradors del sistema per a la gestió de IDs d'usuari i grups

NFS resol els següents conflictes:

- Permet que una col·lecció arbitrària de clients i servidors comparteixin un sistema d'arxius comú. En la majoria dels casos tots els clients i servidors han de ser a la mateixa xarxa, però no necessàriament.
- Un usuari pot veure els seus arxius independentment on estiguin localitzats, estiguin al seu disc local, a un disc compartit en un servidor o a una màquina que estigui a l'altra costat d'una xarxa.

NFS es pot complementar, i fer servir tant amb *LDAP* com amb *NIS*, *LDAP* ofereix moltes més millores que *NIS* tal i com veurem més endavant. Encara que si tenim una xarxa amb només ordinadors *Unix*, no seria una mala idea fer servir *NIS+NFS*. En el cas de la nostra universitat amb xarxa *Windows-Unix*, la implementació de *LDAP+NFS* facilitaria molt el treball dels administradors.

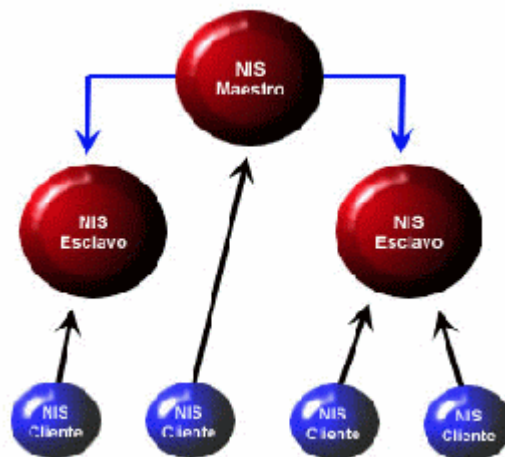
NIS i *NFS* faciliten la labor d'administració de xarxes, fent que es pugui prestar un millor servei.

NIS i *NFS* utilitzen protocols de xarxa per a comunicar-se amb altres màquines de la xarxa. *NIS* i *NFS* utilitzen el protocol de comunicació *TCP/IP*.

NIS és una base de dades distribuïda que reemplaça còpies d'arxius de configuració replicats per un arxiu central.

En lloc de manejar varies còpies d'arxius (com */etc/hosts*, */etc/passwd*, ...) s'utilitza una sola còpia que es modifica i s'emmagatzema en el servidor i és distribuïda entre els clients. No tots els arxius són candidats a ser emmagatzemats a un servidor central, com és el cas del */etc/fstab* ja que el seu contingut variarà molt d'un equip a un altre.

NIS i *NFS* treballen utilitzant el model client-servidor. Sota *NIS* un servidor és una màquina que conté arxius de dades per a *NIS*, anomenats mapes. Els clients són màquines que demanen informació sobre aquests mapes. Els servidors es poden subdividir també en mestres i esclaus, tal i com veiem a la figura.



Els servidors mestres són els veritables posseïdors dels mapes i s'encarregaran del seu manteniment i distribució. Els esclaus tindran la informació dels mapes del servidor i respondran les qüestions dels clients.

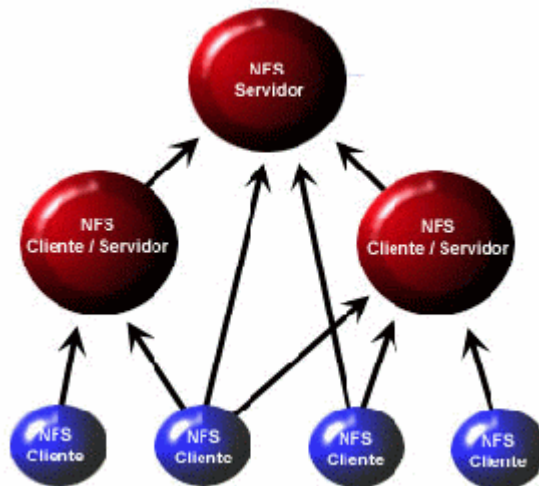
Un cop configurat un client per a que utilitzi *NIS* i el servidor està en marxa, alguns arxius deixaran de ser utilitzats en la seva totalitat (per exemple */etc/hosts*) o són complementats per *NIS* (com el */etc/passwd*). Uns altres en canvi només són útils si *NIS* està en funcionament.

Els mapes *NIS* no són guardats com a arxius ASCII. Els mapes són convertits a un format binari anomenat DBM, per raons d'eficiència en les cerques. *NIS* pot ser utilitzat per alguna cosa més que administrar l'arxiu de passwords, però no arriba al potencial que pot oferir *LDAP* per administrar usuaris i moltes coses més.

NFS és un sistema d'arxius distribuït que proveeix d'accés, de manera transparent a discs remots. *NFS* permet l'administració centralitzada d'aquests discs.

NFS utilitza el protocol RPC (Remote Procedure Call).

Sota *NFS* no existeix el concepte de client o servidor pur. Com es pot veure a la següent imatge, un servidor pot exportar un sistema d'arxius i pot muntar un sistema d'arxius a la vegada.



Hi ha dos aspectes bàsics en l'administració d'un sistema d'arxius usant *NFS*, escollir una nomenclatura dels noms i configurar els clients per tal que s'adhereixin a aquest esquema. Per exemple, podria decidir-se que els usuaris d'una companyia siguin agrupats segons el seu departament, això implica que tots els clients haurien de muntar els directoris remots seguint unes normes. Hem de saber que *NFS* va ser dissenyat per emascarar les complexitats de la xarxa, no per fer-les evidents.

5 . LDAP

En aquest capítol farem una breu introducció al servei de directoris, profunditzant un mica més en la implementació realitzada per *OpenLDAP*.

5.1. Conceptes Teòrics

Un servei de directoris és una base de dades optimitzada per la lectura, navegació i cerca. Els directoris solen tenir informació descriptiva basada en atributs i tenen capacitat de filtratge molt avançada. Els directoris generalment no poden suportar transaccions complicades ni esquemes de retorn enrere com els que es troben als sistemes de base de dades dissenyats per manejar grans i complexos volums d'actualització. Les actualitzacions dels directoris són normalment canvis senzills, o tot o res, sempre i quan estigui permès.

Els directoris estan afinats per tal de donar una resposta ràpida a grans volums de cerca. Aquests tenen la capacitat de replicar la informació per tal d'incrementar la disponibilitat i la fiabilitat, al temps que redueixen els temps de resposta. Quan la informació d'un directori es replica, es poden produir inconsistències temporals entre les rèpliques mentre aquesta s'està sincronitzant.

Hi ha moltes formes de donar un servei de directoris. Diferents mètodes permeten emmagatzemar diferents tipus d'informació al directori, tenint requisits diferents sobre com la informació ha de ser referenciada, consultada i actualitzada, com és protegida dels accessos no autoritzats, etc... Alguns serveis de directoris són locals, és a dir, donen el servei en un context restringit (per exemple el servei finger en una única màquina).

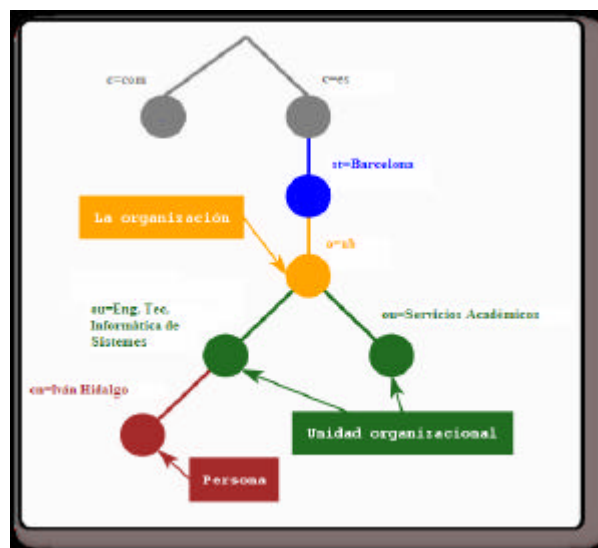
Altres serveis són globals i donen serveis més globals (per exemple, Internet), el serveis globals normalment són distribuïts, això vol dir que les dades estan repartides a diferents equips, els quals cooperen conjuntament per donar aquest servei de directori. Típicament un servei global defineix un espai de noms uniforme que dona la mateixa visió de les dades, independentment on estiguem, en relació a les dades. El servei *DNS* (*Domain Name System*) és un exemple d'un sistema de directori globalment distribuït.

LDAP són les sigles de *Lightweight Directory Access Protocol*, com el seu nom indica és un protocol lleuger per accedir al servei de directori, especialment el basat en *X.500*. *LDAP* s'executa sobre *TCP/IP* o sobre altres serveis de transferència orientats a connexió.

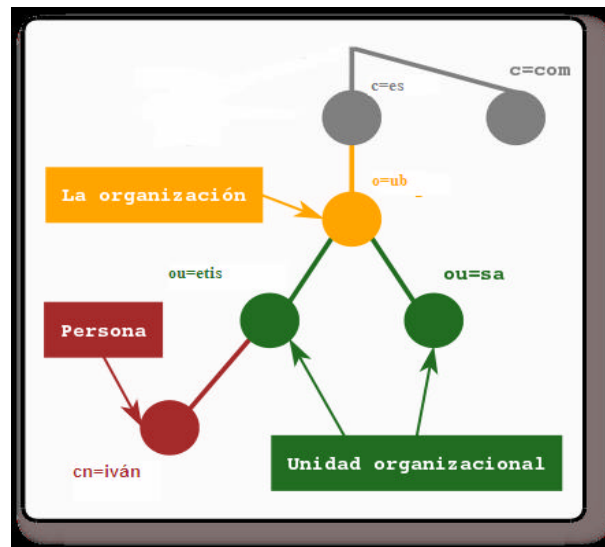
El model d'informació *LDAP* està basat en entrades. Una entrada és una col·lecció d'atributs que tenen un únic i global *Nom Distingit (DN)*. El *DN* s'utilitza per referir-se a una entrada sense ambigüitats. Cada atribut d'una entrada conté un tipus i un o més valors. Els tipus són normalment paraules mnemotècniques, com per exemple *cn* (*common name*), o *mail* per una adreça de correu. La sintaxis de l'atribut depèn del tipus d'atribut. Per exemple, un atribut *cn* pot contenir el valor *Iván Hidalgo*, així com un atribut *mail* ha de contenir un valor del tipus ivan@projecte.com, o un atribut *jpegPhoto* ha de contenir una imatge *JPEG*.

En *LDAP*, les entrades estan organitzades en una estructura jeràrquica d'arbre. Tradicionalment, aquesta estructura representava els límits geogràfics i d'organitzacions.

Les entrades que representaven països apareixien a la part superior de l'arbre, sota aquests països tenim les entrades que representen els estats i les organitzacions nacionals. Sota d'aquestes, poden estar les unitats que representen les unitats d'organitzacions, empleats, documents, impressores, o tot el que puguem imaginar. La següent imatge mostra un exemple d'un arbre de directoris *LDAP* fent ús d'un llenguatge tradicional.



L'arbre també es pot organitzar basant-se en els noms de domini d'Internet. Aquest tipus de nomenclatura s'està tornant molt popular ja que permet localitzar un servei de directori utilitzant els *DNS*. La següent figura mostra un exemple de directori *LDAP* que fa ús dels noms basats en aquests dominis.



LDAP també permet controlar quins atributs són requerits i permisos a una entrada fent ús de l'atribut denominat *objectClass*. El valor de l'atribut *objectClass* determina quines regles de disseny (*schema rules*) ha de seguir l'entrada.

Una entrada és referenciada pel seu nom distingit, que es construeix pel nom de la seva pròpia entrada (anomenat *Nombre Relatiu Distingit* o *RDN*) i la concatenació dels noms de les entrades antecessores. Per exemple, la entrada *iván* en l'exemple anterior tindria el següent *RDN*: *uid=iván,ou=etis,dc=ub,dc=es*. El format complet pels DN està descrit al *RFC2253-Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names*.

Per accedir a la informació continguda al nostre servei de directori, *LDAP* defineix operacions per interrogar i actualitzar el directori. Proveeix operacions per afegir i esborrar entrades del directori, modificar una entrada existent i canviar el nom d'aquesta. La major part del temps, en canvi, *LDAP* s'utilitza per buscar informació emmagatzemada al servei de directori. Les operacions de cerca de *LDAP* permeten cercar entrades que concordin amb algun tipus especificat per un filtre de cerca.

La informació pot ser sol·licitada des de cadascuna de les entrades que concordin amb el criteri establert. Per exemple, si es vol cercar un subarbre del directori que està per sota de *dc=ub,dc=es* a persones amb el nom *Iván Hidalgo*, s'obté l'adreça de correu electrònic de cada entrada que concordi. *LDAP* permet fer aquestes i moltes més cerques molt fàcilment.

Alguns serveis de directoris no proveeixen protecció, això fa que qualsevol persona pugui accedir a la informació. *LDAP* conté un mecanisme de autenticació per als clients o confirmació de identitat en un servei de directori, facilitant el camí per a un control d'accés que protegeixi la informació que el servidor suporta, i a més també suporta els serveis de privacitat i integritat.

El servei de directori *LDAP* treballa amb el model Servidor/Client. Un o més servidors *LDAP* contenen les dades que conformen la informació de l'arbre de directori. El client es connecta als servidors i els hi formula preguntes, els servidors li donen una resposta o un punter a on el client pot obtenir informació addicional (un altre servidor *LDAP*.) No importa a quin servidor *LDAP* es connecti el client, aquest sempre hauria d'obtenir la mateixa visió del directori, un nom representat per un servidor *LDAP* referència la mateixa entrada que qualsevol altre servidor *LDAP*. Aquesta característica és molt important al serveis globals de directoris com és *LDAP*.

Tècnicament *LDAP* és un protocol d'accés a directori per al servei de directori *X.500*, el servei de directori d'*OSI*. Inicialment els clients *LDAP* accedien a través de portes d'enllaç al servei de directori *X.500*. Aquesta porta executava *LDAP* entre el client i la porta d'enllaç, i el protocol *X.500* d'accés al directori (*DAP*) entre la porta d'enllaç i el servidor *X.500*.

DAP és un protocol extremadament pesat que opera sobre una pila de protocol *OSI* completa i requereix una quantitat significativa de recursos computacionals, en canvi *LDAP* està dissenyat per operar sobre *TCP/IP* proporcionant una funcionalitat similar a la de *DAP*, però amb un cost inferior.

Tot i encara que *LDAP* es continua utilitzant per accedir al servei de directori *X.500* a través de la seva porta d'enllaç, avui en dia és més comú implementar *LDAP* directament als servidors *X.500*.

El dimoni autònom de *LDAP*, o *slapd* és una mena de servidor de directoris lleugers *X.500*, és a dir, no implementa el *DAP X.500* sinó un subconjunt de models *X.500*.

LDAPv3 va ser desenvolupat als anys 90 per reemplaçar a *LDAPv2*. *LDAPv3* incorpora les següents característiques a *LDAP*:

- Autenticació forta gracies a l'ús de *SASL*
- Protecció d'integritat i confidencialitat fent ús de *TLS(SSL)*
- Internacionalització gracies a l'ús d'*Unicode*
- Revisions i continuacions.
- Descobrimet d'esquemes
- Extensibilitat (controls, operacions esteses...)

LDAPv2 és un històric , moltes de les implementacions amb *LDAPv2* (incloent *slapd*) no s'adapten a les especificacions tècniques de *LDAPv2*, la interacció entre les diferents implementacions de *LDAPv2* és molt limitada. Com *LDAPv2* difereix significativament de *LDAPv3* la interacció entre les dues versions pot ser una mica problemàtica. *LDAPv2* ha d'evitar-se, així que en la implementació d'*OpenLDAP* ve deshabilitat per defecte.

Per implementar *LDAP* al nostre servidor farem servir l' *OpenLDAP*, *OpenLDAP* és de lliure distribució. La majoria de distribucions *GNU/Linux* ja incorporen els paquets binaris d'*OpenLDAP*, encara que sinó fos el cas, el podríem baixar de la pàgina principal del projecte *OpenLDAP*, www.openldap.org.

5.2. LDAP Servidor

5.2.1. Conceptes Teòrics

El servidor *LDAP* és l'encarregat de acceptar les connexions dels clients *LDAP* i donar resposta a les consultes enviades pels clients. El servidor pot contestar amb la resposta corresponent o també amb una indicació a on pot aconseguir més informació, normalment un altre servidor *LDAP*. No té importància amb quin servidor és connecti, el client sempre veurà la mateixa vista del directori *LDAP*.

El servidor de *LDAP* conté un parell de dimonis que escolten sempre si hi ha alguna connexió per part d'un client *LDAP*. Els dimonis que utilitza el servidor *LDAP* són *slapd* i *slurpd*, *slapd* és un servidor de directori *LDAP* que s'executa en diferents plataformes. Algunes de les característiques més interessants de *slapd* són:

- Implementa la versió 3 de *Lightweight Directory Access Protocol*.
- Suporta *LDAP* sobre *IPv4*, *IPv6* i *Unix IPC*.
- Conté suport d'autenticació forta gràcies a l'ús de *SASL*. La implementació de *SASL* de *slapd* fa ús del *software Cyrus SASL*, el qual dóna suport a gran nombre de mecanismes d'autenticació tals com *DIGEST-MD5*, *EXTERNAL* i *GSSAPI*.
- Conté proteccions de privacitat e integritat gràcies a l'ús de *TLS* (o *SSL*). La implementació *TLS* de *slapd* fa ús del *software OpenSSL*.
- Es pot configurar per restringir l'accés a la capa de *sockets* basant-se en la informació topològica de la xarxa. Aquesta característica fa ús dels *TCP wrappers*.
- Proveeix facilitats de control d'accés molt potents, permeten controlar l'accés a la informació de les seves bases de dades. Pot controlar l'accés a les entrades basant-se en la informació d'autorització de *LDAP*, a l'adreça *IP*, en els noms de domini i altres criteris
- Suporta el control d'accés a la informació tan dinàmic com estàtic.
- Suporta *Unicode* i etiquetes de llenguatges.

slapd ve amb una sèrie de backends per a diferents bases de dades, els diferents backends que incorpora *slapd* són:

- *BDB*, un *backend* d'una base de dades transaccional d'alt rendiment.
- *LDBM*, un *backend* lleuger basat en *DBM*, *SHELL* una interfície per a *scripts* de shell.
- *PASSWD* un *backend* simple per a l'arxiu *passwd*.

El *backend BDB* fa ús de *Sleepycat Berkeley DB* i *LDBM* utilitza *Berkeley DB* o *GDBM*.

slapd és pot configurar per a servir múltiples bases de dades al mateix temps. Això significa que un únic servidor *slapd* pot respondre a peticions de diferents porcions lògiques de l'arbre *LDAP*, fent ús del mateix o diferents backends de base de dades.

Si es necessita més personalització *slapd* permet escriure els seus propis mòduls fàcilment. *slapd* consisteix en dos parts: un frontend que maneja les comunicacions de protocol amb els diferents clients *LDAP*, i mòduls que manegen tasques específiques, com poden ser les operacions amb les bases de dades. Degut a que aquestes dues peces es comuniquen a través d'una *API C* ben definida, podem escriure els nostres propis mòduls, que estendran *slapd* de múltiples formes. També existeixen nombrosos mòduls programables de bases de dades. Aquests permeten a *slapd* accedir a fonts de dades externes fent ús de llenguatges de programació molt populars, tals com *Perl*, *shell*, *SQL* i *TLC*.

slapd fa ús de fils(*threads*) per a obtenir un alt rendiment. Un procés únic multifil(*multithread*) maneja totes les peticions entrants. L'ús de fils(*threads*) fa reduir la càrrega del sistema així com proveeix d'alt rendiment.

slapd es pot configurar per que mantingui còpies de la informació del directori.

L'esquema que utilitza *LDAP*, un únic mestre/múltiples esclaus és vital en ambients amb un volum alt de peticions, on un únic servidor *slapd* no podria proveir la disponibilitat ni la seguretat necessàries. *slapd* inclou també un suport experimental per la replicació de múltiples mestres. *slapd* suporta dos mètodes de replicació: *Sync LDAP* i *slurpd*.

slapd pot ser configurat com un servei proxy caché *LDAP*.

slapd és altament configurable a través d'un únic arxiu de configuració que permet modificar tot allò que es necessiti canviar. Les opcions per defecte són raonables la qual cosa facilita una mica el treball.

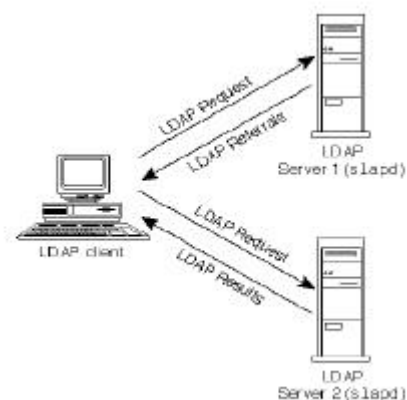
slapd és un dimoni que, amb l'ajut de *slapd*, permet proveir el servei de replicació. És el responsable de distribuir els canvis realitzats en la base de dades *slapd* principal fins a les diferents replicues *slapd*. Aquest dimoni allibera a *slapd* de preocupar-se per l'estat de les rèpliques (si s'han caigut, si no són accessibles, quan s'han modificat...) i maneja automàticament el reenviament de les peticions fallides. *slapd* i *slurpd* es comuniquen a través d'un arxiu de text, que s'utilitza per emmagatzemar els canvis ocorreguts.

5.3. LDAP Client

5.3.1. Conceptes Teòrics

Els clients *LDAP* seran totes aquelles màquines que cercaran els servidors *LDAP* de la seva xarxa per tal de enviar-li una consulta que el servidor *LDAP* haurà de filtrar, solucionar i respondre a aquesta consulta. El client rebrà la resposta del servidor que li farà autenticar-se, obtenir el resultat d'una cerca del directori *LDAP*, etc. Podem configurar que totes les aplicacions del client *LDAP* que utilitzin *PAM*, facin servir el directori *LDAP* per a la autenticació. La configuració d'aquestes aplicacions la podrem veure posteriorment.

Un esquema bàsic del funcionament del client seria el que mostra a la següent figura:



El primer pas que farà el client *LDAP* serà obrir una connexió *TCP* sobre el servidor *LDAP* i farà un lligam entre client i servidor. Aquest lligam inclourà el nom del directori on el client vol autenticar-se i les credencials que utilitza per autenticar-se. Aquestes credencials podem ser simples passwords o passwords més certificats que seran utilitzats per autenticar el client. Un cop el client s'autentifica, el servidor li respon si aquesta autenticació ha estat correcta o no. Llavors el servidor processa la resposta, i dóna els resultats convenients a la pregunta. Un cop el client ha rebut la informació, es desconnecta avisant prèviament al servidor de la seva desconnexió. El servidor un cop li arriba la informació que el client s'ha desconnectat, acaba la connexió.

5.4. LDAP Segur

5.4.1. Conceptes Teòrics

LDAP permet als seus clients i servidors fer ús de *TLS* (*Transport Layer Security*) i *SSL* per a donar major integritat i major protecció de la confidencialitat de les dades. Hem de pensar que aquestes dades, han d'estar quan més protegides millor. *LDAP Segur* ens permet consolidar el nostre servei de directori. Gràcies a la seguretat de la pròpia xarxa i l'ús de certificats alhora d'autenticar-se al servei de directori., podem assegurar una gran protecció de les dades.

LDAP Segur només aporta a *LDAP* la utilització del xifrat al transmetre les dades i els certificats per millorar la seguretat, per la qual cosa tot el que hem explicat al punt anterior ens servirà ara. El canvi vindrà a l'hora de configurar *LDAP* de forma segura. Com veurem més endavant.

Com per la configuració de *LDAP Segur* ens caldrà utilitzar certificats, a continuació veurem teòricament els protocols utilitzats per *LDAP* per a xifrar la connexió i garantir l'autenticació.

4.4.2. SSL i TLS

El protocol *SSL* és un sistema dissenyat i proposat per Netscape Communications Corporation. Aquest protocol es troba a la pila d'*OSI*, entre els nivells de *TCP/IP* i els protocols d'enllaç (*HTTP*, *FTP*,...). *SSL* proporciona serveis de seguretat xifrant les dades intercanviades entre servidor i client amb un algoritme de xifrat simètric, i xifrant la clau de sessió mitjançant un algoritme de xifrat de clau pública (normalment *RSA*).

La clau de sessió serà la encarregada de xifrar les dades que venen i van cap al servidor segur. Sempre es genera una clau diferent per a cada transacció, això comporta que encara que algú ataquí el sistema en una transacció, això no farà que pugui desxifrar futures transaccions a partir d'aquesta. *MD5* s'utilitza com l'algoritme de hash.

SSL proporciona xifrat de dades, autenticació de servidors, integritat de missatges i opcionalment, autenticació de client per a connexió *TCP/IP*.

Quan el client demana al servidor segur una comunicació segura, el servidor obre un port xifrat, gestionat per un *software* anomenat *Protocol SSL Record*, que es troba per sobre del protocol *TCP* a la pila *OSI*. Serà el *software* d'alt nivell, *Protocol SSL Handshake*, qui farà ús del *Protocol SSL Record* i el port obert pel servidor per comunicar-se de forma segura amb el client.

Durant el *Protocol SSL Handshake*, el client i el servidor intercanviaran una sèrie de missatges per a negociar les millores de seguretat. Aquest protocol segueix sis fases, que explicarem de manera resumida:

- La primera fase, Client i servidor s'encarregaran de posar-se d'acord sobre el conjunt d'algoritmes per mantenir la intimitat i l'autenticació.
- La fase d'intercanvi de claus, en la que el protocol intercanviarà informació sobre les claus, de tal manera que al final totes dues parts, client i servidor, compartiran una clau mestra.
- La fase de producció de la clau de sessió, que serà la utilitzada per xifrar les dades intercanviades.
- La fase de verificació del servidor, estarà present només quan utilitzem *RSA* com algoritme d'intercanvi de claus, i servirà per a que el client autentiqui al servidor.
- La fase d'autenticació del client, en la que el servidor sol·licita al client un certificat *X.509* (en el cas que sigui necessària la autenticació del client).
- Per finalitzar tenim la fase fi, que indica que ja es pot començar la sessió segura.

El *Protocol SSL Record* especifica la forma d'encapsular les dades transmeses i rebudes. La porció de dades del protocol té tres components:

- *MAC-DATA* = codi d'autenticació del missatge
- *ACTUAL_DATA* = dades d'aplicació a transmetre
- *PADDING-DATA* = dades requerides per omplir el missatge quan s'utilitza xifrat en bloc.

Encara i tot, a *SSL* li manca molts dels elements necessaris per a construir un sistema de transaccions segura a Internet.

Per posar un exemple a *SSL* no hi ha forma de saber quan s'ha fet una transacció, quins han estat i quins han intervingut en aquesta. *SSL* no proporciona formes d'emetre rebuts vàlids que identifiquin una transacció.

Encara i la manca d'elements necessaris, *SSL* no ha pogut ser desbancat per cap altre protocol, degut a que *SSL* és una tecnologia ràpida, molt fàcil d'implementar, barata, còmoda per a l'usuari, que no ha de saber com funciona, només utilitzar-la.

Per a intentar corregir les deficiències observades a *SSL* v3 es va buscar un nou protocol que permetés transaccions segures per Internet, sobre tot, tenint en compte que *SSL* és propietat de Netscape. El resultat d'aquesta cerca va ser *TLS*, que permet una compatibilitat total amb *SSL* però amb la diferència que *TLS* és un protocol públic, estandarditzat per la *IETF*.

TLS busca integrar a un esquema tipus *SSL* al sistema operatiu, a nivell de la capa *TCP/IP*, per a que l'efecte *túnel* que es va implementar amb *SSL* sigui realment transparent a les aplicacions que s'estiguin executant. *TLS* surt de les mateixes bases que *SSL*, però es diferencia de *SSL* en diversos aspectes fundamentals:

- En la fase 4 del *Protocol SSL Handshake*, el client només contestarà amb un missatge si són *SSL*.
- Les claus de sessió es calculen de maneres diferents.
- A l'hora d'intercanviar les claus, *TLS* no suporta l'algoritme simètric *Fortezza*, que sí suporta *SSL*. Això és degut a que la cerca d'un codi públic, ja que *Fortezza* és de propietat privada.
- *TLS* utilitza dos camps més al *MAC* que *SSL*, la qual cosa el fa més segur.

A pesar de millorar *SSL* i de ser públic, *TLS* no està tenint encara l'acceptació desitjada.

6. Samba

6.1. Conceptes Teòrics

Samba és una eina de xarxa extremadament útil per qualsevol persona que en la seva xarxa tingui tant sistemes *Unix* com *Windows*. *Samba* s'executa en un sistema *Unix*, permetent als sistemes *Windows* compartir arxius i impressores amb la màquina *Unix*, a la vegada que els usuaris *Unix* tenen accés als recursos compartits per als sistemes *Windows*.

Encara que sembli natural fer ús de servidors *Windows* per utilitzar arxius i impressores en una xarxa a on hi hagi clients *Windows*, existeixen moltes i bones raons per escollir un servidor *Samba* per aquests serveis. *Samba* és un *software* compatible que s'utilitza en un sistema operatiu fiable com és *Unix*, donant com a resultat la reducció de problemes i un baix cost de manteniment. A part de tot això, *Samba* ofereix un millor rendiment en càrregues de treball extremadament dures, sobrepasant a un servidor *Windows 2000* en un factor 2 a 1 en un *PC* amb la mateixa configuració de hardware, d'acord amb els benchmarks publicats per tercers. Quan un *PC* ja no pugui aguantar les peticions dels clients degut a una alta càrrega de treball, el servidor *Samba* es pot traslladar fàcilment a un mainframe *Unix* propietari, el qual pot sobrepassar en molt un *PC* corrent amb *Windows*. A més a més *Samba* té un gran avantatge en quant a cost: és lliure. No només el *software* està a la seva disposició lliurement, sinó que no es necessita cap tipus de llicència per als clients, executant-se en sistemes operatius de gran qualitat i lliures, tals com *GNU/Linux* i *FreeBSD*.

Samba és una suite d'aplicacions *Unix* que parla el protocol *SMB* (*Server Message Block*) El sistema operatiu *Microsoft Windows* i *OS/2* utilitzen *SMB* per compartir per xarxa arxius i impressores a més de per realitzar tasques associades. Gràcies al suport d'aquest protocol *Samba* permet a les màquines *Unix*, entrar en joc, comunicant-se amb el mateix protocol de xarxa que *Microsoft Windows* i aparèixer com un altre sistema *Windows* a la xarxa (mirant des de la perspectiva d'un client *Windows*).

El servidor *Samba* ofereix els següents serveis:

- Compartir un o varis sistemes d'arxiu.
- Compartir un o varis sistemes d'arxiu distribuïts.
- Compartir impressores instal·lades al servidor entre clients *Windows* de la xarxa.
- Ajudar als clients permetent-li navegar per la xarxa.
- Autenticar als clients que ingressen a un domini *Windows*.
- Proveir o ajudar amb un servei de resolucions de noms *Windows* (*WINS*)

La suite de *Samba* també inclou eines per als clients, que permeten als usuaris de sistemes *Unix* accedir als directoris e impressores que els sistemes *Windows* i servidors *Samba* comparteixen a la xarxa.

Samba és la idea de Andrew Tridgell, qui actualment lidera l'equip de desenvolupament de *Samba*. El projecte va néixer a 1991 quan feia una suite per connectar ordinadors *VAX DEC* amb els d'altres companyies. Sense conèixer la transcendència del que estava fent, va crear un programa servidor d'arxius per a un estrany protocol que formava part de la suite de *PathWorks*. Aquest protocol va passar a anomenar-se més tard *SMB*. Uns anys més tard el va alliberar com el seu servidor *SMB* particular i el va començar a distribuir per Internet amb el nom de *SMB Server*. Nom que no va poder mantenir perquè ja estava en ús. Així que va intentar el següent per donar-li un altre nom des de *Unix*:

```
$ grep -i '^s.*m.*b' /usr/dict/words
```

Obtenint com a una de les respostes: *samba* i d'aquí va sorgir el seu nom.

Avui en dia la suite *Samba* funciona a partir d'un parell de dimonis *Unix* que permeten la compartició de recursos entre els clients *SMB* en una xarxa. Aquests dimonis són:

- *smbd*: Permet la compartició d'arxius i impressores en una xarxa *SMB* i proporciona autenticació i autorització d'accés per a clients *SMB*.
- *nmbd*: Suporta el servei de noms *NetBIOS* i *WINS*, que és una implementació de *Microsoft* del servidor de noms *NetBIOS* (*NBNS*). Aquest dimoni també ajuda afegint la possibilitat de navegar per la xarxa.

Samba actualment és mantingut i actualitzat per uns voluntaris a les ordres de *Andrew Tridgell* i, igual que el nucli *Linux* els autors de *Samba* el distribueixen com a *software* open source, sota el termes de la llicència *GPL* (*GNU General Public License*). Des de la seva concepció, el desenvolupament de *Samba* ha estat patrocinat per la *Australian National University*, a partir d'aquesta moltes altres empreses com *HP, IBM, LinuxCare, VA Linux Systems*, han patrocinat als desenvolupadors de *Samba*.

Microsoft també ha contribuït oferint la definició del seu protocol d'Internet estàndard (*Common Internet File System, CIFS*) *SMB* (*Server Message Block*) al grup *IETF* (*Internet Engineering Task Force*) en 1996.

Samba pot ajudar la coexistència de màquines *Windows* i *Unix* en la mateixa xarxa. Existeixen moltes raons per les quals podríem instal·lar un servidor *Samba* en la nostra xarxa, entre les qual tenim:

- No poder disposar d'un servidor *Windows* complet, pel seu preu, encara que ens faci falta la funcionalitat d'aquest
- Les llicències per a que cada client pugui accedir al servidor *Windows* siguin prohibitives en quant a diners.
- Tenir un àrea comú per dades i directoris, tant per *Unix* com per *Windows*.
- Donar suport a usuaris que tenen ordinadors amb sistemes operatius tant *Unix* com *Windows*.
- Compartició d'impressores *Windows* i *Unix*.
- Integrar l'autenticació de *Windows* i *Unix*, mantenint una única base de dades pels comptes dels usuaris que funcioni en tots dos sistemes.
- Establir una xarxa entre sistemes *Unix* i *Windows* utilitzant un únic protocol.

Samba utilitza *NetBIOS*, *NetBIOS* assigna un nom a cada màquina que pot ser traduït a una *IP* llegible. Gràcies a aquesta traducció, l'administració de les diferents màquines es fa més senzilla.

En 1984, *IBM* va dissenyar una *API* simple per connectar en xarxa els seus ordinadors, amb el nom de *Network Basic Input/Output System (NetBIOS)*, que havia de intercanviar instruccions amb els ordinadors a través de xarxes *IBM PC* o *TokenRing*. A finals de 1985, *IBM* va alliberar aquest protocol, el que va fer que apareguessin diferents implementacions, com per exemple la *NetBIOS* per *IPX* de *Novell*.

Per Internet, una tecnologia que començava a aflorar en aquesta època, els protocols escollits van ser *TCP/IP UDP/IP* així com les implementacions *API NetBIOS* sobre aquests.

TCP/IP fa ús dels números per representar les direccions i *NetBIOS* utilitza noms. Aquest va ser el gran problema a l'hora de ajuntar aquests dos protocols, però al 1987 el grup *IETF (Internet Engineering Task Force)* va publicar els document per fer que *NetBIOS* pogués treballar sobre una xarxa *TCP/UDP*. Aquests documents són la base de les implementacions que existeixen avui en dia, incloent aquelles que són proporcionades per *Microsoft* pels seus sistemes operatius o per *Samba*.

Des de llavors, l'estàndard que aquests documents lideren s'ha convertit en *NetBIOS* sobre *TCP/IP*, o *NBT*.

NBT ofereix tres serveis sobre una xarxa:

- Un servei de noms
- Servei de comunicació amb datagrames.
- Servei de comunicació amb sessions.

El servei de noms permet donar un nom a cada ordinador de la xarxa i que es pugui convertir en un adreça *IP* llegible. Com fan els serveis *DNS* a Internet. El serveis de datagrames i sessions s'utilitzen per transmetre dades entre màquines *NetBIOS* en la xarxa.

A continuació podem veure els protocols sobre els que corre *Samba*:

OSI				TCP/IP	
Aplicación	SMB				Aplicación
Presentación					
Sesión	NetBIOS	NetBEUI	NetBIOS	NetBIOS	TCP/UDP
Transporte	IPX		DECnet	TCP & UDP	
Red		IP			
Enlace	802.2, 802.3, 802.5	802.2 802.3, 802.5	Ethernet V2	Ethernet V2	Ethernet u otras
Física					

Com podem veure *Samba* pot córrer sobre diferents protocols, tal com el *IPX* de *Novell*, *NBT* o *NetBEUI*, el que ens permet utilitzar *Samba* no només per xarxes *Unix* i *Windows*, sinó amb més sistemes operatius.

Samba és pot configurar per tal que actuï com un controlador de domini primari (*PDC*), en el cas del nostre projecte serà imprescindible que actuï com a tal. L'autenticació d'usuaris mitjançant un controlador de domini a *Windows* és similar als sistemes *Unix*. Per poder accedir al nostre controlador de domini ens caldrà un nom d'usuari i una clau vàlida, que son autenticats a través de la base de dades de claus del nostre *PDC*, en el nostre cas l'encarregat d'autenticar els usuaris serà *LDAP*. Si la clau no es vàlida ho notificarà a l'usuari de *Windows* i no podrà accedir al domini.

Si el nom d'usuari i la clau és vàlida, podrem accedir al domini i a qualsevol dels recursos d'aquest al qual l'usuari tingui drets sense necessitat de tornar a autenticar-te. Dit d'una altre manera, el nostre *PDC* retorna una senyal al client que li permet accedir a qualsevol recurs sense haver de consultar de nou al controlador primari del domini. Això suposarà una reducció important al tràfic de xarxa.

Com podem veure, el fet que *Samba* actuï com a *PDC* serà una peça molt important al nostre projecte, ja que serà la forma de poder autenticar-nos a màquines *Windows* amb el mateix nom d'usuari i clau que tindríem a *Unix*.

5.2. smbldap-tools

5.2.1. Conceptes Teòrics

smbldap-tools són un conjunt d'*scripts* que s'executen sobre les eines del sistema *user{add/del/mod}* i *group{add/del/mod}* per permetre la manipulació d'usuaris i grups emmagatzemats a un directori *LDAP*, destinats a sistemes *Samba-LDAP* i *PAM/nss_ldap*.

Adicionalment s'han dissenyat alguns *scripts* per facilitar la migració de servidors *PDC Windows NT 4.0* o servidors *PDC Samba-LDAP*. Algunes d'aquestes eines són *smbldap-populate*, *smbldap-migrate-groups* i *smbldap-migrate-accounts*.

L'última versió d'aquestes eines es troben a <http://samba.idealx.org>. La versió utilitzada a l'hora de realitzar la nostra instal·lació és la 0.8.4.

7. CUPS

7.1. Conceptes Teòrics

CUPS, Common *Unix* Printing System és un sistema d'impressió portable i extensible per a *Unix*. Històricament a *Unix* la impressió s'ha realitzat amb dos tipus de sistemes, el dimoni d'impressió de *Berkeley* (*LPD*) i el sistema d'impressió en línia d'AT&T.

Aquests sistemes d'impressió es va dissenyar en la dècada dels setanta a partir del qual es va afegir diversos nivells de suport per a tot tipus d'impressores. Als darrers anys s'han realitzat molts intents per desenvolupar una interfície estàndard d'impressió, alguns exemples serien l'estàndard de *POSIX* desenvolupat per la *IEEE* i el Protocol d'impressió de Internet (*IPP*) fet per la *IETF*. El protocol d'impressió estàndard de *POSIX* defineix un conjunt comú d'eines per la consola *Unix* tal com una interfície en *C* per a la administració i treballs d'impressió, però no va tenir èxit i va ser abandonat per la *IEEE*.

IPP defineix una sèrie d'extensions al Protocol de Transferència de Hipertext 1.1 (*HTTP*) que afegien suport pels serveis d'impressió remota. La primera versió d'*IPP* va ser acceptada per la *IETF* al 1999 i posteriorment ha actualitzat el conjunt d'especificacions per a *IPP/1.1*.

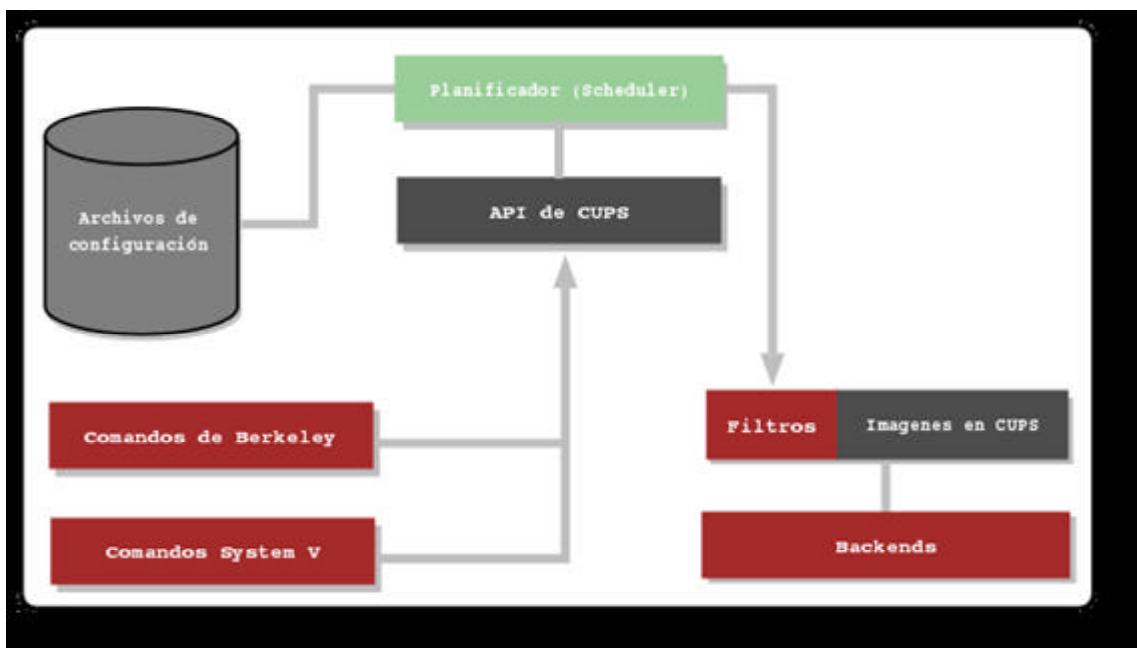
Just al contrari que *POSIX*, *IPP* ha estat acceptat per les grans empreses i s'ha impulsat per a ser la solució estàndard per a la impressió en xarxa de tots els sistemes operatius.

CUPS utilitza *IPP/1.1* per proporcionar un sistema d'impressió complet i modern, destinat a sistemes *Unix*, que pot ser ampliat per donar suport a noves impressores, dispositius i protocols, a la vegada que garanteix la compatibilitat amb les aplicacions *Unix* existents. *CUPS* és *software* lliure i és distribueix sota els termes *GPL* i *LGPL* (*Llicència pública general i Llicència pública general de llibreries*) del projecte *GNU*.

La primera versió de *CUPS* es va basar en *IPP/1.0* i va sortir al 1998. Des de llavors s'han publicat moltes actualitzacions per la versió 1.0, per corregir errors i afegir seguretat i portabilitat.

Avui en dia *CUPS* va per la versió 1.1 usant *IPP/1.1*, s'han afegit funcionalitats demandades pels seus usuaris. *CUPS 1.1* també té actualitzacions que podem consultar a través de la seva pàgina web www.CUPS.org.

Al igual que molts altres sistemes d'impressió *CUPS* es basa en un procés central de planejament (*scheduling*) d'impressió, que planifica tots els treballs d'impressió, processa les comandes d'administració i facilita la informació de l'estat de la impressora als programes locals i remots, informant a l'usuari que ho necessiti. A continuació podem veure l'organització bàsica de *CUPS*:



El planificador és un servidor *HTTP/1.1* que maneja peticions *HTTP*. A part de ocupar-se de les peticions enviades (*POST*) per la impressora a través del protocol d'*IPP*, el planificador també actua com un servidor web les funcions del qual serien mostrar la documentació, monitoritzar l'estat de les impressores i proveir d'una interfície per realitzar les tasques d'administració de les impressores.

També administra la llista d'impressores disponibles en una xarxa i reparteix els treballs d'impressió com sigui precis fent us dels filtres i backends apropiats.

Els arxius de configuració que conté *CUPS* són els següents:

- Arxius de configuració del servidor *HTTP*
- Arxius de definició de les impressores i les classes
- Els arxius de configuració dels tipus *MIME* i les regles de conversió.
- Els arxius *PPD* (*PostScript Printer Description*)

L'arxiu de configuració del servidor *HTTP* s'ha creat molt similar a l'arxiu de configuració d'*Apache*, per facilitar la seva edició, i defineix totes les propietats de control d'accés al servidor.

Els arxius de definició d'impressores i classes, llisten les cues i classes d'impressió disponibles. Els treballs enviats a una classe, són reenviats a la primera impressora disponible en aquesta classe, fa servir un model *Round-Robin*.

Els arxius de configuració tipus *MIME* llisten els tipus *MIME* suportats (*text/plain*, *application/postscript*, etc.) i les regles *màgiques* de l'autodetecció dels tipus de format d'un arxiu. El servidor *HTTP* els utilitza per determinar el camp *Content-Type* (tipus de contingut) per les peticions *GET* i *HEAD* així com pel manegador de peticions *IPP* per determinar el tipus d'arxiu quan es rebí un treball d'impressió o una petició d'enviament d'arxiu amb un format de document *application/octet-stream*.

Els arxius de regles de conversió *MIME* llisten els filtres disponibles, aquests filtres s'utilitzen quan un treball és despatxat, de tal forma que una aplicació pot enviar un arxiu convenientment formatat al sistema d'impressió, el qual convertirà el document en un format imprimible, si és necessari. Cada filtre té un cost relatiu associat, de forma que l'algoritme d'elecció de filtres pot escollir el conjunt de filtres que convertirà l'arxiu al format necessari amb el menor *cost total*.

Els arxius *PPD* descriuen les capacitats de totes les impressores , no només de les impressores *PostScript*. Existeix un arxiu *PPD* per a cada impressora.

Els arxius *PPD* per a impressores no *PostScript* defineixen un filtre addicional, a través de l'atribut *cupsFilter*, per a suportar els controladors de la impressora.

L'*API* de *CUPS* conté funcions de conveniència específiques de *CUPS* per als treballs de la cua d'impressió, obtenció d'informació de la impressora , accés als recursos a través de *HTTP* i *IPP*, així com manipular arxius *PPD*. Al contrari que la resta de *CUPS*, l'*API* de *CUPS* es distribueix sota els termes de la llicència *LGPL* del projecte *GNU*, per permetre el seu ús a aplicacions no *GPL*.

CUPS proveeix les interfícies de les comandes de consola de *System V* i *Berkeley*, que permeten l'enviament de treballs i comprovació de l'estat d'una impressora.

Les comandes *lpstat* i *lpcstatus* també mostren impressores de xarxa (*impressora@xarxa*) quan la cerca d'impressores està habilitada.

Les comandes d'administració de *System V* se subministren per manegar les impressores i les classes. Les eines d'administració de *Berkeley* (*lpc*) només són suportades en mode lectura, per comprovar l'estat actual de les cues d'impressió i del planificador.

El programa de filtrat que conté *CUPS* llegeix des de l'entrada estàndard o des d'un arxiu , si se li passa com a paràmetre. Tots els filtres han de poder suportar un conjunt comú d'opcions incloent el nom de la impressora, la *ID* del treball, el número de còpies i les opcions del treball. Aquestes sortides són enviades a la sortida estàndard.

Els filtres es subministren per a múltiples formats d'arxiu e inclouen arxius d'imatge i filtres de cerca *PostScript*, que suporten impressores no *PostScript*. Múltiples filtres s'executen en paral·lel per produir el format de sortida necessari.

El filtre de cerca de *PostScript* està basat en el nucli de *GhostScript 5.0*. En lloc d'utilitzar els controladors d'impressió i front-ends de *GhostScript*, el filtre de *CUPS* utilitza un controlador d'impressió genèric de cerca i un front-end compatible amb *CUPS* per donar suport a qualsevol tipus d'impressora *raster* des de qualsevol filtre.

La llibreria d'imatges *CUPS* proporciona funcions de manipulació de grans imatges, fent conversions de l'espai de color i una administració del mateix, escalant les imatges a imprimir i administrant els fluxos de pàgines *raster*. Aquesta llibreria s'utilitza pels arxius de filtre d'imatges *CUPS*, pel RIP *PostScript* i tots els controladors d'impressores *raster*.

Un programa *backend* és un filtre especial que envia les dades a imprimir a un dispositiu o una connexió de xarxa. *CUPS 1.1* proveeix backends per als ports paral·lel, sèrie, USB, protocols com LPD, *IPP* i connexions AppSocket (JetDirect).

Les últimes versions de *Samba* inclouen un *backend*, el *smbpool*, que es pot utilitzar amb *CUPS 1.0* o *1.1* per imprimir des de *Windows*.

Aquest *backend* de *samba*, serà el responsable que ens permeti imprimir en una xarxa *Unix-Windows*.

Tradicionalment, la impressió en xarxa ha estat una de les eines més complicades de portar a terme en *Unix*. Una d'aquestes raons és que cada sistema operatiu basat en *Unix* afegeix les seves pròpies extensions al protocol LPD (l'estàndard anterior d'impressió en xarxa) fent la impressió entre plataformes molt complicada, i la impressió en xarxes amb sistemes *Unix-Windows* impossible. Gràcies a *Samba* i *CUPS*, aquesta tasca s'ha facilitat en gran mesura.

Una altra raó dels problemes de la impressió en xarxa a *Unix* era que s'havia d'administrar cada impressora en xarxa des de la màquina client.

CUPS proporciona cerca d'impressores, semblant a la que utilitza *Windows*, el que permet que tots els clients puguin accedir a totes les impressores de la xarxa disponibles, això significa que només es necessita configurar el servidor i automàticament els clients podran veure i utilitzar aquestes impressores.

CUPS també permet associar impressores en xarxa idèntiques en *classes implícites*. Això permet als clients enviar treballs a classes implícites i realitzar la impressió en la primera impressora o classe disponible. També es poden activar de manera molt senzilla funcions de control d'errades i balanceig de càrrega, definint la mateixa impressora o múltiples servidors.

CUPS inclou controladors per a molts tipus d'impressores com *EPSON* o *HP*, el que ens permet que la instal·lació d'aquestes no sigui complicada, amb una interfície molt semblant a la utilitzada per *Windows*.

8. Configuració LDAP

La instal·lació i configuració de *LDAP*, es portarà a terme de tal forma que al finalitzar-la, el sistema sobre el que s'hagi instal·lat hauria d'estar llest per a autenticar usuaris a través del servei de directoris. Aquest és l'objectiu final d'aquest capítol, en següents capítols s'aniran afegint les funcionalitats necessàries per a que es compleixi amb els requisits de treball.

Per l'instal·lació de *OpenLDAP* van agafar des d'un principi la versió 2.1.30, encara que hem durant el transcurs del projecte s'han fet actualització de les noves versions de *LDAP*, a dia d'avui cap versió nova a estat un problema afegit alhora de configurar *LDAP*.

Tota la configuració del nostre servidor *LDAP* està basada en un sistema operatiu *Debian/GNU-Linux*, per tant totes les comandes emprades per la instal·lació i configuració estan basades en aquest sistema.

A continuació veurem quina és la manera d'instal·lar i configurar *LDAP* pel seu correcte funcionament, així com de totes les possibilitats que ens permet afrontar *LDAP*.

8.1. Instal·lació LDAP

El primer pas per instal·lar *OpenLDAP*, és instal·lar els paquets *slapd* i *ldap-utils*. Com hem vist a la part teòrica, *slapd* és un servidor de directori *LDAP* que s'executa en diferents plataformes. Per tal d'instal·lar *slapd*, escriure'm al nostre shell:

```
$ apt-get install slapd
```

Un cop instal·lat el sistema ens mostrarà la pantalla de configuració inicial del paquets *slapd*. Des de aquesta pantalla podrem modificar a nivell bàsic el nostre dimoni *slapd*.

Suposarem que el nostre domini *DNS* o *host* serà *projecte.ldap*, aquest mateix nom ens servirà per referir-nos al nostre domini *LDAP*.

La primera pantalla de configuració ens demanarà el domini sobre el qual executarem el nostre servidor *slapd*, a partir d'ara suposarem que el nostre domini serà *projecte.ldap*.

Un cop hem ficat el nostre domini, ens demanarà el nom de l'organització que està instal·lant *OpenLDAP*, en aquest cas posarem el mateix nom que el nostre domini, *projecte.ldap*.

A continuació vindrà una part important de la configuració de *OpenLDAP*, ens demanarà la clau per al administrador del servei *LDAP*, l'administrador *LDAP* és com una mena de superusuari (*root*) a *OpenLDAP*, així que és molt important escollir una bona clau, un cop hem afegit la clau, ens demanarà tornar a repetir-la per tal de estar segurs de que la clau que hem posat sigui aquella que volíem.

Un cop tenim configurat el nostre administrador *LDAP*, ens demanarà el tipus de *backend* que farem servir per la connexió *LDAP*, ens donarà a escollir entre dues opcions, la opció del *backend* de *Berkeley (BDB)* i el *LDBM*, tots dos han estat explicat als conceptes teòric de *LDAP*. Pel nostre projecte farem servir *LDBM*, entre altres raons degut a que aquest *backend* utilitza una *API* genèrica que permet que sigui compatible en diferents plataformes, en canvi *BDB* no ofereix aquesta característica i a més a més la *API* utilitzada a *Debian* és de molta més complexitat que la de *LDBM*.

Posteriorment ens demanarà si volem fer un *backup* de les possibles dades anteriors que tinguessin al nostre servei de directori *LDAP*, si és la primera vegada que fas l'instal·lació d'aquest dimoni, no et farà falta fer aquest *backup*. En cas contrari, si hem reinstal·lat *slapd* seria una bona idea guardar les dades anteriors per tal de tenir una via d'escapament en cas d'un error greu.

Per finalitzar ens donarà l'opció de permetre a *slapd* mantenir la compatibilitat amb la versió 2 de *LDAP*. En el nostre cas, respondrem negativament a aquesta qüestió, degut a que *LDAP* versió 2 està desfasada i en desús.

Un cop instal·lat *slapd*, haurem d'instal·lar *ldap-utils*, per instal·lar-ho executarem la comanda:

```
$ apt-get install ldap-utils
```

El paquet *ldap-utils* ens dona una sèrie d'utilitats per al paquet *OpenLDAP*. Aquestes utilitats poden accedir local o remotament al servidor *LDAP* i conté tots els programes per tal que el client pugui accedir al servidor *LDAP*. Aquest paquet s'haurà d'instal·lar també a totes les màquines clients.

Un cop efectuada la instal·lació i configuració bàsica dels paquets *slapd* i *ldap-utils*, tindrem un servidor *LDAP* instal·lat i executant-se, encara que aquest no estigui ajustat als objectius que persegueix el nostre projecte. Per tal de comprovar que el dimoni *slapd* s'està executant, farem servir un parell de consultes al sistema. La primera consistirà en veure si el dimoni *slapd* es troba a la llista de processos que actualment s'està executant al sistema, per tal de fer això escriurem a la línia de comandes:

```
$ ps aux | grep slapd
```


La resposta que ens donarà el sistema serà alguna cosa semblant a aquesta:

```
USER  PID %CPU %MEM  VSZ  RSS TTY  STAT  START  TIME  COMMAND
root  4453  0.0  0.5 12144 3004 ?    S    12:52  0:00  /usr/sbin/slapd
root  4455  0.0  0.5 12144 3004 ?    S    12:52  0:00  /usr/sbin/slapd
root  4456  0.0  0.5 12144 3004 ?    S    12:52  0:00  /usr/sbin/slapd
```

Per comprovar finalment que el dimoni està executant-se correctament, procedirem a verificar que estigui escoltant a la xarxa, ja que ha de estar sempre escoltant les peticions que li arribi dels clients. Per tal de comprovar-ho farem ús de la següent instrucció.

```
$ netstat -utap | grep ldap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address  State      PID/Program name
tcp    0      0  *ldap          *.*             LISTEN     4453/slapd
```

Un cop comprovat que el dimoni *slapd* s'està executant al sistema correctament, es verificarà que la connexió amb aquest estigui permesa. Per realitzar això farem servir una comanda que ens ofereix *LDAP*, *ldapsearch*. *ldapsearch* ens permet fer cerques al nostre servei de directori *LDAP*.

ldapsearch obre una connexió a un servidor *LDAP* i realitza una cerca usant els paràmetres especificats a la crida a la funció. Si volem veure tots els paràmetres que podem posar a *ldapsearch* només haurem de veure el manual de *ldapsearch*, executant:

```
$ man ldapsearch
```

Un cop hem après totes les possibles opcions que ens dona *ldapsearch* per tal de fer la cerca dins del nostre servei de directori, utilitzarem la següent comanda per que ens faci una cerca simple als nostre directori *LDAP*.

```
$ldapsearch -x -b " -s base '(objectclass=*)' namingContexts
```

Resultat d'aquesta comanda tindrem per pantalla la següent informació:

```
# extended LDIF
# LDAPv3
# base <> with scope base
# filter: (objectclass=*)
# requesting: namingContexts
dn:
namingContexts: dc=projecte,dc=ldap
# search result
search: 2
result: 0 Success
# numResponses: 2
# numEntries: 1
```

8.2. LDAP

8.2.1. Configuració

En aquest punt donarem els primers retocs inicials a la configuració per defecte de *OpenLDAP*.

Primer de tot modificarem l'arxiu */etc/default/slapd*, en aquest arxiu es configuraran els aspectes relatius a la execució del dimoni *slapd*, tals com paràmetres passat al arrancar, usuari i grup d'execució del dimoni, etc. A continuació anirem desglossant els canvis que tindrà aquest arxiu per adequar-se a la funcionalitat que volem pel nostre projecte.

Per defecte, el dimoni *slapd* s'executa com usuari *root*, cosa que no és recomanable per qüestions de seguretat. Descriurem com podem fer que *slapd* sigui executat per un usuari i grup diferents a *root* i com modificar l'arxiu */etc/default/slapd* per tal de canviar-lo.

Abans de poder executar el dimoni *slapd* amb un usuari i grup específic, s'ha de crear aquest usuari i grup al sistema, en cas de no existir.

El nostre usuari i grup de sistema s'anomenarà "*slapd*". Per tal de crear-lo executarem:

```
$ addgroup --system slapd  
Añadiendo el grupo slapd (133)...  
Hecho.  
$ adduser --home /var/lib/ldap --shell /bin/false --no-create-home --ingroup slapd --system  
adduser: Aviso: El directorio home que usted especificó ya existe.  
Añadiendo usuario del sistema slapd...  
Añadiendo nuevo usuario slapd (126) con grupo slapd.  
No se crea el directorio home.
```

Podem veure que la *home* de l'usuari *slapd* és el directori */var/lib/ldap* que és on tenim emmagatzemada la nostra base de dades *LDAP*.

Abans de continuar amb la següent modificació haurem de aturar el dimoni *slapd*. Per tal d'aturar-lo haurem d'executar al shell:

```
$ /etc/init.d/slapd stop  
Stopping OpenLDAP: slapd.
```

Un cop aturat haurem de canviar el propietari i grup d'alguns arxius i directoris relacionats amb *slapd* amb l'usuari i grup creat anteriorment *slapd*, per a que funcioni amb normalitat. Els canvis s'han de fer als següents directoris així com els arxius que els contenen:

- */etc/ldap*
- */var/lib/slapd*
- */var/lib/ldap*
- */var/run/slapd*

Per fer el canvi de usuari i grup executarem:

```
$ chown -R slapd.slapd /etc/ldap /var/lib/slapd /var/lib/ldap /var/run/slapd
```

Per finalitzar el canvi de propietari i grup haurem de modificar el fitxer */etc/default/slapd* per tal d'indicar-li al dimoni quin és l'usuari i grup amb el qual s'ha d'executar a partir d'ara. Aquesta característica és configura assignant els valors corresponents a les variables *SLAPD_USER* i *SLAPD_GROUP*, i els valors que hem de posar a l'arxiu són els següents:

```
SLAPD_USER="slapd"  
SLAPD_GROUP="slapd"
```

Ara només haurem d'arrancar de nou el dimoni *slapd* per que s'executi amb el nou usuari. Per fer-ho escriurem al shell:

```
$ /etc/init.d/slapd start
```

Per comprovar que el dimoni *slapd* s'executa amb l'usuari i grup creat executarem la funció:

```
$ ps aux | grep slapd
```

Que donarà la següent resposta :

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START TIME	COMMAND
slapd	12728	0.0	0.6	12216	3556	?	S	15:02 0:00	/usr/sbin/slapd -g slapd -u slapd
slapd	12729	0.0	0.6	12216	3556	?	S	15:02 0:00	/usr/sbin/slapd -g slapd -u slapd
slapd	12730	0.0	0.6	12216	3556	?	S	15:02 0:00	/usr/sbin/slapd -g slapd -u slapd

Com podem comprovar al veure els processos en execució *slapd* s'executa amb el nou grup i usuari tal i com indica la línia `-g slapd -u slapd`.

La configuració per defecte del dimoni *slapd* fa que escolti en totes les interfícies de xarxa presents al sistema, aquesta característica no és desitjable, per aquest motiu veurem com podem modificar aquesta situació.

Les especificacions de les interfícies de xarxa, així com el protocol utilitzat en cadascuna d'elles (*ldap*, *ldaps*, *ldapi*) es realitzarà en l'arxiu `/etc/default/slapd` que hem modificat abans. Dintre d'aquest, la variable `SLAPD_SERVICES` posseirà les interfícies a on vulguem que escolti *slapd*. A l'arxiu `/etc/default/slapd` haurem de cercar la variable abans esmentada i afegir:

```
SLAPD_SERVICES="ldap://projecte.ldap:389/ldaps://projecte.ldap:636"
```

L'adreça serà `projecte.ldap` perquè és el nom de domini que varem donar quan varem configurar *slapd* un cop instal·lat.

El protocol *ldap* especifica les interfícies i els ports a on escolten *slapd* amb la característica de que les connexions que s'estableixin no faran ús del xifrat.

El protocol *ldaps* especifica les interfícies i els ports a on escolta *slapd* amb la característica de que les connexions que s'estableixen a la mateixa faran ús del xifrat.

Adicionalment es pot establir un nou protocol de comunicacions, *ldapi*, destinat a les peticions realitzades des de *sockets Unix*. Aquest tipus de protocol no el farem servir en el nostre projecte.

Un cop hem assignat les interfícies necessàries, s'ha de reiniciar el dimoni *slapd* executant la següent funció:

```
$ /etc/init.d/slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: slapd.
```

Per comprovar que el dimoni està escoltant en les interfícies donades, mirarem els processos que corren al sistema, amb la funció *netstat -utap* comprovarem que estigui escoltant les interfícies correctes:

```
$ netstat -utap | grep ldap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 projecte.ldap:ldap *.* LISTEN 12817/slapd
tcp 0 0 projecte.ldap:ldaps *.* LISTEN 12817/slapd
```

Com podem veure *slapd* està escoltant a *ldap* i *ldaps*, les dues interfícies que li hem donat.

Una altra forma per comprovar a quines interfícies escolta *slapd* és amb la comanda *,ps -aux | grep slapd* que ens donarà la següent informació:

```
USER START TIME COMMAND
slapd 15:19 0:00 /usr/sbin/slapd -h ldap://projecte.ldap:389/ldaps://projecte.ldap:636-g slapd -u slapd
slapd 15:19 0:00 \_ /usr/sbin/slapd -h ldap://projecte.ldap:389/ldaps://projecte.ldap:636-g slapd -u slapd
slapd 15:19 0:00 \_ /usr/sbin/slapd -h ldap://projecte.ldap:389/ldaps://projecte.ldap:636-g slapd -u slapd
```

Inicialment *slapd* escoltava al port 389 en totes les interfícies, un cop modificat l'arxiu */etc/default/slapd* i reiniciat el dimoni escolta en les interfícies requerides. Amb els arguments passats a l'arxiu ara especifiquem el *host* on ha d'escoltar i amb quin protocol.

Un cop tenim definit on ha d'escoltar procedirem a modificar l'arxiu de configuració global empleat pels clients *LDAP*. En aquests moments establirem unes opcions inicials, encara que posteriorment anirem modificant aquest arxiu. Aquest arxiu en la majoria dels casos el trobem a */etc/ldap/ldap.conf*

La modificació bàsica que portarem a terme serà posar la informació de on està el nostre servei de directori, així com la base d'aquest i el port on escolta.

Primer haurem de dir-li a la variable *HOST* que es troba a l'arxiu que escolti a *projecte.ldap* que és el nostre domini *LDAP*. Per fer això cercarem l'entrada *HOST* a l'arxiu i la modificarem posant:

HOST projecte.ldap

Seguidament li donarem la informació a l'arxiu del nom distingit per a la base de les cerques, cercarem l'entrada *BASE* a l'arxiu i la modificarem per tal que quedi com:

BASE dc=projecte, dc=ldap

I per finalitzar li direm a quin port ha d'escoltar cercant l'entrada *PORT* a l'arxiu i modificant-la de la següent manera:

port 389

El port 389, és el port estàndard on escolta *ldap*, si utilitzéssim *LDAP* Segur hauríem de canviar aquest port, com ja veurem a la secció *LDAP* Segur.

Finalment haurem de canviar els permisos de l'arxiu */etc/ldap/ldap.conf* per tal que pugui ser llegit per tothom (l'arxiu serà utilitzat per tots els nostres usuaris). Per fer-ho executarem:

\$ chmod 644 /etc/ldap/ldap.conf

També haurem de comprovar que l'arxiu */etc/ldap/slaped.conf* només el propietari tingui permisos de lectura, per fer-ho executarem la comanda:

\$ chmod 600 /etc/ldap/slaped.conf

Un cop fetes aquestes modificacions podem dir que tenim el nostre servei de directoris *LDAP* gairebé llest per tal de autenticar usuaris en *Unix*, però abans haurem d'instal·lar algunes utilitats al client com *ldap_utils*, *pam_ldap* i *nss_ldap*.

ldap_utils ens dona una sèrie d'utilitats per poder accedir remotament al servidor *LDAP* i disposa de tots els programes per a que el client pugui accedir al servidor *LDAP*. Per tal d'instal·lar *ldap_utils* executarem:

```
$ apt-get install ldap_utils
```

ldap_utils no necessita cap tipus de configuració.

pam_ldap permet fer ús d'un servidor *LDAP* per l'autenticació d'usuaris (comprovació de claus) a totes aquelles aplicacions que utilitzem *PAM*.

Suposarem que tots els ordinadors clients de la nostra xarxa utilitzen sistemes operatius *Debian/GNU Linux*, com és el cas de la nostra universitat.

Per tal de fer servir *pam_ldap*, haurem d'instal·lar el paquets *libpam-ldap*, per a fer-ho haurem de executar:

```
$ apt-get install libpam-ldap
```

libpam-ldap ens permet utilitzar el nostre servidor *LDAP* per autenticar usuaris que utilitzin *PAM* si l'utilitzem amb el paquet *libnss-ldap*, aquest últim ens permetrà utilitzar *LDAP* com un servidor de noms.

Un cop instal·lat el paquets per primera vegada ens sortirà la pantalla de configuració de *Debian* per fer una configuració bàsica d'aquest paquets.

Primer de tot ens demanarà el *host* del nostre servidor *LDAP*, seria bo en aquest cas posar l'adreça *IP* del servidor, ja que si posem el nom del domini *LDAP* (en el nostre cas *projecte.ldap*) i tenim un problema amb la resolució de noms, els clients no podran autenticar-se a cap màquina de la xarxa. Si donem la adreça *IP* ens evitarem que pugui aparèixer aquest error.

Posteriorment ens demanarà el nom distingit de la base de les cerques, que ja varem donar al configurar el servidor *LDAP* i al configurar l'arxiu */etc/ldap/ldap.conf*.

Per tant haurem de posar el nom distingit *dc=projecte, dc=ldap*.

Un cop donat el nom distingit ens demanarà quina versió de *LDAP* utilitzarem, i com que el nostre servidor utilitza la versió 3 d'*LDAP*, *pam_ldap* també l'utilitzarà.

Després ens demanarà si les aplicacions que canviïn les claus per medi de *PAM* al client es comportin com si ho fessin localment, aquest cas ens interessa per tal de centralitzar la configuració dels usuaris, llavors respondrem afirmativament.

La següent pantalla de configuració ens demanarà si es necessita autenticar-se per tal d'accedir a la base de dades de *LDAP*, a aquesta pregunta respondrem negativament, ja que això implicaria una pèrdua de temps per l'usuari, ja que cada cop que volgués cercar o autenticar-se al directori *LDAP* hauria de posar la clau adequada per tal de permetre'l accedir. En qüestions de seguretat no implicaria inseguretat al sistema, ja que l'usuari encara que no hagi de autenticar-se per accedir a la base de dades *LDAP*, només podrà llegir les dades, de cap manera podrà modificar-les ni esborrar-les, això és tasca de l'administrador *LDAP* que hem definit anteriorment.

Un cop fet el pas anterior, ens demanarà el compte de l'administrador *LDAP* per tal de poder modificar a la base de dades *LDAP* quan una aplicació canviï claus per mitjà de *PAM*, ja que l'administrador de *LDAP* és l'únic que pot modificar la base de dades i prèviament havíem contestat afirmativament a la opció del comportament local si es canvien les claus per medi de *PAM*, per aquest motiu li respondrem posant:

cn=admin,dc=projecte,dc=ldap

i després ens demanarà la clau de l'administrador dues vegades per tal de comprovar que ha estat ben introduïda.

Per finalitzar la configuració bàsica, ens demanarà el mètode de xifrat de les claus quan siguin modificades per una aplicació *PAM*. Ens donarà a escollir entres les següents opcions:

- *clear* : No té cap xifrat
- *crypt* : És el valor per defecte. Utilitza el mateix xifrat que el sistema.
- *nds*: Utilitza l'estil del *Novell Directory Services*, primer esborra l'antiga clau i després l'actualitza amb un clau sense xifrat.
- *ad* : Utilitza l'estil de l'*Active Directory*, crea una clau *Unicode* i actualitza l'atribut *unicodePwd*
- *exop* : Li diu a *pam_ldap* que utilitzi les claus al mode que permet *OpenLDAP*, per aplicar l'algoritme de hashing especificat a */etc/ldap/slapd.conf*, en comptes de fer hashing localment i escriure el resultat directament dins de la base de dades.

En el nostre cas, escollirem la darrera opció, ja que d'aquestes maneres reduïrem el tràfic a la xarxa.

Tota la configuració de *pam_ldap* la trobem a l'arxiu */etc/pam_ldap.conf*, per posteriors modificacions de *pam_ldap* haurem d'editar l'arxiu, en aquest instant l'arxiu contindrà la informació que li hem donat anteriorment.

Aquest arxiu ha de poder ser llegit per tots els usuaris, per assegurar-nos de que així sigui cert executarem:

```
$chmod 644 /etc/pam_ldap.conf
```

Un cop configurat *pam_ldap*, només ens faltaria fer la configuració dels diferents serveis que utilitza *PAM*, de manera que aquests utilitzin *LDAP* per a la comprovació de la clau. Cada servei que pot fer ús de *PAM* per l'autenticació té el seu propi arxiu al directori */etc/pam.d/*. Per fer que els serveis facin servir *LDAP* en la comprovació de claus s'ha de modificar l'arxiu de configuració de cadascun.

PAM permet configurar el mètode d'autenticació que utilitzaran les aplicacions que facin ús de mateix. Això fa que puguem afegir fàcilment opcions d'autenticació, com pot ser l'autenticació utilitzant una base de dades *LDAP*.

A continuació mostrarem els arxius que s'han de modificar per tal de aconseguir l'autenticació amb *LDAP*.

Fa poc temps el sistema operatiu *Debian* ha canviat la manera de configurar *PAM*. Actualment hi ha seccions comuns a totes les aplicacions que utilitzen *PAM*. Aquestes seccions comuns estan localitzades al directori */etc/pam.d* i estan als arxius que tenen com a prefix *common-*.

S'ha de comprovar si el directori */etc/pam.d* conté aquests arxius. De totes maneres podem configurar totes dues opcions com veurem a continuació.

Els arxius que contenen les seccions comuns a totes les aplicacions que utilitzen *PAM* són els següents:

- */etc/pam.d/common-account* .
- */etc/pam.d/common-auth* .
- */etc/pam.d/common-session* .
- */etc/pam.d/common-password* .

Les modificacions a fer en cadascun dels arxius seran les següents.

L'arxiu *common-account* ha de contenir únicament les següents entrades:

<i>account required</i>	<i>pam_unix.so</i>
<i>account sufficient</i>	<i>pam_ldap.so</i>

L'arxiu `common-auth` ha de contenir únicament les següents entrades:

```
auth sufficient pam_unix.so
auth sufficient pam_ldap.so try_first_pass
auth required pam_env.so
auth required pam_securetty.so
auth required pam_unix_auth.so
auth required pam_warn.so
auth required pam_deny.so
```

L'arxiu `common-session` ha de contenir únicament les següents entrades:

```
session required pam_limits.so
session required pam_unix.so
session optional pam_ldap.so
session required pam_mkhome.so skel=/etc/skel/ umask=0022
```

Volem afegir la opció que un usuari creat a la base de dades *LDAP* pugui crear el seu directori *home* quan s'autentifica per primer cop al nostre servidor. Com que les *homes* dels usuaris seran compartides gràcies a *NFS*, tal com veurem més endavant, un cop creat l'usuari, provarem d'autenticar-nos amb aquest al nostre propi servidor, un cop autenticats el mòdul `pam_mkhome.so` crearà el directori *home*, que posteriorment es compartirà. Per portar a terme aquesta opció utilitzarem la llibreria `pam_mkhome.so` passant-li com a paràmetres on volem posar el *home* d'aquest usuari.

L'arxiu `common-paswd` ha de contenir únicament les següents entrades:

```
password required pam_cracklib.so retry=3 minlen=8 difok=4
password sufficient pam_unix.so use_authok md5 shadow
password sufficient pam_ldap.so use_authok
password required pam_warn.so
password required pam_deny.so
```

En el cas que al nostre sistema no disposem dels arxius *common-*, a la documentació de *pam-ldap* disposem de totes les aplicacions que tenim a */etc/pam.d/* tan sols haurem de copiar aquests arxius al directori abans esmentat.

Ara que ja tenim modificat totes les aplicacions *PAM* per què utilitzin *LDAP*, podem dir que el nostre sistema està preparat per autenticar als usuaris *Unix*. Però abans de fer-ho seria recomanable fer algunes proves amb la nova configuració.

Per portar a terme aquestes proves utilitzarem la comanda *pamtest*.

pamtest accepta dos paràmetres: el primer és el nom del servei al qual es connectarà per a realitzar l'autenticació i el segon el nom d'usuari que s'autenticarà al servei.

pamtest es troba dins de la llibreria *libpam-dotfile*, per tant, si no la tenim disponible la podrem instal·lar executant:

```
$ /usr/bin/apt-get install libpam-dotfile
```

Uns exemples de execució de la comanda *pamtest* amb possibles resultats diferents serien els següents:

```
$ pamtest passwd usuari
```

```
Trying to authenticate <usuari> for service <passwd>.
```

```
Password:[Clau de l'usuari]
```

```
Authentication successful.
```

```
$ pamtest ssh usuari
```

```
Trying to authenticate <usuari> for service <ssh>.
```

```
Password:[Clau fallida de l'usuari]
```

```
Failed to authenticate: Authentication service cannot retrieve authentication info.
```

```
$ pamtest ssh usuari
```

```
Trying to authenticate <usuari> for service <ssh>.
```

```
Password:[Clau de l'usuari]
```

```
Authentication successful.
```

Un cop comprovats tots els serveis que tenim al directori */etc/pam.d* donant una autenticació positiva, ens indicarà que totes les aplicacions *PAM* podran utilitzar *LDAP* correctament.

Un altre dels paquets a instal·lar per tal de dur a terme l'autenticació als clients serà *libnss-ldap*.

Per tal d'instal·lar el paquets *libnss-ldap* executarem:

```
$ apt-get install libnss-ldap
```

Un cop s'instal·la el paquet ens sortirà la ventana de configuració de *Debian*, la configuració del paquet *libnss-ldap* és molt semblant a la de *pam-ldap*.

Primer ens demanarà l'adreça del servidor *LDAP*, com hem dit abans la millor opció seria posar l'adreça *IP* per evitar-nos problemes. Un cop posem l'adreça del servidor *LDAP* ens demanarà el nom distingit de la base de cerca i la versió d'*LDAP* que utilitzarem, posarem *dc=projecte*, *dc=ldap* per la base de cerca i utilitzarem la versió 3 de *LDAP*, tal i com varem posar també a la configuració de *pam-ldap*.

Posteriorment ens demanarà si es necessita autenticar-se per accedir al servidor *LDAP*, a la qual cosa li respondrem negativament.

Després ens donarà l'opció de fer que l'arxiu de configuració de *libnss-ldap* només pugui ser modificat pel seu propietari (fa un *chmod 0600* de l'arxiu de configuració).

Un cop fetes totes les configuracions, haurem terminat d'instal·lar i configurar *libnss-ldap*. Per tal de fer modificacions posteriors, l'arxiu on tenim la configuració de *libnss-ldap* es troba a */etc/libnss-ldap.conf*, aquest arxiu ha de ser accessible en mode lectura per tots el usuaris, per assegurar-nos de que aquest requisit es porta a terme, executarem:

```
$chmod 644 /etc/libnss-ldap.conf.
```

Per tal que el paquet treballi correctament amb *LDAP*, haurem de modificar l'arxiu */etc/nsswitch.conf* per a que utilitzi la base de dades *LDAP*.

L'arxiu */etc/nsswitch.conf* és el fitxer de configuració de la base de dades del sistema i del sistema de commutació dels serveis de noms (*Name Service Switch, nss*). Aquest arxiu ens indica l'ordre i procediment a seguir per a la cerca de la informació requerida, com pot ser la cerca de hosts o usuaris.

La forma de configurar aquest arxiu és molt simple, primer s'ha d'especificar la base de dades subjecta a la cerca, primera columna, a continuació del procediment que s'utilitzarà per a realitzar una cerca sobre aquesta base de dades, darreres columnes.

Llavors només ens farà falta configurar el procediment de cerca per a que faci ús de *LDAP*.

Per fer-ho modificarem l'arxiu */etc/nsswitch.conf*, al qual li afegirem una columna a totes les bases de dades subjectes a la cerca on posi *ldap*, un cop modificat l'arxiu quedaria de la següent forma:

```
passwd:    files ldap
group:     files ldap
shadow:    files ldap
hosts:     files ldap dns
```

La primera columna que conté *passwd*, *group*, *shadow* i *hosts* ens indiquen la base de dades de cerca.

Les següents columnes que contenen *files*, *ldap* i *dns* ens indica el procediment de cerca i el seu ordre, així el procediment de cerca primer mirarà els arxius locals (*files*), després mirarà en el directori *LDAP* (*ldap*) i en el cas de que la base de dades de cerca sigui de hosts, l'últim serà els *dns*.

Com podem veure no s'elimina l'ús del fitxers locals (*files*), ja que alguns usuaris i grups d'usuaris (com pot ser *root*) sempre han de poder autenticar-se localment. Si no posem la columna per a l'ús del fitxers locals, i el nostre servidor *LDAP* cau, cap usuari podria accedir a la màquina fins que torni a estar actiu el servidor *LDAP*. A més, per modificacions locals sempre hem de tenir l'usuari *root*.

La instal·lació del paquet *libnss-ldap* ens dóna a la seva documentació un arxiu d'exemple de com ha de ser modificat */etc/nsswitch.conf* per tal que treballi amb *LDAP*. L'arxiu d'exemple el podem trobar a:

/usr/share/doc/libnss-ldap/examples/nsswitch.ldap.

nss-ldap espera que les comptes siguin objectes amb els seus atributs: *uid*, *uidNumber*, *gidNumber*, *homeDirectory* i *loginShell*. Aquests objectes són permesos per la classe objecte (*objectClass*) *posixAccount*.

Un cop modificat l'arxiu */etc/nsswitch.conf* per tal de comprovar que tot funciona de manera correcta, és a dir, que realitza correctament l'ordre de cerca en les diferents bases de dades del sistema, utilitzarem la comanda *getent* posant com a paràmetre la base de dades de cerca desitjada, com per exemple *getent hosts*. Com a resultat de la comanda ens hauria de mostrar la base de dades consultada per pantalla correctament. En el cas d'executar *getent hosts* ens mostrarà totes les entrades que tenim a l'arxiu */etc/hosts*.

Un cop hem arribat a aquest punt, els sistemes *Unix* ja estaran preparats per autenticar usuaris a través de *LDAP*. Posteriorment veurem les diferents maneres d'afegir usuaris a *LDAP* i com fer que les màquines *Windows* puguin autenticar-se en *LDAP* mitjançant *Samba*

8.3. LDAP Segur

En aquest capítol veurem com crear una unitat certificadora i els certificats necessaris per utilitzar una connexió segura amb *LDAP*. Veurem també com configurar *LDAP* per tal que utilitzi *LDAP* Segur en totes les connexions al nostre servei de directori.

LDAP conté les opcions necessàries per donar suport *SSL/TLS*.

Per tal de poder crear els nostres certificats haurem de tenir instal·lat *OpenSSL*, si el nostre sistema no disposa d'*OpenSSL* el podrem instal·lar fent servir la comanda

```
$ apt-get install openssl
```

8.3.1. Creació certificats

Per habilitar les connexions *SSL/TLS* cap al servidor, es necessita la presència d'un certificat al servidor per part dels protocols *SSL/TLS*. A més, al establir una connexió *SSL*, el certificat del servidor només proporciona una connexió segura i xifrada al servidor. Si es desitja autenticar al client, s'ha de donar al servidor *LDAP* el certificat i la clau del client.

Hi ha dues maneres de crear i instal·lar un certificat al servidor, tots dos mètodes necessiten la creació d'un certificat per al servidor, enviar-li als clients *LDAP* i realitzar els canvis apropiats als arxius de configuració *LDAP*. Tots dos necessiten l'ús de comandes *OpenSSL* que sol·licitaran informació per la creació del certificat. Les dues maneres de crear el certificat són ,crear un certificat autosignat o crear un certificat emès per una entitat certificadora de confiança. En el nostre cas crearem una entitat certificadora de confiança i l'utilitzarem per crear els certificats.

Per a la creació del nostre certificat haurem de crear una carpeta al directori */var/myca* a on desarem els certificats.

Per la creació de la nostra entitat certificador executarem l'script que ens dona *OpenSSL CA.sh*, si a aquest script li passem com a paràmetre l'opció *-newca* tal i com veiem a continuació:

```
$ /var/myca/CA.sh -newca
```

Un cop executada la comanda ens demanarà certa informació per la creació de l'entitat certificadora, entre la qual trobem les inicials del país, la província, el nom de la nostra organització, el nom comú i l'e-mail.

```
CA certificate filename (or enter to create)
Making CA certificate ...
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Barcelona
Locality Name (eg, city) []:projecte.ldap
Organization Name (eg, company) [Internet Widgits Pty Ltd]:projecte.ldap
Organizational Unit Name (eg, section) []:projecte.ldap
Common Name (eg, YOUR name) []:projecte.ldap
Email Address []:
```

El següent pas serà crear el certificat i la clau privada del servidor, per fer-ho haurem d'utilitzar la comanda següent:

```
$ openssl req -new -nodes -keyout newreq.pem -out newreq.pem
```

L'argument `-nodes` ens crea la clau sense xifrat, ja que `LDAP` només treballa amb claus privades no xifrades.

Un cop executada la comanda ens demanarà certa informació per la creació de certificat, entre la qual trobem les inicials del país, la província, el nom de la nostra organització, el nom comú i l'e-mail. És molt important posar com a nom comú, el nom del domini del nostre servidor (en el nostre cas `projecte.ldap`) ja que si no posem això provocarà errors alhora de fer ús del certificat del servidor.

```
Generating a 1024 bit RSA private key
```

```
...+++++
```

```
.....+++++
```

```
writing new private key to 'newreq.pem'
```

```
----
```

```
You are about to be asked to enter information that will be incorporated  
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
----
```

```
Country Name (2 letter code) [AU]:ES
```

```
State or Province Name (full name) [Some-State]:Barcelona
```

```
Locality Name (eg, city) []:Barcelona
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:projecte.ldap
```

```
Organizational Unit Name (eg, section) []:projecte.ldap
```

```
Common Name (eg, YOUR name) []:projecte.ldap
```

```
Email Address []:projecte@ldap.com
```

```
Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
```

```
A challenge password []:[Clau]
```

```
An optional company name []:
```

Un cop creat el certificat, la nostra entitat certificadora de confiança l'haurà de signar, per fer-ho farem servir l'script *CA.sh* utilitzat anteriorment però amb el paràmetre *-sign*.

La sortida que ens donarà aquesta comanda serà la següent:

```
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 1 (0x1)
  Validity
    Not Before: Jun 29 14:07:32 2005 GMT
    Not After : Jun 29 14:07:32 2006 GMT
  Subject:
    countryName           = ES
    stateOrProvinceName  = Barcelona
    localityName         = Barcelona
    organizationName     = projecte.Idap
    organizationalUnitName = projecte.Idap
    commonName           = projecte.Idap
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      BD:F6:94:41:DF:97:AA:2A:0E:01:71:34:0F:D8:BC:25:CE:53:FC:FF
    X509v3 Authority Key Identifier:
      keyid:23:33:25:21:26:9C:54:C7:79:48:42:E9:35:46:46:A2:DE:05:C0:21
  DirName:/C=ES/ST=Barcelona/L=projecte.Idap/O=projecte.Idap/OU=projecte.Idap/CN=projecte.Idap
    serial:D5:52:D0:1F:3C:FE:24:B9
Certificate is to be certified until Jun 29 14:07:32 2006 GMT (365 days)
Sign the certificate? [y/n]:y
(.....)
Signed certificate is in newcert.pem
```

Un cop realitzada l'operació ja tenim els certificats i claus necessàries , ara només quedarà configurar *LDAP* per a que utilitzi aquests certificats i claus.

Per tal de encapsular tota la informació, mourem els certificats a dins de la carpeta */etc/ldap/ssl* i canviarem el nom dels certificats i claus per major enteniment.

El primer pas serà copiar els certificats al directori */etc/ldap/ssl*. En el cas que no estigui creat el directori el crearem amb la funció:

```
$ mkdir /etc/ldap/ssl
```

Posteriorment copiarem l'arxiu *cacert.pem* de la nostra entitat certificadora, a dins del directori */etc/ldap/ssl* executant:

```
$ cp /var/myca/cacert.pem /etc/ldap/ssl
```

i mourem i renombrarem el certificat i la clau privada creada fent servir la següent comanda:

```
$ mv /var/myca/newcert.pem /etc/ldap/ssl/servercert.pem
```

```
$ mv /var/myca/newreq.pem /etc/ldap/ssl/serverkey.pem
```

La clau privada només ha de poder ser llegida per l'usuari que executa el dimoni *slapd*, en canvi el certificat ha de ser poder ser llegit per tots els usuaris, per fer-ho utilitzarem la comanda:

```
$chown slapd.slapd /etc/ldap/ssl/serverkey.pem
```

Un cop fet això ja tindrem els certificats i claus disposats perquè *LDAP* els utilitzi, només queda configurar els diferents arxius de configuració de *LDAP* per tal que utilitzi els certificats alhora de autenticar als usuaris.

8.3.2. Configuració

Amb la configuració prèviament feta de *LDAP*, en aquests moments només ens farà falta afegir un parell de línies i modificar tantes altres als arxius de configuració de *OpenLDAP*.

A l'arxiu de configuració del dimoni *slapd* haurem d'afegir les següents entrades per tal que *slapd* faci ús dels certificats *SSL*.

```
TLSCipherSuite HIGH:MEDIUM:+SSLv2  
TLSCACertificateFile /etc/ldap/ssl/cacert.pem  
TLSCACertificatePath /etc/ldap/ssl/  
TLSCertificateFile /etc/ldap/ssl/servercrt.pem  
TLSCertificateKeyFile /etc/ldap/ssl/serverkey.pem  
TLSVerifyClient Demand
```

Com podem veure amb aquestes línies li estem dient a *slapd* on es troben els certificats, les claus i que ha de verificar al client sempre.

Com al configurar *LDAP* de forma no segura havíem incorporat a l'arxiu de configuració */etc/default/slapd*, que el dimoni *slapd* escoltés també a la interfície que utilitza *LDAP* en mode segur: *ldaps://projecte.ldap*, no farà falta tocar res.

En canvi, sí que haurem de modificar l'arxiu */etc/ldap/ldap.conf*, necessari pels clients *LDAP* per tal de dir-li que utilitzi els certificats creats, per fer-ho editarem l'arxiu i afegirem les línies següents:

```
PORT 636  
ssl yes  
TLS_CACER /etc/ldap/ssl/cacert.pem  
TLS_KEY /etc/ldap/ssl/serverkey.pem  
TLS_REQCERT never
```

Li indiquem a l'arxiu de configuració on tenim el certificats i les claus, que ha d'escoltar pel port 636 dedicat a les connexions segures a *LDAP* i que faci ús de *SSL*, no volem que el client verifiqui el servidor, sinó que el servidor verifiqui que el client sigui segur. Per això li passem el paràmetre *never* (mai) a la línia *TLS_REQCERT*.

Com hem vist al capítol anterior, les aplicacions que necessiten *PAM* per autenticar-se han de fer-ho mitjançant *LDAP*, llavors, al canviar a format segur, ens farà falta modificar l'arxiu de configuració de *PAM* */etc/pam_ldap.conf* i */etc/libnss_ldap*.

A tots dos haurem fer les mateixes modificacions, i s'ha de posar tant a l'un com l'altre les següents línies:

```
port 636
ssl on
tls_cacertfile /etc/ldap/ssl/cacert.pem
tls_ciphers HIGH:MEDIUM:+SSLv2
tls_cert /etc/ldap/ssl/servercert.pem
tls_key /etc/ldap/ssl/serverkey.pem
```

Com podem veure els valors són molts semblants als utilitzats a l'arxiu */etc/ldap/ldap.conf*. Li diem on ha d'escoltar i els certificats a utilitzar.

Per tal de comprovar la bona funcionalitat del nostre servidor *LDAP* en mode segur, podem executar una cerca bàsica indicant-li la interfície on ha d'escoltar, per fer-ho escriurem a la shell:

```
$ ldapsearch -x -b " -s base '(objectclass=*)' namingContexts -H ldaps://projecte.ldap
```

Si la sortida d'aquesta execució no ens dona cap error, voldrà dir que tenim el nostre servidor *LDAP* Segur funcionant i actiu per l'autenticació d'usuaris.

8.4. Eines de migració clients Linux a LDAP

Si volem implementar *LDAP* a una xarxa on tenim configurat *NIS* i els usuaris existents haurien d'estar a la nova implementació de xarxa amb el servei de directori *LDAP*, trobem un conjunt d'eines desenvolupades per *PADL Software* que ens permet fer la migració d'usuaris. Aquest conjunt d'eines s'anomenen *MigrationTools*.

Les *MigrationTools* són una sèrie d'*scripts* en llenguatge *Perl* que ens permet migrar usuaris, grups, alies, hosts, protocols, *RPCs* i serveis de *NIS* a *LDAP*.

Aquestes eines necessiten de les comandes *ldapadd* i *ldif2dbm* que són distribuïdes amb *OpenLDAP* per funcionar, ja que l'execució dels *scripts* per la migració ens retorna un arxiu *LDIF* amb la informació requerida, aquests arxius es poden afegir al directori *LDAP* mitjançant la comanda *ldapadd*. Els *scripts* més importants que disposem al paquet *MigrationTools* són els següents:

- *migrate_base.pl* : Crea la base de cerca *LDAP* a partir del sistema anterior.
- *migrate_aliases.pl* : Exporta els alies que trobem a l'arxiu */etc/aliases* a *LDAP*.
- *migrate_group.pl* : Exporta els grups que tenim a l'arxiu */etc/group* a *LDAP*.
- *migrate_hosts.pl* : Exporta els hosts que tenim a l'arxiu */etc/hosts* a *LDAP*.
- *migrate_networks.pl* : Exporta la informació que tenim a l'arxiu */etc/network*.
- *migrate_passwd.pl* : Exporta els usuaris que tenim al fitxer */etc/passwd*.
- *migrate_protocols.pl* : Exporta els protocols que tenim al fitxer */etc/protocol*.
- *migrate_services.pl* : Exporta els serveis que tenim al fitxer */etc/services*.
- *migrate_netgroup.pl* : Exporta els netgroup que tenim a */etc/netgroup*.
- *migrate_rpc.pl* : Exporta els *RPCs* que trobem a */etc/rpc*.

Per tal d'instal·lar les *MigrationTools*, descarregarem el paquet de la pàgina web del fabricant <http://www.padl.com/download/MigrationTools.tgz>.

Un cop descarregat el paquet haurem de descomprimir-lo, per fer-ho executarem al nostre shell:

```
$ tar -xzf MigrationTools.tgz /etc/
```

Un cop descomprimit accedim al directori creat a l'hora de descomprimir el paquet per tal de procedir a la configuració de les eines.

Editarem l'arxiu de configuració de *MigrationTools* *migrate_common.ph*, dins del arxiu haurem de modificar les següents línies:

```
$DEFAULT_MAIL_DOMAIN= "projecte.ldap"  
$DEFAULT_BASE = "dc=projecte, dc=ldap"
```

La línia *\$DEFAULT_MAIL_DOMAIN* ens indica el domini de correu electrònic utilitzat per l'atribut mail a l'arxiu *migrate_passwd.pl*. Encara i que no tenim domini de correu electrònic haurem de posar-ho ja que pot donar errors a l'hora de migrar els usuaris.

La línia *\$DEFAULT_BASE* ens indica la base de cerca d'*OpenLDAP* que faran servir les eines *MigrationTools* per tal de realitzar la migració.

Un cop definit l'arxiu de configuració ja podem utilitzar el conjunt d'eines. Uns exemples de com utilitzar aquestes eines els tenim a continuació:

```
$/etc/MigrationTools-46/migration_passwd.pl /etc/passwd passwd.ldif  
$/etc/MigrationTools-46/migration_group.pl /etc/group group.ldif
```

Com podem veure l'execució dels *scripts* de migració ens demana l'arxiu a migrar i el nom de l'arxiu *LDIF* resultant. Un cop finalitzat el procés de migració, mitjançant l'arxiu *LDIF* i la comanda *ldapadd* podrem afegir al nostre servei de directori la informació que conté aquest arxiu. Per afegir el fitxer *LDIF* utilitzarem la comanda:

```
$ ldapadd -x -D 'dc=projecte,dc=ldap' -w -F /etc/MigrationTools-46/passwd.ldif
```

```
$ ldapadd -x -D 'dc=projecte,dc=ldap' -w -F /etc/MigrationTools-46/group.ldif
```

Amb aquestes senzilles operacions podem traspasar grans quantitats d'informació d'un servidor de nom *NIS* a *LDAP*, sense la important pèrdua de temps que comportaria crear-los tots de nou.

8.5. Compartir directori personal home

Per tal de compartir la *home* dels nostres usuaris a altres màquines *Unix*, utilitzarem *NFS* (*Network File System*), tal com hem explicat anteriorment *NFS* va ser desenvolupat per permetre muntar una partició que pertanyi a una màquina remota com si en fos local. Ens proporciona, per tant, un mètode ràpid i eficaç de compartir arxius i espai de disc entre diferents ordinadors d'una xarxa que suportin aquest sistema.

Per tal de configurar *NFS* perquè ens permeti compartir les *homes* dels usuaris, haurem de tenir instal·lat *portmap* i el paquet *nfs-utils*, que el podem trobar a la majoria de distribucions, a l'ordinador que faci de servidor de disc (en el nostre cas, serà l'ordinador on tenim el nostre directori *LDAP*).

portmap ens permetrà realitzar connexions *RPC* (*Remote Procedure Call*) al servidor i és l'encarregat de permetre o no l'accés al servidor als equips que especifiquem.

Per saber si tenim el *portmap* instal·lat executarem la comanda:

```
$ ps aux | grep portmap
```

Que ens hauria donar una sortida semblant a la següent:

```
rpc 1261 0.0 0.1 1560 568 ? S 15:48 0:00 portmap
```

Per saber si *NFS* està en marxa a la nostre màquina farem una consulta a *portmap* per què ens indiqui quins serveis té en marxa.

Per fer-ho durem executar la comanda:

```
$ rpcinfo -p
```

Que donarà una sortida semblant a la següent:

```
programa vers proto puerto
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
```

Com podem veure, *NFS* està posat en marxa, ja que *portmap* proporciona el seu servei. Haurem de verificar quan instal·lem per primer cop que *portmap* proporciona el servei *NFS*, ja que en cas contrari, és normalment a causa de que el paquet *nfs-utils* no es troba instal·lat al sistema.

Un cop tenim el serveis en marxa només ens quedarà determinar quins fitxers hem de compartir. En el nostre cas, haurem de compartir la carpeta */home*. Per fer-ho haurem d'editar el fitxer */etc/exports* i introduir la següent línia.

```
/home/ XXX.XXX.XXX.0/255.255.255.0 (rw)
```

Amb aquesta línia li estem indicant a *NFS* que volem exportar el directori */home/* del nostre servidor al nostre rang de adreces locals en mode lectura/escriptura, els usuaris han de poder escriure a la seva *home* des de qualsevol màquina. En cas que fos necessari també podem indicar-li que només exporti a una sola màquina, o en mode de només lectura.

Per tal de donar una mica més de seguretat és recomanable editar els fitxers */etc/hosts.allow* i */etc/hosts.deny* per a acabar d'especificar quins ordinadors de la xarxa poden fer ús dels serveis del servidor. La documentació de *NFS* recomana les següents entrades:

```
/etc/hosts.deny
portmap:ALL
lockd:ALL
mountd:ALL
rquotad:ALL
statd:ALL
```

/etc/hosts.allow

portmap:XXX.XXX.XXX.0/255.255.255.0

lockd:XXX.XXX.XXX.0/255.255.255.0

mountd:XXX.XXX.XXX.0/255.255.255.0

rquotad:XXX.XXX.XXX.0/255.255.255.0

statd:XXX.XXX.XXX.0/255.255.255.0

Podem afinar més la seguretat si diem a cada servei quina *IP* específica pot fer ús d'aquest. En el nostre cas, dient-li el rang d'*IPs* ens anirà bé.

Un cop finalitzada la configuració de *NFS* perquè exporti les *homes* dels usuaris, haurem reiniciar el dimoni *nfsd* per tal que rellegeixi el fitxer */etc/exports* per tal d'activar els canvis fets a l'arxiu. També podem executar la següent comanda per activar els canvis:

\$ exportfs - ra

Un cop tenim el servidor de discs funcionant correctament, veurem com accedir des de un ordinador client. Per tal de fer-ho haurem d'autenticar-nos com a usuari *root* a la màquina client, per tal de poder accedir als fitxers compartits utilitzarem la comanda:

\$ mount <servidor>:<directori compartit> <punt de muntatge>

El nostre servidor és la màquina *XXX.XXX.XXX* o *projecte.ldap*, el directori compartit és */home* i el punt de muntatge a la màquina serà la carpeta */home* per tal que la compartició sigui del tot transparent.

Així bastarà amb executar la següent comanda per poder accedir al nostre directori compartit:

\$ mount projecte.ldap:/home /home

Per tal de comprovar que hem exportat adequadament el directori */home* del nostre servidor *LDAP*, bastarà amb fer un `ls -la /home`, i ens sortiran totes les *homes* dels usuaris que tenim al nostre directori *LDAP*. Com encara no en tenim cap d'usuari creat podem crear un fitxer a la carpeta *home* i fixar-nos que des de la màquina client també estigui.

Per tal d'automatitzar el muntatge per a que cada cop que iniciem la màquina client els sistema de fitxers compartit al servidor sigui muntat, haurem de afegir la següent informació a la màquina client:

```
XXX.XXX.XXX.XXX:/home /home nfs rw,hard,intr 0 0
```

On *XXX.XXX.XXX.XXX* és el servidor *NFS*, */home* és el directori compartit i */home* és el punt de muntatge.

Amb totes aquestes modificacions, ja podem fer que un usuari que s'autentifiqui a una màquina *Unix* sobre el nostre servei de directori *LDAP*, faci ús del *home* que aquest usuari té al servidor *LDAP* gràcies al *NFS* (*Network File System*)

8.6. Problemes

A l'hora de configurar *LDAP* hem d'anar molt en compte amb totes les modificacions que fem als arxius de configuració. És molt recomanable reiniciar el dimoni *slapd* cada cop que fem una modificació important, ja que si intentem modificar tot de cop i ens dona un error, no sabrem on començar a buscar. Un dels possibles errors que podem cometre és canviar l'usuari d'execució del nostre dimoni *slapd* i no canviar les entrades de l'arxiu de configuració */etc/default/slapd* *SLAPD_USER* i *SLAPD_GROUP*, si no posem a aquestes entrades l'usuari correcte d'execució de *slapd*, el nostre dimoni *slapd* mai s'executarà i ni tan sols executant-ho amb mode depuració ens donarà una pista per saber a on es troba l'error. I si hem modificat moltes entrades a l'arxiu de configuració abans de reiniciar el nostre dimoni, lo més probable és que haurem de tornar a començar des del principi per tal de veure on trobem l'error.

Si cada cop que modifiquem els arxius de configuració reiniciem el domini, podem tornar enrere ja que sabem exactament a quin punt el dimoni funcionava correctament.

Un altre tipus d'error ens pot vindre al executar la comanda *ldapsearch*, que la sortida donada per la comanda ens doni un error. *ldapsearch* disposa d'un mode depuració, si li passem l'argument *-d -1* *ldapsearch* s'executarà en mode depuració total, per donar-nos més facilitats alhora de veure els possibles errors. A continuació veurem un exemple de com arribar a solucionar aquets tipus d'errors i la causa d'aquest.

Suposem que la sortida de la nostra consulta *ldapsearch* en mode depuració sigui la següent:

```
$ ldapsearch -d -1 -x -b " -s base '(objectclass=*)' namingContexts  
ldap_create  
ldap_bind_s  
ldap_simple_bind_s  
ldap_sasl_bind_s  
ldap_sasl_bind  
ldap_send_initial_request
```

```

ldap_new_connection
ldap_int_open_connection
ldap_connect_to_host: TCP projecte.ldap:389
ldap_new_socket: 3
ldap_prepare_socket: 3
ldap_connect_to_host: Trying XXX.XXX.XXX.XXX:389
ldap_connect_timeout: fd: 3 tm: -1 async: 0
ldap_ndelay_on: 3
ldap_is_sock_ready: 3
ldap_ndelay_off: 3
ldap_int_sasl_open: host=projecte.ldap
ldap_open_defconn: successful
ldap_send_server_request
ber_flush: 14 bytes to sd 3
  0000: 30 0c 02 01 01 60 07 02 01 03 04 00 80 00      0....`.....
ldap_write: want=14, written=14
  0000: 30 0c 02 01 01 60 07 02 01 03 04 00 80 00      0....`.....
ldap_result msgid 1
ldap_chkResponseList for msgid=1, all=1
ldap_chkResponseList returns NULL
wait4msg (infinite timeout), msgid 1
wait4msg continue, msgid 1, all 1
** Connections:
* host: projecte.ldap port: 389 (default)
  refcnt: 2 status: Connected
  last used: Tue Mar 9 16:18:26 2005
** Outstanding Requests:
* msgid 1, origid 1, status InProgress
  outstanding referrals 0, parent count 0
** Response Queue:
  Empty
ldap_chkResponseList for msgid=1, all=1
ldap_chkResponseList returns NULL
ldap_int_select
read1msg: msgid 1, all 1
ber_get_next
ldap_read: want=8, got=0
ber_get_next failed.
ldap_perror
ldap_bind: Can't contact LDAP server (81)

```


Si anem reseguint la informació que ens dona *ldapsearch*, veurem que el *host* amb qui establim la connexió és correcte (*ldap_connect_to_host: TCP projecte.ldap:389*) i que es connecta satisfactoriament al mateix (*ldap_open_defconn: successful*), però just en aquest moment és quan començem a tenir errors.

Podem comprovar que la informació que ens dona no ens permet aclarir quina pot ser exactament la causa de l'error que tenim. Però el dimoni *slapd* és pot executar en diferents nivells de depuració per tal de veure molt millor que està passant.

Els nivells de depuració que conté *slapd* són els següents:

Nivell	Descripció
-1	Habilita tota la depuració
0	Sense depuració
1	Rastreja las trucades a funcions
2	Depura el manegament de paquets
4	Rastreig de depuració intensiu
8	Administració de la connexió
16	Mostra els paquets enviats i rebuts
32	Processat de cerca per filtre
64	Processat de l'arxiu de configuració
128	Processat de la llista de control d'accés
256	<i>stats log connections/operations/results</i>
512	<i>stats log entries sent</i>
1024	Mostra les comunicacions amb els backends de la shell
2048	Mostra les entrades analitzades (<i>parsing</i>)

slapd te moltes opcions alhora d'executar-se si veiem el manual de *slapd* (*man slapd*, al nostre *shell*) podem veure aquestes opcions d'execució:

Per tal de fer que *slapd* s'executi en mode depuració haurem de escriure aquesta opció a la nostre shell:

```
$ slapd -d -1 -h ldap://projecte.ldap:389/
```

Com hem vist anteriorment, la opció “-d” li diu a *slapd* que s'ha d'executar-se de forma segura i l'opció *-1* ens diu el nivell de depuració en aquest cas habilita totes les depuracions.

Ara ja tenim el nostre servidor *slapd* en mode depuració de tal forma que si ara executem la cerca anterior amb *ldapsearch* que ens havia donat problemes, *slapd* ens donarà la següent resposta:

```
daemon: activity on 1 descriptors
daemon: new connection on 9
fd=9 DENIED from unknown (XXX.XXX.XXX.XXX)
daemon: closing 9
daemon: activity on:
daemon: select: listen=6 active_threads=0 tvp=NULL
```

Podem veure que dona un error de *DENIED from unknown* i la *IP* que es connecta al servidor *LDAP*. Això ens pot donar una pista de perquè pot ser degut.

Les opcions de configuració per defecte de *OpenLDAP* a *Debian GNU/Linux* habilita el suport dels *TCP Wrappers*. Si tenim una configuració restrictiva dels *TCP Wrappers*, pot ser que aquesta sigui la causa dels problemes de connexions. Haurem de fixar-nos als fitxers */etc/hosts* */etc/hosts.allow* i */etc/hosts.deny*. En el nostre cas, si posem la *IP*, o el rang d'*IPs* adequat al */etc/hosts.allow* ens permetrà corregir aquest error i que *slapd* s'executi de forma correcta.

Un cop la hem posada i tornem a executar *slapd* en mode depuració veurem aquesta informació:

```

daemon: activity on 1 descriptors
daemon: new connection on 9
conn=2 fd=9 ACCEPT from IP=XXX.XXX.XXX.XXX:32852 (IP=XXX.XXX.XXX.XXX:389)
daemon: added 9r
daemon: activity on:
daemon: select: listen=6 active_threads=0 tvp=NULL
connection_read(9): checking for input on id=2
ber_get_next
(...)
=> access_allowed: read access granted by read(=rscx)
ber_get_next on fd 9 failed errno=0 (Success)
do_unbind
(...)

conn=2 op=2 UNBIND
connection_resched: attempting closing conn=2 sd=9
connection_close: conn=2 sd=9
daemon: removing 9
conn=2 fd=9 closed
daemon: select: listen=6 active_threads=0 tvp=NULL
daemon: activity on 1 descriptors
daemon: select: listen=6 active_threads=0 tvp=NULL

```

Com podem veure, ara si que tenim un connexió correcta ja que s'ha acceptat la mateixa.

Un altre error comú, però en aquest cas a l'hora de posar en marxa el nostre servidor de forma segura, consisteix en la creació del seu certificat, al crear el certificat amb la comanda :

```
$ openssl req -new -nodes -keyout newreq.pem -out newreq.pem
```

o al executar l'script `CA.sh -newca`

Al executar aquestes comandes ens demanarà una certa informació que li hem de passar manualment. Hi ha una entrada que ens demanarà el *Common Name*, hem de teclejar el nom del domini del nostre servidor, en el nostre cas *projecte.ldap* i no el nostre nom con suggereix *OpenSSL*, el no posar el nom del nostre domini comportarà errors a l'hora de fer servir el certificat.

També tindrem problemes a l'hora de configurar el nostre servidor *LDAP* de forma segura, si quan configurem els arxius de configuració */etc/ldap/ldap.conf*, tant als clients com al servidor, li marquem com a *demand* l'entrada *TLS_REQCERT*.

Si reiniciem el dimoni *slapd* amb aquesta configuració, es quedarà en un bucle i mai s'engegarà, degut a que tenim configurat el nostre servidor *LDAP* de forma segura de tal forma que els clients han de autenticar que són qui diuen ser al servidor, i no a la inversa. La solució resideix a modificar l'entrada de l'arxiu de configuració */etc/ldap/ldap.conf* i posar *TLS_REQCERT never*.

9. Configuració Samba

El nostre servidor *Samba* s'instal·larà i configurarà per actuar com a *PDC* (*Primary Domain Controller*) de la nostra xarxa. La informació dels comptes de usuaris s'emmagatzemaran al directori *LDAP* que ja havíem configurat prèviament, i entre altres coses ens donarà serveis d'impressió i perfils mòbils.

A continuació veurem com realitzar aquesta configuració i com donar suport, en l'estructura *LDAP*, per emmagatzemar les dades relatives a comptes d'usuaris *Samba*.

Un cop afegida aquesta estructura al directori *LDAP*, els usuaris que s'emmagatzemin tindran la possibilitat d'autenticar-se en qualsevol sistema *GNU/Linux* i/o *Windows* que faci ús de *LDAP* per realitzar aquesta autenticació. La particularitat serà que tindran el mateix tipus de compte d'accés per a tots els sistemes, tant a *GNU/Linux* com *Windows*, a tota la xarxa.

L'última actualització de *Samba* ens va instal·lar la versió 3.0.14a del paquet.

9.1. Instal·lació

Hem de diferenciar la instal·lació d'un servidor *Samba* de la d'un client. Posteriorment veurem com instal·lar un i l'altre, així com comprovar que tot funcioni correctament.

En moltes ocasions un mateix ordinador pot actuar com a client i servidor *Samba*. El servidor *Samba* serà aquell sistema que doni serveis tals com l'autenticació, compartició d'arxius i unitats, i el client serà aquell que els faci servir, accés als recursos compartits, autenticació...

El paquet principal del servidor *Samba* és *samba*, per tal d'instal·lar-ho haurem d'executar la següent comanda:

```
$ apt-get install samba
```

El paquet *samba* depèn del paquet *samba-common*, que s'instal·larà automàticament al executar la instrucció anterior.

Un cop hem s'ha fet la instal·lació ens sortirà la pantalla de configuració de *Debian*. El primer pas que ens demanarà serà el nom del nostre domini o grup de treball, en el nostre cas el nom serà *PROJECTE*.

La següent pantalla de configuració ens donarà a escollir la forma en la qual volem que s'executi *Samba*, amb *dimonis* o *inetd*. Escollirem la opció dels *dimonis*, ja que aquesta, dins d'un entorn on l'ús de *Samba* sigui freqüent, com és el cas de les aules de la nostra universitat, és molt més eficient que utilitzar un superservidor *inetd*.

A continuació ens demanarà l'opció de crear un arxiu destinat a emmagatzemar les claus d'usuaris *Samba*. Per tal de mantenir la compatibilitat amb el comportament de per defecte de la majoria de sistemes *Windows*, *Samba* s'ha de configurar per a que utilitzi claus xifrades, la qual cosa ens obliga a crear un fitxer diferent del */etc/passwd* per emmagatzemar les claus. El fitxer és creat automàticament en cas de confirmar aquesta configuració, però les claus s'hauran d'introduir manualment mitjançant la comanda *smbpasswd* que veurem més endavant.

Com volem mantenir aquesta compatibilitat, respondrem afirmativament a l'opció de crear l'arxiu de claus. Aquest és creat a */var/lib/samba/passdb.tdb*.

La següent pantalla de configuració ens dona l'opció de utilitzar claus xifrades. Els clients *Windows* més moderns es comuniquen amb els servidors *Samba* utilitzant claus xifrades. Si volem utilitzar claus en text pla, haurem de canviar un paràmetre al registre de *Windows*. És molt recomanable utilitzar claus xifrades, per tant aquesta serà la nostra opció, però haurem de comprovar que tenim un fitxer */etc/smb/smbpasswd* vàlid i que les claus que té el fitxer han estat afegides mitjançant el programa *smbpasswd*.

Per finalitzar la configuració del paquet *samba*, ens donarà l'opció d'utilitzar *DHCP* per a configurar *WINS*, en el cas del nostre projecte i de la universitat, les *IP* seran donades per un servidor *DHCP* de la xarxa. Per tant respondrem afirmativament a aquesta qüestió.

Un cop realitzada la configuració inicial del paquet *samba* ja tindrem instal·lat i configurat el nostre servidor *Samba*, encara que no contempla totes les necessitats de la nostra xarxa, això ho veurem més endavant.

En aquest moment estem en condicions de instal·lar els paquets idonis pels clients *Samba*. Els clients *Samba* tindran com a base els paquets *smbclient* i *smbfs*.

La instal·lació de *smbclient* i *smbfs* no ens donarà cap opció de configuració, els paquets ens instal·larà diverses eines. Per tal de veure les eines instal·lades podem executar:

```
$ dpkg -L smbclient | grep bin  
$ dpkg -L smbfs | grep bin
```

Amb la següent resposta:

```
/usr/bin/smbclient  
/usr/bin/smbtar  
/usr/bin/rpcclient  
/usr/bin/smbspool  
/usr/bin/smbtree  
/usr/bin/smbcacls  
/usr/bin/smbcquotas  
/usr/bin/smbmount  
/usr/bin/sbumount  
/usr/bin/smbmnt  
/sbin/mount.smbfs  
/sbin/mount.smb
```

smbclient i *smbfs* s'utilitzaran per a clients *Unix* a *Samba*, més endavant veurem les utilitats d'aquestes eines.

9.2. Configuració Samba-LDAP

Abans de continuar amb la configuració de *Samba*, haurem de realitzar diverses modificacions a la configuració de *OpenLDAP*, de tal forma que estigui preparat per tal de suportar les característiques de *Samba*.

El primer pas que hem de realitzar és copiar l'esquema de samba al directori d'esquemes d'*OpenLDAP*. L'arxiu d'esquemes per a *Samba* es troba al paquet *samba-doc*, en el cas que no estigui instal·lat al nostre sistema, podem instal·lar el paquet executant:

```
$ apt-get install samba-doc
```

El directori d'esquemes d'*OpenLDAP* es troba a */etc/ldap/schema/* i l'esquema samba el podem trobar a la documentació de samba que tenim al paquet *samba-doc*.

El directori on es troba l'esquema samba que utilitzarà *LDAP* és */usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz*.

Per copiar l'esquema al directori d'esquemes executarem:

```
$ cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema  
$ gunzip /etc/ldap/schema/samba.schema.gz  
$ chown slapd.slapd /etc/ldap/schema/samba.schema  
$ chmod 644 /etc/ldap/schema/samba.schema
```

Per finalitzar, només queda afegir el nou esquema al fitxer de configuració de *slapd* i reiniciar el dimoni. Per fer-ho haurem d'editar l'arxiu */etc/ldap/slapd.conf* i afegir a la secció *#Schema and objectClass definitions* la següent línia:

```
include /etc/ldap/schema/samba.schema
```

La classe objecte (*objectClass*) *sambaSamAccount* definida a l'esquema *samba.schema* depèn dels següents esquemes que ja tenim al arxiu de configuració */etc/ldap/slapd.conf*.

```
include      /etc/openldap/schema/cosine.schema
include      /etc/openldap/schema/inetorgperson.schema
include      /etc/openldap/schema/nis.schema
```

L'esquema de *samba* s'ha d'inserir després dels esquemes anteriors, ja que tal i com hem dit depèn d'aquests i el dimoni *slapd* llegeix línia a línia l'arxiu de configuració.

Si posem l'esquema de *samba* davant dels altres esquemes, al reiniciar el dimoni *slapd*, ens donarà un error, ja que *slapd* no trobarà els esquemes dels quals depèn *Samba*.

Per finalitzar haurem de reiniciar el dimoni *slapd* executant:

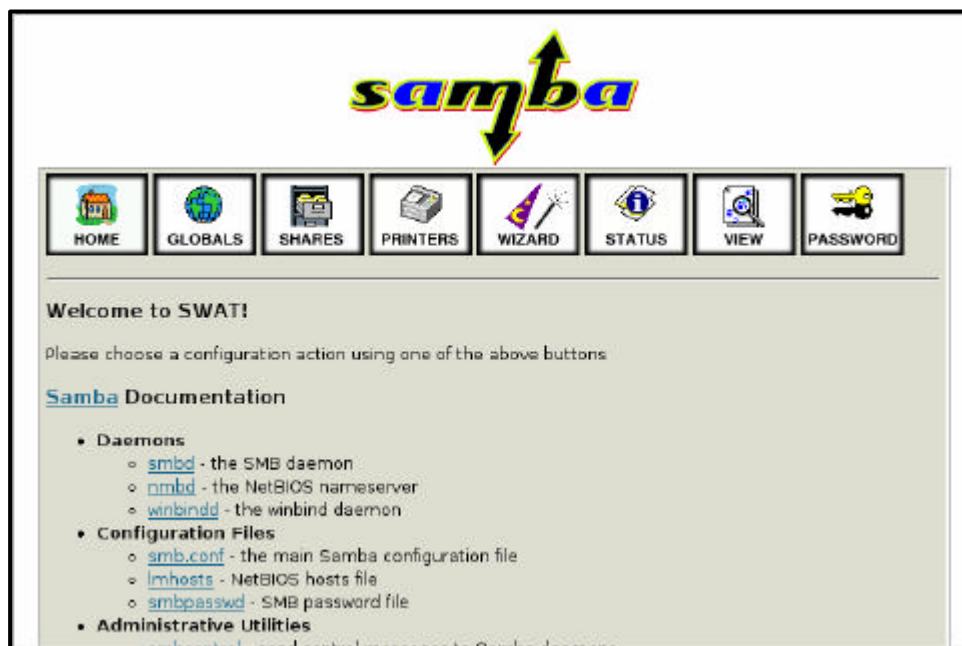
```
$ /etc/init.d/slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: slapd.
```

A partir d'ara entrarem en detall de la configuració de *Samba*. Primer mostrarem com és l'estructura d'un arxiu de configuració per a *Samba* i després procedirem a mostrar les diferents opcions de configuracions per obtenir el resultat idoni pel nostre projecte.

La configuració de *Samba* s'emmagatzema en l'arxiu *smb.conf*, que en el sistema *Debian GNU/Linux* es troba al directori */etc/samba/*. L'edició d'aquest arxiu és pot fer mitjançant un editor de text o fent us d'eines gràfiques com la que dona *Samba: SWAT*.

Per tal d'executar *SWAT* (*Samba Web Administration Tool*), escriurem les següents línies al nostre navegador web <http://projecte.ldap:901/>

Per tal de poder entrar a *SWAT* ens demanarà un nom d'usuari i clau que tingui permisos per executar aquesta eina. Escriurem l'usuari *root* i la seva clau, un cop entrada correctament la informació, entrarem a la pantalla d'inici de *SWAT*, que tindrà el següent aspecte:



Mitjançant aquesta interfície web, podrem *trosetejar* l'arxiu de configuració de *Samba* en diferents seccions (*HOME*, *GLOBALS*, *SHARES*, *PRINTERS*). Si entrem en les diferents seccions, ens mostrarà totes les opcions disponibles i les podrem modificar molt fàcilment.

SWAT també ens ofereix un assistent (botó *WIZARD*) per tal de configurar fàcilment *Samba*, i ens permet veure l'estat del nostre servidor *Samba*, podem veure tot el fitxer de configuració i, afegir i esborrar claus a *Samba*.

Encara i que *SWAT* ens facilitarà molt configurar el nostre sistema *Samba*, editarem l'arxiu de configuració `/etc/samba/smb.conf` sense aquesta eina, i explicarem les diferents opcions dins d'aquest arxiu.

L'arxiu *smb.conf* utilitza la mateixa sintaxis que els antics fitxers *.ini* de *Windows 3.1*. Cadascun dels arxius consistien en diverses seccions, cadascuna de les seccions comença amb el nom de la secció entre claudàtors ([]) en una nova línia. Cadascuna contenia zero o més parells clau/valor separats per un signe d'igualtat (=). L'arxiu de configuració de *Samba* és un arxiu en text pla, que podem editar amb qualsevol editor de texts, com per exemple *vim*.

Cada secció a l'arxiu *smb.conf* representa un recurs compartit al servidor *Samba*.

Una de les seccions que inclou l'arxiu *smb.conf* és la secció *[global]*.

La secció *[global]* és especial, ja que és on tenim les opcions que s'apliquen a tot el servidor *Samba* i no només a un recurs compartit en particular.

Un arxiu bàsic *smb.conf* podria ser el següent:

[global]

workgroup = **GRUPODETRABAJO**

netbios name = **MINOMBRE**

[recurs-compartit1]

path = */tmp*

[recurs-compartit2]

path = */altre_directori_compartit*

És molt important validar en tot moment el contingut de l'arxiu *smb.conf* cercant possibles errades, sobretot un cop hem fet una modificació en l'arxiu.

Per fer aquesta verificació utilitzarem la comanda *testparm*. Si *testparm* s'executa correctament, donarà un llistat de tots els serveis carregats. Si per algun motiu hi hagués qualsevol error, ens ho donaria al executar-ho, donant-nos informació per tal de corregir-ho.

Si fem la comprovació amb l'arxiu *smb.conf* que tenim un cop instal·lat *Samba*, un cop configurat bàsicament *samba*, executant *testparm* de la següent manera:

```
$ testparm
```

Ens donarà la següent resposta:

```
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
[ENTER]
```

```
$ Global parameters
```

```
[
```

```
global]
```

```
workgroup = PROJECTE
server string = SAMBA-LDAP
obey pam restrictions = Yes
passwd backend = tdbsam, guest
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snewsUNIX\spassword:* %n\n
```

```
*Retype\snewsUNIX\spassword:* %n\n .
```

```
syslog = 0
log file = /var/log/samba/log.%m
max log size = 1000
dns proxy = No
panic action = /usr/share/samba/panic-action %d
invalid users = root
```

```
[homes]
```

```
comment = Home Directories
create mask = 0700
directory mask = 0700
browseable = No
```

[printers]

comment = All Printers

path = /tmp

create mask = 0700

printable = Yes

browseable = No

[print\$]

comment = Printer Drivers

path = /var/lib/samba/printers

Com podem veure la línia *Loaded services file OK* ens indica que no tenim cap error, això vol dir que l'arxiu de configuració de *Samba*, fins el moment és correcte, encara que no tingui les prestacions adequades pel nostre projecte.

A partir d'aquest moment veurem com configurar *Samba* per tal que sigui un Controlador Primari de Domini (*PDC*) de la nostra xarxa i que emmagatzemi la seva base de dades *SAM* al nostre servidor *LDAP*.

Per a la configuració utilitzarem les següents variables:

- Nom de domini= *PROJECTE* (Definit a la configuració bàsica de *Samba*)
- Nom del servidor *NetBIOS* = *PROJECTELDAP*
- El directori *home* dels usuaris *Samba* els tindrem a:
/home/samba/users/NOMUSUARI
- Els perfils mòbils estaran emmagatzemats a
/home/samba/profiles/NOMUSUARI

Com hem vist per sobre anteriorment, a la secció `[global]` de *smb.conf* configurarem el paràmetres globals del servidor. Haurem de definir els programes que seran utilitzats per a que un usuari pugui canviar la seva clau (*passwd program*) i el diàleg que s'establirà entre el servidor i el client durant aquest intercanvi.

L'opció *add user script* de la secció *[global]* permet al dimoni de *Samba* afegir, com a usuari *root*, una nova màquina. Quan una màquina contacta amb el domini, aquest script és crida i la nova màquina s'afegeix al domini. Això fa que l'administració dels comptes per a màquines sigui molt senzilla. Per raons de seguretat no totes les màquines podran entrar al domini, només aquelles que el seu administrador tingui un compte amb els suficients privilegis com per entrar-hi.

En el cas de no fer ús de l'opció *add user script* hauríem de posar a mà totes les màquines del nostre domini, la qual cosa implicaria una gran pèrdua de temps.

A continuació mostrarem els paràmetres més importants alhora de configurar l'arxiu *smb.conf*.

Secció [global]

Dins de la secció *[global]* trobem els següents paràmetres:

Paràmetres de definició

- *workgroup = PROJECTE* : És la definició del nom del domini
- *netbios name = PROJECTELDAP* : Nom *NetBIOS* amb el que el servidor *Samba* es donarà a conèixer
- *server string = SAMBA-LDAP* : Descripció del servidor.

Paràmetres d'autenticació

- *security = user* : Opció necessària per a l'administració de dominis per part de *Samba*
- *obey pam restriction = yes* : Opció que fa que *Samba* faci cas de les restriccions de *PAM*
- *encrypt passwd = true* . Activa el xifrat per l'emmagatzemament de claus

- *passdb backend = ldapsam:ldap://projecte.ldap/* : El valor d'aquest paràmetre indica a *Samba* que les claus s'emmagatzemaran i recuperaran del nostre servidor *LDAP*.
- *guest account = guest* : Usuari invitat, podrà accedir als recursos que continguin el paràmetre *guest ok* sense necessitat d'autenticar-se.
- *invalid user = root* : Llista d'usuaris que no se li permet l'accés a *Samba*, com veurem posteriorment, aquest valor s'haurà de comentar en ocasions especials.
- *unix passwd sync = yes* : S'activa la sincronització entre les claus *Unix* i *Samba*
- *passwd program = /usr/local/sbin/smbldap-passwd -o %u* : Programa utilitzat durant el canvi d'una clau d'un usuari.
- *passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n* : Text que es mostrarà durant el canvi d'una clau mitjançant *Samba*.

Paràmetres LDAP

- *ldap admin dn= cn=admin,dc=projecte,dc=ldap* : Li diu a *Samba* qui serà l'usuari encarregat de realitzar les operacions per tal d'afegir, esborrar o modificar comptes d'usuari. Com hem vist anteriorment, aquest usuari només pot ser l'administrador d'*LDAP*.
- *ldap ssl = off* : Determina si xifrem o no les comunicacions entre el servidor *Samba* i el servidor *LDAP*, quan configurem *SAMBA-LDAP* de forma segura haurem de modificar aquest valor.
- *ldap delete dn= no* : aquest paràmetre especifica si al realitzar una operació d'esborrat a *ldapsam*, s'esborra l'entrada completa o només els atributs específics de *Samba*.
- *ldap filter=(amp(uid=%u)(objectclass=sambaSamAccount))* : Indica el filtre de cerca per a *LDAP*.
- *ldap suffix = dc=projecte,dc=ldap* : Paràmetre que especifica la base per totes les cerques en *ldap*.

- *ldap user suffix = ou=people* : Paràmetre que indica on s'afegeixen els usuaris dins de l'arbre *LDAP*.
- *ldap group suffix = ou=groups* : Paràmetre que indica on s'afegeixen els grups dins de l'arbre *LDAP*.
- *ldap machine suffix = ou=machines* : Paràmetre que indica on s'afegeixen les màquines dins de l'arbre *LDAP*.

Paràmetres d'impressió

- *load printers = yes* : Paràmetre que càrrega automàticament la llista d'impressores disponibles.
- *printing = CUPS* : Estil d'impressió a utilitzar. En el nostre cas farem servir *CUPS*, que posteriorment configurarem.
- *printcapname = CUPS* : Estil d'impressió a utilitzar.
- *printer admin = @domainadmins* : Grup d'usuaris que tenen permís per afegir i configurar impressores.

Paràmetres de Controlador de Domini

- *os level = 80* : Paràmetre que controla el nivell del sistema operatiu de *Samba*. Les diferents màquines *Windows* veuen *Samba* com un servidor *Microsoft*, variant el nivell d'*os level* li diem quin tipus de servidor seria, per exemple, si l'*os level* fos igual a 34, les màquines *Windows* veurien *Samba* com un servidor *WindowsNT*.
- *preferred master = yes*.
- *domain master = yes*.
- *local master = yes*.
- *domain logons = yes*.

Totes les opcions anteriors, fan que *Samba* actuï com a Controlador Primari del Domini, totes quatre han de ser certes per tal que *Samba* actui com a *PDC* a la xarxa.

- *logon path = \\%L\profiles\%u*: Especifica la ruta dels perfils de l'usuari
- *logon drive = H:* Especifica la ruta local a les màquines *Windows* on es crearà el directori *home*.
- *logon home = \\%L\%u\.profile*: Especifica on es troba el directori *home* al servidor.
- *socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192* : Opció disponibles per tal de millorar el rendiment del servidor *Samba*
- *idmap uid = 10000-20000* : Indiquen el rang d' identificadors d'usuaris que s'utilitzaran al mapejar usuaris *Unix*
- *idmap gid = 10000-20000* : Indiquen el rang d' identificadors de grups que s'utilitzaran al mapejar grups *Unix*.
- *template shell = /bin/bash* : *Shell* que el dimoni *winbindd* afegirà a la informació d'un usuari.
- *add user script = /usr/local/sbin/smbldap-useradd -w %u* : Per afegir màquines utilitzarem les eines *smbldaptools* que posteriorment configurarem.

Aquestes son totes les modificacions que ens caldria fer a la secció *[global]*, per implementar el nostre servidor *Samba*.

Secció [homes]

Aquesta secció ens permet la compartició del directori *home* dels usuaris, de manera que, depenent quin usuari s'hagi autenticat al sistema, *Samba* compartirà el seu directori personal únicament a ell.

Els paràmetres més importants d'aquesta secció són:

- *browseable = yes* : Indica si el recurs es mostrarà a la llista de recursos compartits.
- *writeable = yes* : Permet escriure dades als directoris *homes*, si el valor fos *no* , els *homes* dels usuaris serien de només lectura.
- *create mask = 0700* : Màscara de creació d'arxius, indica els permisos que tindran els arxius de nova creació.
- *directory mask = 0700* : Màscara de creació de directoris, indica els permisos que tindran els directoris de nova creació.

Secció [netlogon]

El recurs compartit *netlogon* juga un paper fonamental en el suport d'inici de sessió a un domini. Aquest recurs compartit es dona en tots els controladors de domini de *Microsoft*. S'utilitza per donar *scripts* d'inici de sessió, per emmagatzemar arxius de polítiques de grups, així com la localització d'altres eines comuns que es puguin necessitar per al procés d'inici de sessió. Aquest és un recurs essencial a un controlador de domini.

Els paràmetres més importants d'aquesta secció es mostren a continuació:

- *path = /home/samba/netlogon* : Directori a on emmagatzemarem els *scripts*.
- *writeable = no* ; El recurs serà de només lectura.
- *write list = @domainadmins* : Llista d'usuaris/grups que tindran permisos d'escriptura al recurs.

Secció [profiles]

Aquest recurs compartit s'utilitzarà per emmagatzemar els perfils d'escriptori dels usuaris. Cada usuari ha de tenir un directori en l'arrel d'aquest recurs compartit. Aquest recurs ha de tenir permisos d'escriptura per als usuaris i hauria tenir permisos de lectura globals. *Samba-3* té un mòdul *VFS* denominat *fake_permission* (permisos "falsos") que s'haurien d'instal·lar en aquest recurs. Aquest mòdul permet a un administrador *Samba* fer el directori de només lectura per a tothom. Això només és útil si s'ha creat correctament el perfil.

Els paràmetres més importants d'aquesta secció es mostren a continuació:

- *path=/home/samba/profiles* : Directori on s'emmagatzemaran els perfils mòbils, sota aquest directori cada usuari tindrà una carpeta amb el seu nom.
- *writable = yes* : permet escriure al recurs compartit
- *browseable = no* : Indica si el recurs es mostrarà a la llista de recursos compartits, en aquest cas no serà així.
- *create mask = 0600* : Màscara de creació d'arxius, indica els permisos que tindran els arxius de nova creació al recurs.
- *directory mask = 0700* : Màscara de creació de directoris, indica els permisos que tindran els arxius de nova creació al recurs.

Secció [printers]

Aquest és un recurs compartit especial que crea automàticament els serveis d'impressió. La forma en la qual treballa és la següent: si es crea un recurs compartit amb el nom [printers] en l'arxiu de configuració *smb.conf*. Samba llegirà automàticament l'arxiu de definició de les seves impressores i crearà automàticament una impressora compartida per cada impressora que aparegui a l'arxiu de definició. Per exemple si tenim tres impressores definides com *HP*, *Canon* i *Kyocera*, Samba donarà tres impressores compartides amb els seus respectius noms, cada una configurada amb les opcions que tingui el recurs compartit [printers].

El paràmetres més importants d'aquesta secció són els següents:

- *browseable = no* : Indica si aquest recurs apareixerà a la llista de recursos compartits, en aquest cas no apareixerà.
- *path=/tmp* : Directori que utilitzarà Samba com a cua d'impressió
- *printable = yes* :Quan aquest paràmetre és afirmatiu, els clients que es connectin al servidor, podran obrir, escriure i enviar arxius a la cua d'impressió, és a dir, al directori especificat al paràmetre path.
- *guest ok = no* :No es permetrà les autenticacions sense autenticació a aquest recurs.
- *writable = no* :No es permetrà escriure al recurs compartit
- *create mask = 0700* :Màscara de creació d'arxius, el valor d'aquest paràmetre indicarà els permisos que tindrà un arxiu de nova creació.

Secció `[print$]`

Igual que els servidors d'impressió *Windows* NT, per a suportar la descàrrega de controladors per part de clients amb diferents arquitectures, s'han de crear diversos subdirectoris dins del mateix servei `[print$]`. Aquests directoris es correspondran amb cada una de les arquitectures suportades. *Samba* també fa ús d'aquest esquema, així com el nom de recurs ha de ser `[print$]`, els subdirectoris que hem de tenir han de ser exactament els noms que detallarem a continuació (podem eliminar aquells directoris referents a arquitectures que no necessitem).

`[print$]--+`

```
--W32X86      # controladores para Windows NT x86
--WIN40       # controladores para Windows 95/98
--W32ALPHA    # controladores para Windows NT Alpha_AXP
--W32MIPS     # controladores para Windows NT R4000
```

Aquesta estructura de directoris han d'estar sota el directori `/var/lib/samba/printers`.

Si no tinguéssim creats aquesta estructura de directori, crearem aquells directoris per a les arquitectures que volem tenir suport.

Els paràmetres més importants dins d'aquesta secció són:

- `path = /var/lib/samba/printers`: Directori on s'emmagatzemaran els controladors d'impressió per les diferents arquitectures.
- `browseable=yes`: Aquest paràmetre ens indica que el recurs serà visible a la llista de recursos compartits.
- `writeable=no`: No es permet escriure al recurs compartit.
- `guest ok=no`: No es permeten connexions sense autenticació a aquest recurs.
- `write list = root, @domainadmins`: Llista d'usuaris/grups que tenen permís d'escriptura al recurs compartit.

Com a exemple de creació d'un recurs compartit mitjançant *Samba*, compartirem el nostre directori temporal */tmp*, per fer-ho afegirem els següents paràmetres a l'arxiu *smb.conf*

- *[tmp]* : Nom del recurs compartit
- *comment = Temporal* : Comentari del recurs compartit creat
- *writeable = yes* : Es permet l'escriptura a aquest recurs compartit.
- *path = /tmp* : Directori que compartirem del nostre sistema
- *guest ok = no* : No es permeten les connexions anònimes al directori, tot usuari s'ha d'identificar per entrar a aquest recurs.

També podem compartir unitats físiques com el *floppy* o el *CDROM*, a continuació veurem que podem fer per compartir una unitat de *CDROM*.

Per compartir el nostre *CDROM*, afegirem els següents valors a l'arxiu de configuració de *Samba* */etc/samba/smb.conf*.

- *[cdrom]* : Nom del recurs compartit.
- *comment = cdrom* : Comentari del recurs compartit creat.
- *locking = no* : No es bloquejaran els arxius a petició dels clients, simplement s'informarà de que aquest ha estat efectiu.
- *path = /mount/cdrom* : Ruta a on trobem el nostre recurs compartit
- *guest ok = yes* : No ens farà falta autenticar-nos per tal de utilitzar aquest recurs compartit.

Si volem veure totes les opcions que ens aporta l'arxiu de configuració de *Samba*, a la documentació de l'arxiu de configuració tindrem gran informació. Per tal d'accedir al manual executarem:

```
$ man smb.conf
```

Per tal de comprovar que el nostre servidor *Samba* actua com a controlador de domini primari reiniciarem els dimonis de samba amb la comanda:

```
$ /etc/init.d/samba restart
```

I executarem la comanda *testparm*:

```
$ testparm
```

Ens hem de fixar que a la sortida d'aquesta comanda, ens aparegui a la línia *Server Role* la següent resposta:

```
Server role: ROLE_DOMAIN_PDC
```

Un cop configurat el nostre arxiu de configuració de *Samba*, dient-li que ha d'actuar com un *PDC* (Controlador de Domini Principal) i indicant-li que ha d'anar a cerca el nostre servei de directori *LDAP* per tal d'autenticar-se els clients, i abans de considerar el nostre servidor *Samba* completament configurat, s'han de fer una sèrie de modificacions al sistema, modificacions que veurem a continuació:

Samba necessita saber la clau de l'administrador del directori *LDAP* per poder accedir a aquest, per aquest motiu és necessari indicar-li manualment aquesta clau, per fer-ho haurem executar la següent comanda:

```
$ smbpasswd -w clau
```

```
Setting stored password for "cn=admin,dc=projecte,dc=ldap" in secrets.tdb
```

Hem de tenir en compte que si l'administrador de *LDAP* canvia, haurem de canviar el valor del paràmetre *ldap admin dn* de l'arxiu de configuració de *Samba*, així com tornar a cridar a la comanda anterior per tal de indicar-li a *Samba* la clau del nou administrador.

Com a partir d'ara emmagatzemarem totes les claus relacionades amb *Samba* al nostre directori *LDAP*, haurem d'impedir que tots aquells usuaris que no siguin l'administrador *LDAP*, tinguin accés a les *hashes* de les distintes claus emmagatzemades al directori *LDAP*. Per tar de portar a terme aquesta restricció afegirem les següents línies a l'arxiu de configuració del dimoni *slapd* */etc/ldap/slapd.conf*:

```
access to attrs=sambaLMPassword,sambaNTPassword
  by dn="cn=admin,dc=projecte,dc=ldap" write
  by * none
```

Com a objectiu de millorar el rendiment de les cerques dins del directori *LDAP*, s'afegiran una sèrie d'índexs a l'arxiu de configuració del dimoni *slapd*.

Els índexs que afegirem, incrementen la velocitat en les cerques realitzades sobre els objectes *sambaSamAccount* i sobre *posixAccount* i *posixGroup*.

Els índexs a afegir són els següents:

```
# Requerido por OpenLDAP
index objectclass      eq
index default          sub
index cn                pres,sub,eq
index sn                pres,sub,eq
# Requerido para soportar pdb_getsampwnam
index uid              pres,sub,eq
# Requerido para soportar pdb_getsambapwrid()
index displayName     pres,sub,eq
# Descomente las siguientes líneas si está almacenando entradas
# posixAccount y posixGroup en el directorio
index uidNumber      eq
index gidNumber     eq
index memberUid     eq
# Samba 3.*
index sambaSID      eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq
```

Un cop hem fet els canvis a l'arxiu `/etc/ldap/slapd.conf` haurem de regenerar els índexs per tal que `LDAP` els utilitzi la propera vegada que es faci una cerca. Per regenerar-los haurem executar:

```
$ slapindex -f /etc/ldap/slapd.conf
```

Un cop realitzats afegida la regla de control d'accés i els índexs per tal de millorar la cerca, haurem reiniciar el nostre servidor `LDAP` per tal de guardar tots els canvis fets a l'arxiu de configuració de `slapd`.

Per reiniciar el servidor `LDAP`, executarem:

```
$ /etc/init.d/slapd restart  
Stopping OpenLDAP: slapd.  
Starting OpenLDAP: slapd.
```

A l'hora de modificar l'arxiu de configuració de `Samba`, s'han definit una sèrie de directoris per a diferents paràmetres dins de les seccions `[global]`, `[netlogon]` i `[profiles]` dedicats a diferents tasques dins de `Samba`, com pot ser emmagatzemar perfils mòbils dels usuaris, `scripts` per a `netlogon` o el directori `home` dels usuaris.

Per crear aquests directoris, executarem:

```
$ mkdir -pm 755 /home/samba/  
$ mkdir -pm 755 /home/samba/netlogon /home/samba/users  
$ mkdir -pm 1757 /home/samba/profiles
```

Un cop hem fet totes les modificacions pertinents per tal que `Samba` faci de `PDC` (Controlador Primari de Domini) verificarem que tot el que s'ha realitzat fins ara funciona correctament. Per comprovar que el nostre servidor `Samba` s'executa sense cap mena d'errors, farem ús del programa `testparm`, que ja varem utilitzar al inici de la configuració del servidor.

Per executar-ho haurem de escriure la següent comanda a la nostra shell:

```
$ testparm
```

testparm ens retornarà la següent informació:

```
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[netlogon]"
Processing section "[profiles]"
Processing section "[printers]"
Processing section "[print$]"
Processing section "[tmp]"
Processing section "[cdrom]"
Loaded services file OK.
Server role: ROLE_DOMAIN_PDC
Press enter to see a dump of your service definitions
```

Si li donem a la tecla *Intro*, tal com ens indica, *testparm* ens donarà tota la informació que tenim a l'arxiu *smb.conf*.

Com podem veure a la línia marcada amb negreta, l'arxiu de configuració no ens dona cap tipus d'error.

Un cop tenim l'arxiu de configuració de *Samba* funcionant correctament i lliure de possibles errors, el servidor *Samba* haurà de llegir de nou la seva configuració. La forma de fer-ho seria escrivint la següent comanda:

```
$/etc/init.d/samba reload
Reloading /etc/samba/smb.conf (smbd only).
```

Encara i que *Samba* li és suficient amb llegir de nou el seu arxiu de configuració per a que els canvis tinguin efecte, reiniciarem els dimonis de *Samba* per tal de veure els logs d'aquests per evitar possibles errors.

Per reiniciar el servidor *Samba* executarem:

```
$ /etc/init.d/samba restart
```

```
Stopping Samba daemons: nmbd smb.
```

```
Starting Samba daemons: nmbd smb.
```

Després de reiniciar els dimonis de *Samba*, farem un cop d'ull als arxius de log dels dimonis de *Samba* que es troben a `/var/log/samba/log.nmbd` i `/var/log/samba/log.smbd`.

Si editem l'arxiu de *log* del dimoni *nmbd*, trobarem la següent informació:

```
[2005/05/28 16:29:35, 0] nmbd/nmbd.c:main(664)
  Netbios nameserver version 3.0.2a-Debian started.
  Copyright Andrew Tridgell and the Samba Team 1994-2005
[2005/05/28 16:29:35, 0] nmbd/nmbd_logonnames.c:add_logon_names(163)
  add_domain_logon_names:Attempting to become logon server for workgroup
PROJECTE on subnet XXX.XXX.XXX.XXX
[2005/05/28 16:29:35, 0]
nmbd/nmbd_become_dmb.c:become_domain_master_browser_bcast(282)
  become_domain_master_browser_bast: Attempting to become domain master browser
on workgroup PROJECTE on subnet XXX.XXX.XXX.XXX
[2005/05/28 16:29:35, 0]
nmbd/nmbd_become_dmb.c:become_domain_master_browser_bcast(295)
  become_domain_master_browser_bcast: querying subnet XXX.XXX.XXX.XXX for
domain master browser on workgroup PROJECTE
[2005/05/28 16:29:39, 0] nmbd/nmbd_logonnames.c:become_logon_server_success(124)
  become_logon_server_success: Samba is now a logon server for workgroup
PROJECTE on subnet XXX.XXX.XXX.XXX
[2005/05/28 16:29:43, 0]
nmbd/nmbd_become_dmb.c:become_domain_master_stage2(113)
  *****
  Samba server PROJECTELDAP is now a domain master browser for workgroup
PROJECTE on subnet XXX.XXX.XXX.XXX
  *****
[2005/05/28 16:29:58, 0] nmbd/nmbd_become_lmb.c:become_local_master_stage2(396)
  *****
  Samba name server PROJECTELDAP is now a local master browser for
workgroup PROJECTE on subnet XXX.XXX.XXX.XXX
```

Podem comprovar que *Samba* s'ha convertit en un controlador de domini sota la subxarxa *XXX.XXX.XXX.XXX*, tal i com volíem. El domini que administra *Samba* és *PROJECTE*.

Per finalitzar comprovarem l'arxiu de log del dimoni *smbd*. Si editem l'arxiu que el podem trobar a */var/log/samba/log.smbd* ens donarà la següent informació:

```
[2005/05/28 16:29:35, 0] smbd/server.c:main(747)
smbd version 3.0.2a-Debian started.
Copyright Andrew Tridgell and the Samba Team 1992-2005
[2005/05/28 16:29:35, 0] printing/print_CUPS.c:CUPS_printer_fn(108)
Unable to connect to CUPS server localhost - Conexión rehusada
```

Com en aquests moments encara no tenim instal·lat el servidor d'impressió *CUPS*, *Samba* no pot contactar amb ell, aquests problema el solucionarem més endavant, ja que encara que tinguem aquest error podem treballar tranquil·lament amb *Samba* sense cap tipus de problema.

A partir d'aquest moment podem dir que el nostre servidor *LDAP* està configurat adequadament per a la autenticació d'usuaris en màquines *Windows* a través del servidor *LDAP*.

9.3. Configuració Samba-LDAP-Segur

La configuració del nostre servidor *Samba* per que utilitzi *LDAP* Segur per l'autenticació d'usuaris a màquines *Windows*, no comporta gran dificultat, només haurem de modificar les següents línies de l'arxiu de configuració de *Samba* que es troba a */etc/samba/smb.conf*

```
passdb backend = ldapsam:ldaps://projecte.ldap  
ldap ssl = yes
```

Com podem veure només modificarem la interfície *LDAP* a on escoltarà *Samba*, canviant la interfície no segura (*ldap://projecte.ldap*) per la segura (*ldaps://projecte.ldap*).

Per finalitzar només li haurem de dir a *Samba* que utilitzi el protocol *SSL* per la connexió xifrada amb el nostre servidor *LDAP*.

Un cop modificades aquestes opcions, haurem reiniciar *Samba* amb la comanda:

```
$/etc/init.d/samba restart  
Stopping Samba daemons: nmbd smbd.  
Starting Samba daemons: nmbd smbd.
```

Per comprovar que no tenim cap tipus de problema en la modificació de l'arxiu de configuració de *Samba* perquè utilitzi *LDAP* Segur, executarem la comanda:

```
$ testparm
```

L'execució de *testparm* ens donarà la següent sortida:

```
Load smb config files from /etc/samba/smb.conf  
Processing section "[homes]"  
Processing section "[netlogon]"  
Processing section "[profiles]"  
Processing section "[printers]"
```

Processing section "[print\$]"

Processing section "[tmp]"

Processing section "[cdrom]"

Loaded services file OK.

Server role: ROLE_DOMAIN_PDC

Press enter to see a dump of your service definitions

Si li donem a la tecla Intro, tal com ens indica, *testparm* ens donarà tota la informació que tenim a l'arxiu *smb.conf*.

Podem veure que la línia **Loaded services file OK**. Ens diu que l'arxiu de configuració és correcte, per tant podem dir que ja tenim el nostre *Samba* preparat per autenticar els clients *Windows* de forma segura amb el protocol *SSL*.

Un cop comprovat que tot funciona correctament, només ens quedarà instal·lar les eines *smbldap-tools*, per tal de aconseguir la perfecta integració entre *LDAP* i *Samba*.

8.4. smbldap-tools

Els *scripts* que tenen el conjunt d'eines de *smbldap-tools* necessiten el paquet *libnet-ldap-perl*, per la qual cosa si no ho tenim instal·lat, haurem instal·lar el paquet executant la comanda:

```
$apt-get install libnet-ldap-perl
```

Suposem que l'arxiu *smbldap-tools-0.8.4.tgz* que hem descarregat de la web d'*IDEALX* (creadors de les eines *smbldap-tools*) està localitzat al nostre arxiu temporal */tmp*.

El primer que haurem de fer és descomprimir l'arxiu, per fer-ho executarem la següent comanda:

```
$ tar xzf /tmp/smbldap-tools-0.8.4.tgz -C /tmp/
```

Un cop hem descomprimit l'arxiu, haurem de canviar el propietari i grup del *scripts* per *root*, recordem que *root* és l'administrador del nostre servidor *Samba*, per fer-ho executarem:

```
$ chown -R root.root /tmp/smbldap-tools-0.8.4/*
```

Un cop fet el canvi de permisos, haurem traspasar els *scripts* al directori */usr/local/sbin* per tal que pugui executar-se directament, podem identificar els *scripts* perquè son tots aquells que tenen el prefix *smbldap-*. Per fer la copia dels *scripts* executarem:

```
$ cp --remove-destination /tmp/smbldap-tools-0.8.4/smbldap-* /usr/local/sbin/  
$ cp --remove-destination /tmp/smbldap-tools-0.8.4/smbldap*.pm /usr/local/sbin/
```

Un cop tenim els *scripts* copiats i disposats per la seva execució, copiarem els arxiu de configuració de *smbldap-tools* a la carpeta */etc/smbldap-tools*. Aquesta carpeta la tindrem que crear el primer cop que instal·lem *smbldap-tools*. Els arxius de configuració de *smbldap-tools* són aquells que tenen l'extensió *.conf*. Per crear el directori i copiar els arxius de configuració executarem:

```
$ mkdir -m 755 /etc/smbldap-tools/  
$ cp /tmp/smbldap-tools-0.8.4/smbldap*conf /etc/smbldap-tools/  
$ chmod 600 /etc/smbldap-tools/*
```

Per tal de configurar *smbldap-tools*, aquesta eina ens dona la possibilitat d'executar l'script *configure.pl* que ens facilitarà la tasca de configuració. Per tal d'executar l'script escriurem la següent comanda a la nostra *shell*:

```
$ cd /tmp/smbldap-tools-0.8.4/
```

```
$ ./configure.pl
```


Que ens proporcionarà la següent sortida:

```
-----
  smbldap-tools script configuration
-----

Before starting, check
. if your samba controller is up and running.
. if the domain SID is defined (you can get it with the 'net getlocalsid')

. you can leave the configuration using the Ctrl-c key combination
. empty value can be set with the "." character
-----

Looking for configuration files...
Samba Config File Location [/etc/samba/smb.conf] > [ENTER]
smbldap Config file Location (global parameters) [/etc/smbldap-tools/smbldap.conf] > [ENTER]
smbldap Config file Location (bind parameters) [/etc/smbldap-tools/smbldap_bind.conf] > [ENTER]
-----

Let's start configuring the smbldap-tools scripts ...
. workgroup name: name of the domain Samba act as a PDC
  workgroup name [PROJECTE] > [ENTER]
. netbios name: netbios name of the samba controler
  netbios name [PROJECTELDAP] > [ENTER]
. logon script: may be startup.cmd, ... or "" to set it to username.cmd
  logon script [] > [ENTER]
. logon drive: local path to which the home directory will be connected (for NT Workstations). Ex: 'H:'
  logon drive [H:] > [ENTER]
. logon home: home directory location (for Win95/98 or NT Workstation). Ex: '\\PROJECTELDAP\home'
  logon home (leave blank if you don't want homeDirectory) [\\%L%\u\profile] > \\PROJECTELDAP\
. logon path: home directory where roaming profiles are stored. Ex: '\\PROJECTELDAP\profiles\'
  logon path (leave blank if you don't want roaming profile) [\\%L\profiles\%u] > \\PROJECTELDAP\profiles\
. ldap suffix [dc=projecte,dc=ldap] > [ENTER]
. ldap group suffix [ou=groups] > [ENTER]
. ldap user suffix [ou=people] > [ENTER]
. ldap machine suffix [ou=machines] > [ENTER]
. ldap master server: IP adress or DNS name of the master (writable) ldap server
  ldap master server [] > projecte.ldap
. ldap master port [389] > 636 [ENTER]
. ldap master bind dn [cn=admin,dc=projecte,dc=ldap] > [ENTER]
. ldap master bind password [] > [clau]
. ldap slave server: IP adress or DNS name of the slave ldap server: can also be the master one
```

```

ldap slave server [] > projecte.ldap
. ldap master port [389] > [ENTER]
. ldap master bind dn [cn=admin,dc=projecte,dc=ldap] > [ENTER]
. ldap master bind password [] > [clau]
. ldap tls support (1/0) [0] > [ENTER]
. SID for domain PROJECTE: SID of the domain (can be obtained with 'net getlocalsid
PROJECTELDAP')
SID for domain PROJECTE [S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX] > [ENTER]
. unix password encryption: encryption used for unix passwords
unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA) [SSHA] > MD5
. default user gidNumber [513] > 10001
. default computer gidNumber [553] > 10001
. home directory prefix (without username) [/home/] > /home/samba/users/
. default password validation: default time before a user has to change his password
default password validation time (time in days) [45] > 0
. default login shell [/bin/bash] > [ENTER]
=====
backup old configuration files:
/etc/smbldap-tools/smbldap.conf->/etc/smbldap-tools/smbldap.conf.old
/etc/smbldap-tools/smbldap_bind.conf->/etc/smbldap-tools/smbldap_bind.conf.old
writing new configuration file:
/etc/smbldap-tools/smbldap.conf done.
/etc/smbldap-tools/smbldap_bind.conf done.

```

Com podem veure l'script de configuració és molt intuïtiu i gràcies a que el mateix script llegeix l'arxiu de configuració de samba, gairebé no tindrem que configurar res, i només haurem de donar-li a l'enter tota la estona per configurar *smbldap-tools* amb els valors per defecte que el propi script ens dona.

Per finalitzar només ens quedarà instal·lar el programa *mkntpwd*. El codi font d'aquest programa es troba dins del paquet *smbldap-tools*, per tant, s'ha d'accedir al directori on hem descomprimit el paquet.

Allí trobarem un arxiu denominat *mkntpwd.tar.gz* es descomprimeix i compilarem el codi que es troba al seu interior. Finalment copiarem el programa resultant al directori */usr/local/sbin* perquè pugui ser executat des de qualsevol ruta. El programa *mkntpwd* ens farà falta per la interfície web d'administració LDAP, *phpLDAPadmin*, per la creació dels password per màquines *Windows* a partir d'aquesta interfície.

Per tal de desempaquetar i compilar executarem les següents comandes:

```
$ cd /tmp/smbldap-tools-0.8.4/
```

```
$ /bin/tar xzf mkntpwd.tar.gz
```

```
$ cd mkntpwd
```

```
$ make
```

```
$ cp -f mkntpwd /usr/local/sbin/
```

```
$ chmod -v 755 /usr/local/sbin/mkntpwd
```

```
$ chown -v root.root /usr/local/sbin/mkntpwd
```

9.5. Clients Samba a Unix

Una de les coses a tenir en compte és la possibilitat de modificar els recursos compartits al nostre servidor *Samba* des de màquines *Unix*, els recursos compartits que tenim seran utilitzats per màquines *Windows* i podran ser modificats fàcilment des de aquestes.

L'eina que ens permetrà portar a terme els nostres objectius serà *smbclient*. *smbclient* és un client semblant al client *FTP*, que permet l'accés als recursos compartits d'un servidor mitjançant *SMB/CIFS*. Amb *smbclient* podem llistar tots els recursos que tingui compartit un determinat servidor per a un determinat usuari. Per tal de veure la llista de recursos haurem de executar:

```
$ smbclient -L PROJECTELDAP --user=usuari
Password: [clau]
Domain=[PROJECTE] OS=[Unix] Server=[SAMBA-LDAP]
  Sharename      Type      Comment
  -----      ---      -
  netlogon       Disk      Network Logon Service
  print$         Disk      Printer Drivers
  tmp            Disk      Temporal
  cdrom          Disk      Samba server's CD-ROM
  IPC$           IPC       IPC Service (SAMBA-LDAP PDC server)
  ADMIN$         IPC       IPC Service (SAMBA-LDAP PDC server)
  gsruser        Disk      Home Directories
Domain=[PROJECTE] OS=[Unix] Server=[SAMBA-LDAP]

  Server          Comment
  -----      -
PROJECTELDAP  SAMBA-LDAP

  Workgroup       Master
  -----      -
PROJECTE      PROJECTELDAP
```

L'usuari haurà d'estar creat, en cas de no ser així, podem crear-lo tal i com indiquem al capítol 9.

smbclient també permet l'opció d'accedir a dins d'un recurs compartit i poder fer diferents operacions dintre del mateix. Per fer-ho executarem la comanda:

```
$ smbclient --user=usuari //PROJECTELDAP/usuari  
Password: [clau]
```

Un cop executada ens sortirà una línia de comandes com la següent

```
smb: \>
```

Dins d'aquesta línia de comanda podrem utilitzar gairebé totes les funcions de *Unix* per modificar el recurs compartit al qual accedim.

9.6. Afegir clients Windows al domini

Ara veurem com afegir clients *Windows* al nostre domini, en el cas de la nostra xarxa, només disposem d'equips *Windows 2000* i *Windows XP Professional*.

Totes les versions de *Windows 2000* permeten l'opció de afegir-se al domini, en canvi la versió *Home Edition* de *Windows XP*, no permet aquesta opció, ja que *Windows XP Home Edition* és una versió personal, no per usuaris professionals, així que van desestimar afegir-hi aquesta opció.

9.6.1. Microsoft Windows 2000

Per tal de poder afegir una màquina *W2000* al domini haurem de crear la relació de confiança entre la màquina i el servidor *Samba*. Per tal de crear aquesta relació de confiança, haurem d'executar la següent comanda:

```
$ smbpasswd -a -m maquina
```

A on *maquina* serà el nom de la màquina *W2000* que volem afegir al domini.

Un cop creada la relació de confiança, l'únic usuari que té permisos per afegir una màquina al domini és l'usuari *root*, això significa que haurem de fer un *smbpasswd* per l'usuari *root*, per afegir-ho com a usuari *Samba*. Per fer-ho haurem d'estar autenticats a la màquina *Unix* servidor com a usuari *root*. Per afegir *root* a *Samba* haurem d'executar la següent comanda:

```
$ smbpasswd -a  
New SMB password: [clau]  
Retype new SMB password: [clau]
```

Added user root.

En el cas que a l'arxiu de configuració de *Samba* tinguem la línia *invalid users=root* hauríem de comentar-la i reiniciar el nostre servidor *Samba*.

Un cop fets tots els passos previs, podrem configurar la nostra màquina *Windows 2000* per tal d'afegir-la al nostre domini *Samba*.

Per fer-lo clicarem amb el botó dret del ratolí sobre l'icona de l'escriptori *Mi PC* i seleccionarem al menú desplegable l'opció *Propiedades*.

Llavors se'ns obrirà una pantalla, en la qual haurem de seleccionar la pestanya *Nombre del Equipo*, i posar a l'opció *Domini*, el nom del nostre domini *PROJECTE*, i acceptem.

Un cop acceptem ens demanarà el compte d'un usuari que tingui permisos, com hem vist abans aquest usuari és *root*, posem el nom d'usuari i la clau i acceptem. Al cap d'una estona ens donarà la benvinguda al domini *PROJECTE*, reiniciem l'ordinador i ja podrem autenticar-nos a la nostra màquina *Windows 2000* sobre el servei de directori *LDAP*.

L'administrador del domini haurà de afegir un per un els ordinadors al domini, ja que mai se li podrà donar la clau de l'administrador de *Samba* a un usuari per tal d'afegir-se ell mateix. L'administrador del domini haurà de fer tots els passos anteriors a cada ordinador per tal de afegir la màquina al domini, ja que no hi ha eines per que automàticament un màquina s'afegeixi al domini.

9.6.2. Microsoft Windows XP Professional

Per poder afegir un client *Windows XP Professional* a un domini administrat per *Samba*, s'ha de realitzar un canvi al registre de *Windows*. Per veure el registre de *Windows XP Professional*, li donem a *Inicio->Ejecutar* i escrivim *regedit* i acceptem. Ens sortirà la pantalla del *Registre de Windows*. La clau que hem de canviar dins del registre és *requiresignorseal* que la podem trobar a la ruta *[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]* dins del registre. El valor de la clau *requiresignorseal* s'haurà de canviar a 0, amb la qual cosa la clau quedaria de la següent manera:

requiresignorseal =dword:00000000

9.7. Problemes

Un dels problemes que varem trobar a l'hora d'utilitzar *smbclient*, i tal i com tenim la nostra configuració del servidor *Samba* executem *smbclient* per un determinat usuari ens trobarem amb un error *NT_STATUS_LOGON_FAILURE*. Aquest error és degut a que a l'hora d'autenticar-se des de una màquina *Unix* a *Samba*, aquest no reconeix la clau passada i ens dona el missatge d'error. Aquest error és molt complicat de trobar. En el nostre cas varem haver de començar a configurar de nou *Samba* i mirar cada cop que fèiem una modificació que l'eina funcionés correctament. Després de moltes proves, varem observar que el problema radica en la línia del fitxer de configuració *Samba* que es troba a */etc/samba/smb.conf*, *encrypt password = true*.

Si deixem aquest valor com a cert, *smbclient* ens donarà error a l'autenticar-se, en canvi si modifiquem aquesta línia i li diguem que no utilitzi claus xifrades posant *encrypt password = false*, l'eina *smbclient* funcionava correctament.

Per tant a l'hora de utilitzar *smbclient* havíem de modificar aquesta línia i reiniciar el dimoni de *Samba*. Aquesta semblava la única opció. Però al fi d'aquest projecte i després d'actualitzar els paquets de *samba*, aquest error va desaparèixer i va funcionar correctament amb el xifrat de claus. Per tant depenent de la versió dels paquets que tinguem, aquest tipus d'error no estarà resolt. Recomanem sempre mirar diàriament per tal d'actualitzar els paquets. Per realitzar l'actualització haurem de fer un:

```
$apt-get update
```

I seguidament, un

```
$apt-get upgrade
```

Executant aquestes comandes actualitzarem tots els paquets que disposin d'actualitzacions, amb la qual cosa sempre tindrem un sistema actualitzat.

Cal recordar-nos també de comprovar que tot el sistema funcioni correctament un cop feta l'actualització, ja que potser que ens ajudi a solucionar un error, però també en pot comportar d'altres.

Un altre error que ens pot passar, és que el nostre sistema no actuï com controlador primari del domini (*PDC*), per comprovar que això no sigui així executarem la comanda:

```
$testparm
```

Ens hem de fixar que a la sortida d'aquesta comanda, ens aparegui l'opció:

```
Server role: ROLE_DOMAIN_PDC
```

En cas que no ens aparegui aquesta informació, hem de comprovar si hem posat tota la informació a l'arxiu de configuració de *Samba* per que actuï com a *PDC*.

Les entrades que fan que *Samba* actuï com a *PDC* són les següents:

```
security = user
```

```
os level = 34
```

```
local master = yes
```

```
preferred master = yes
```

```
domain master = yes
```

```
domain logons = yes
```

Haurem de mirar que al nostre arxiu de configuració de *Samba*, no faltin cap d'aquestes entrades.

També ens podem trobar errors a l'hora d'afegir una màquina *Windows* al servidor *Samba*. És comú trobar-nos amb un error de relació de confiança a l'hora d'afegir la màquina al domini. Això vol dir que no hem executat la comanda:

```
$ smbpasswd -a -m maquina
```

Un cop executem aquesta comanda, no hauríem de tenir problemes a l'hora d'afegir el client a *Samba*.

10. Creació d'usuaris LDAP

10.1. Manualment

Entre les diferents aplicacions que disposem amb *OpenLDAP*, tenim *ldapadd*. *ldapadd* ens permet afegir usuaris manualment passant-li com a paràmetre un arxiu amb extensió *ldif* on tindrem la informació a afegir a *LDAP*. El format d'arxiu *ldif* (*LDAP Data Interchange Format*) va ser dissenyat i utilitzat per la Universitat de Michigan, és comunament utilitzat també per importar o exportar informació entre diferents servidors *LDAP*, o per descriure un conjunt de canvis globals al nostre directori.

Els fitxers *LDIF* estan basats en una sèrie de registres separats per un separador de línia. Cada registre consisteix en una seqüència de línies que descriuen una entrada al directori *LDAP* o una seqüència de línies que descriuen un conjunt de canvis al directori *LDAP*.

Hem de tenir present que un fitxer *LDIF* pot contenir un conjunt d'entrades o un conjunt de canvis al directori *LDAP*, però no tots dos junts. Hi ha relació entre les operacions de modificació de *LDAP* (*add, delete, modify i modrdn*) i els tipus de opcions per modificar un directori *LDAP* dels arxius *ldif* (també utilitzen *add, delete, modify i modrdn*), aquesta relació és intencionada, ja que permet una modificació del directori molt més ràpida.

Per tal de veure millor com funciona els arxius *LDIF*, crearem a continuació un d'exemple amb dues entrades per afegir al nostre directori *LDAP*:

```
dn: cn=Iván Hidalgo , ou = people , dc=projecte, dc=ldap
```

```
objectclass:top
```

```
objectclass:organizationalPerson
```

```
telephonenumber:93.xxx.xx.xx
```

```
description: Usuari creador del projecte
```

```
cn: Iván Hidalgo
```

```
dn: cn= Susana Crespo , ou= people , dc=projecte,dc=ldap
```

```
objectclass:organizationalPerson
```

```
telephonenumber:93.XXX.XX.XX
```

```
cn: Susana Crespo
```

Com podem veure l'arxiu és molt intuïtiu i només hem de posar en la nomenclatura del servei de directori *LDAP* l'usuari que volem inserir, en el nostre cas, li diem el nom de l'usuari *Iván Hidalgo*, a quina base de cerca el volem afegir (a la base de cerca *ou=people,dc=projecte,dc=ldap*, on tindrem tots els usuaris), de quin tipus d'objecte es tracta (*organitzacional Person*) i més informació addicional que podem afegir (telèfon, *correu electrònic*, *descripció*, *etc...*).

També ens pot ser de ajuda, en el cas que ja continguem usuaris al nostre servei de directori, realitzar una cerca simple amb la comanda:

```
$ Idapsearch -x -b " -s base '(objectclass=*)' namingContexts
```

La sortida d'informació que ens doni aquesta comanda serà en format *LDIF*, per la qual cosa tindrem una bona plantilla per a la creació de nous usuaris.

Un cop tenim creat el nostre fitxer *LDIF*, tan sols hem de cridar la següent comanda per tal que la informació que tenim al fitxer *LDIF* sigui afegida al nostre directori *LDAP* (en el cas que no hi hagi cap tipus d'error a l'hora de crear el fitxer *LDIF*):

```
$ Idapadd -x -D 'dc=projecte,dc=ldap' -w -F arxiu.ldif
```

Un cop fet ja tenim afegida al directori *LDAP* la informació que contenia l'arxiu *LDIF*

10.2. Interfície web

10.2.1. LDAP-Account-Manager

LAM és un frontend web per a l'administració d'usuaris per a comptes *Unix* i *Samba* dins d'un directori *LDAP*. Per tal d'instal·lar *LAM* haurem de tenir instal·lats *php4* i *Apache*, en cas que no fos així a l'hora d'instal·lar *LAM* aquests paquets s'instal·len automàticament.

Per tal de instal·lar el programa executarem la següent comanda:

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

Un cop finalitza la instal·lació ens dedicarem a configurar *LAM*.

El primer pas per a la configuració és l'edició de dos arxius destinats a la configuració, aquests arxius són:

- `/etc/ldap-account-manager/config.cfg` : En aquest arxiu indicarem la clau per administrar els diferents perfils, i el perfil per defecte de *LAM*.
- `/var/lib/ldap-account-manager/config/*.conf` : Els arxius emmagatzemats amb extensió `.conf` corresponen als diferents perfils de *LAM*. Aquests perfils emmagatzemen la informació sota el servidor *LDAP* i les opcions per defecte que s'utilitzaran per gestionar les comptes d'usuari amb *LAM*. No serà necessari modificar el contingut d'aquests arxius ja que es creen i modifiquen fàcilment des de la interfície web.

El següent pas serà accedir a la interfície web de *LAM* amb un navegador web, per fer-ho hem de teclejar la següent *URL* al navegador : <http://projecte.ldap/lam>

Un cop ficada la *URL* al navegador ens sortirà la pantalla principal de *LAM*, tal com veiem a la figura:

LDAP Account Manager

Configuration Login

LAM Login

Enter Username and Password for Account

Username: admin

Password:

Your Language: English (Great Britain)

Login

LDAP server:

Configuration profile: lam lam Change Profile

Al entrar per primer cop a *LAM*, ens farà falta crear un nou perfil adaptat a les necessitats del sistema. Per a fer-ho clicarem sobre el botó *Configuration Login*, que ens donarà la següent pantalla:

LDAP Account Manager

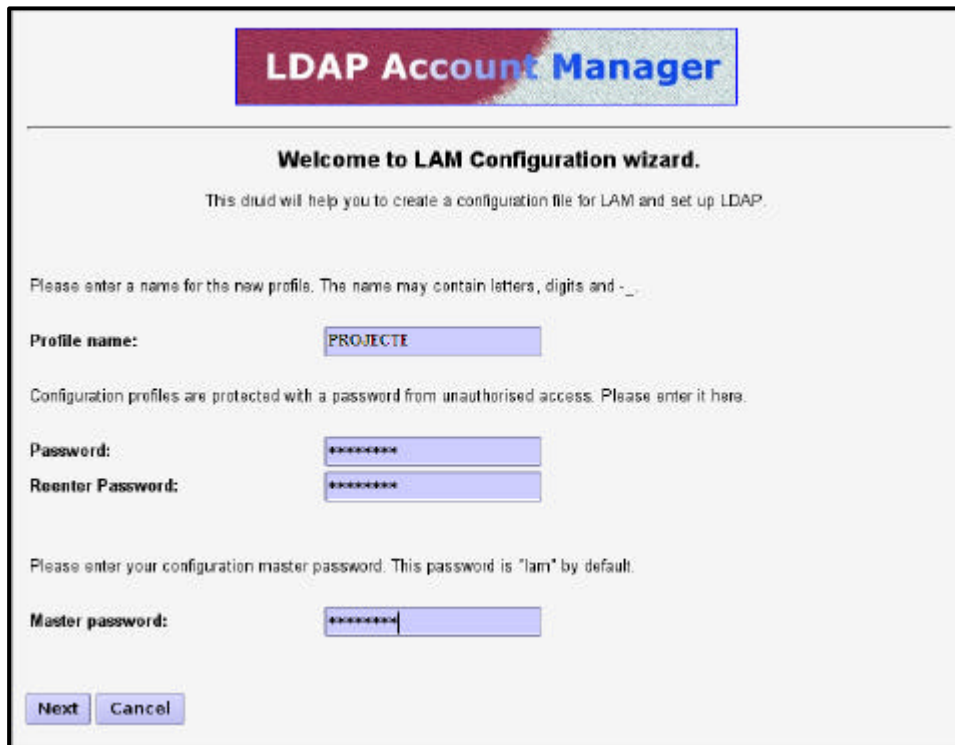
Please enter password to change preferences:

lam Ok Help

Manage profiles Configuration wizard

Back to Login

Seleccionarem l'opció *Configuration Wizard* per crear un nou perfil, un cop clicem l'opció ens sortirà la següent pantalla:

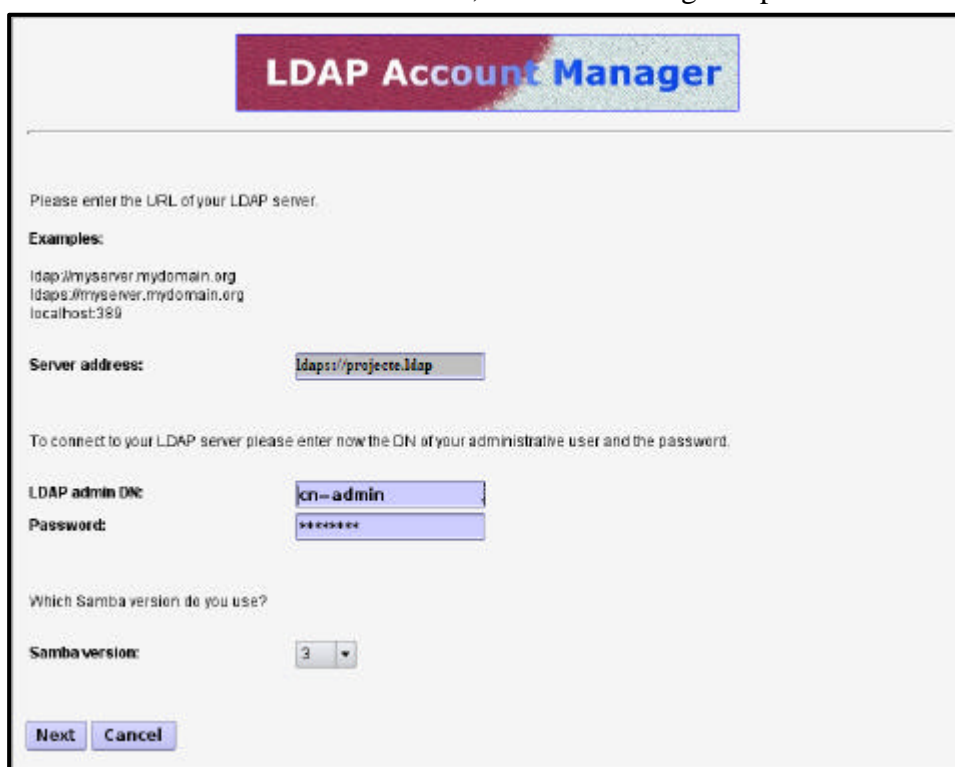


The screenshot shows the 'LDAP Account Manager' configuration wizard. At the top, there is a title bar with the text 'LDAP Account Manager'. Below the title bar, the text reads 'Welcome to LAM Configuration wizard.' followed by 'This wizard will help you to create a configuration file for LAM and set up LDAP.' The main content area contains the following fields and instructions:

- Instruction: 'Please enter a name for the new profile. The name may contain letters, digits and -_.'
- Field: 'Profile name:' with the value 'PROJECTE'.
- Instruction: 'Configuration profiles are protected with a password from unauthorised access. Please enter it here.'
- Field: 'Password:' with masked characters '*****'.
- Field: 'Reenter Password:' with masked characters '*****'.
- Instruction: 'Please enter your configuration master password. This password is "lam" by default.'
- Field: 'Master password:' with masked characters '*****'.

At the bottom left, there are two buttons: 'Next' and 'Cancel'.

Aquí haurem d'indicar el nom que volem posar-li al nostre perfil en el nostre cas li direm *PROJECTE*, i la clau per tal d'accedir a aquest. Tal i com indica la pantalla, a la opció *Master Password* (clau mestra) haurem de posar *lam* que és la clau per defecte de *LAM*, per tal de canviar la clau mestra per defecte, ho haurem de fer des de l'arxiu */etc/ldap-account-manager/config.cfg*, un cop hem respòs a totes les qüestions continuem donant-li al botó *Next*, i anirem a la següent pantalla:



The screenshot shows the next step in the 'LDAP Account Manager' configuration wizard. At the top, there is a title bar with the text 'LDAP Account Manager'. Below the title bar, the text reads 'Please enter the URL of your LDAP server.' followed by 'Examples: ldap://myserver.mydomain.org, ldaps://myserver.mydomain.org, localhost:389'. The main content area contains the following fields and instructions:

- Field: 'Server address:' with the value 'ldaps://projects.lap'.
- Instruction: 'To connect to your LDAP server please enter now the DN of your administrative user and the password.'
- Field: 'LDAP admin DN:' with the value 'cn=admin'.
- Field: 'Password:' with masked characters '*****'.
- Field: 'Which Samba version do you use?' with a dropdown menu showing '3'.

At the bottom left, there are two buttons: 'Next' and 'Cancel'.

Aquesta pantalla està dedicada a la localització del servidor *LDAP* i la versió de *Samba* a utilitzar.

- *Server Adres* : Ens indica l'adreça del nostre servidor *LDAP*, en el nostre cas i ja que tenim configurat *LDAP* i *Samba* de forma segura, li direm que escolti per la interfície *ldaps://projecte.ldap*.
- *LDAP admin dn* : Per tal de connectar-nos a *LDAP*, ens farà falta l'usuari administrador per afegir i modificar valors dins dels servidor de directori *LDAP*.
Com hem vist el nostre usuari administrador és:
cn=admin,dc=projecte,dc=ldap
- Password: Haurem de posar la clau del nostre usuari administrador per tal d'autenticar-nos.

Per finalitzar aquesta pantalla ens demanarà quina versió de *Samba* utilitzarem, en el nostre cas haurem de dir-li la versió 3, que és la que bé per defecte al menú desplegable.

Un cop passem de pantalla *LAM* ens començarà a crear l'estructura de directori *LDAP*, per fer-ho ens demanarà els sufixes a on emmagatzemarà les diferents comptes (usuaris, grups, *hosts*,...). Podem veure a la figura següent la pantalla:

Please enter the suffixes of your LDAP tree where LAM should store the accounts.

User Suffix:

Group Suffix:

Host Suffix:

Domain Suffix:

LAM supports CRYPT, SHA, SSHA, MD5 and SMD5 to generate the hash value of an user password. SSHA and CRYPT are the most common but CRYPT does not support passwords greater than 8 letters. We do not recommend to use plain text passwords.

Password hash type:

LAM caches its LDAP searches, you can set the cache time here. Shorter times will stress LDAP more but decrease the possibility that changes are not identified.

Cache timeout:

Optional settings

Please select here if you want to make additional changes to your configuration profile or if LAM should use default values.

- Ranges for UID and GID numbers
- Attributes in list views
- Language and additional admin users
- Lambdaemon settings and PDF text

Escollim els sufixos *people*, *groups*, *machines* i *domains* respectivament ja que aquests són grups estàndards dins de *LDAP* i ens ho dona automàticament *LAM*, també ens facilitarà la configuració de més aplicacions que utilitzin *Samba*, ja que aquest grups vindran per defecte. A l'hora de posar els sufixos també hem de posar la base de cerca, que en el nostre cas és , *dc=projecte,dc=ldap*.

Per tant els valors del sufixos quedarien de la següent manera:

- **User suffix** = *ou=people,dc=projecte,dc=ldap*
- **Group suffix** = *ou=groups,dc=projecte,dc=ldap*
- **Host suffix** = *ou=groups,dc=projecte,dc=ldap*
- **Domain suffix** = *ou=domain,dc=projecte,dc=ldap*

La següent opció que ens dona aquesta pantalla és escollir el tipus d'algoritme de *hash* a utilitzar per emmagatzemar els claus, en aquest cas escollirem *MD5*.

Les opcions *Caché TimeOut* i *Optional Settings* no les haurem de modificar.

Un cop configurat, i com és la primera vegada que entrem a *LAM*, la següent pantalla ens demanarà de crear els sufixes que anteriorment li hem demanat ja que ell no els troba al servei de directori, li confirmarem que els volem crear i ens donarà pas a la pantalla de creació del domini que s'utilitzarà en *Samba* així com el *SID* del servidor *Samba*.

The screenshot shows the 'LDAP Account Manager' interface. At the top, there is a title bar with the text 'LDAP Account Manager'. Below the title bar, there is a message: 'No domains found, please create one.' The main area is titled 'Domain Settings' and contains several input fields and buttons:

- Domain name:** PROJECTE (with a 'Help' link)
- Domain SID:** 5-1-5-XX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX (with a 'Help' link)
- Next RID (optional):** (with a 'Help' link)
- Next User RID (optional):** (with a 'Help' link)
- Next Group RID (optional):** (with a 'Help' link)
- Algorithmic RID Base:** 1000 (with a 'Help' link)
- Suffix:** ou=domain,dc=projecte,dc=ldap (with a 'Help' link)

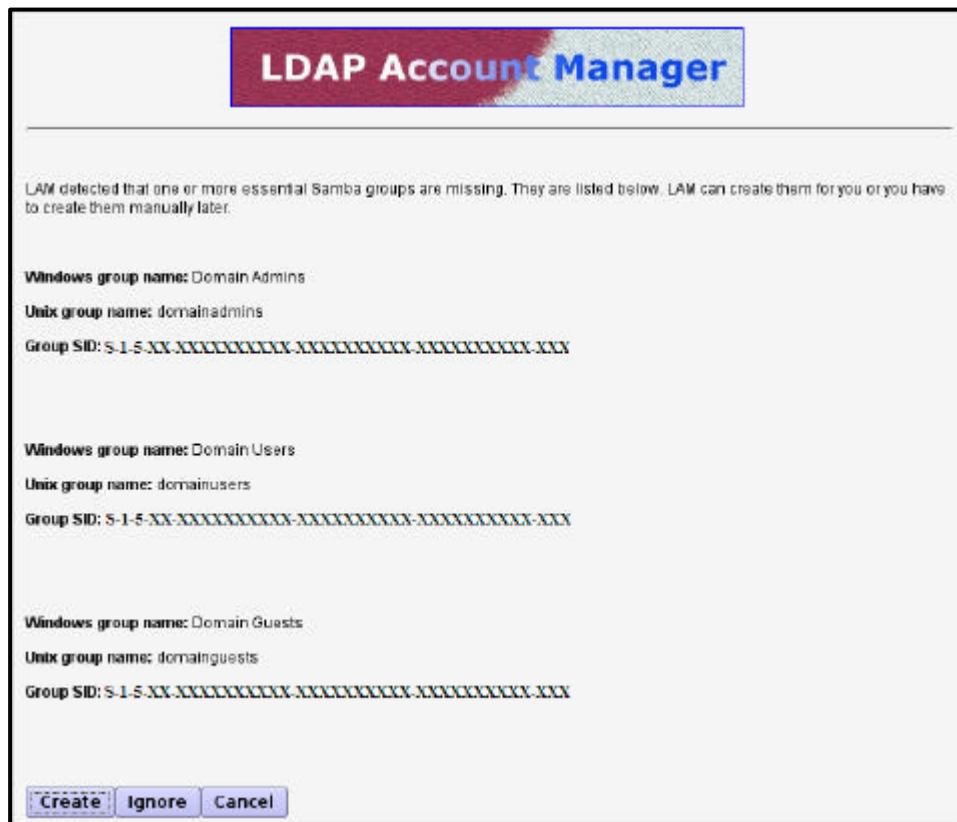
At the bottom of the dialog, there are two buttons: 'Create' and 'Cancel'.

Com a nom de domini li haurem de posar *PROJECTE*, que el varem definir a la configuració de *Samba*. I per obtenir el *SID* del domini executarem la següent comanda al servidor *Samba*:

```
$ net getlocalsid
```

```
SID for domain PROJECTE is: S-1-5-XX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX
```

Un cop tenim les dades posades i continuem, la següent pantalla ens demanarà confirmació per crear una sèrie de grups essencials per a *Samba*. Haurem de crear-los, per fer-ho només hem de cliquejar sobre l'opció *Create*, automàticament ens crearà els grups *Samba*.



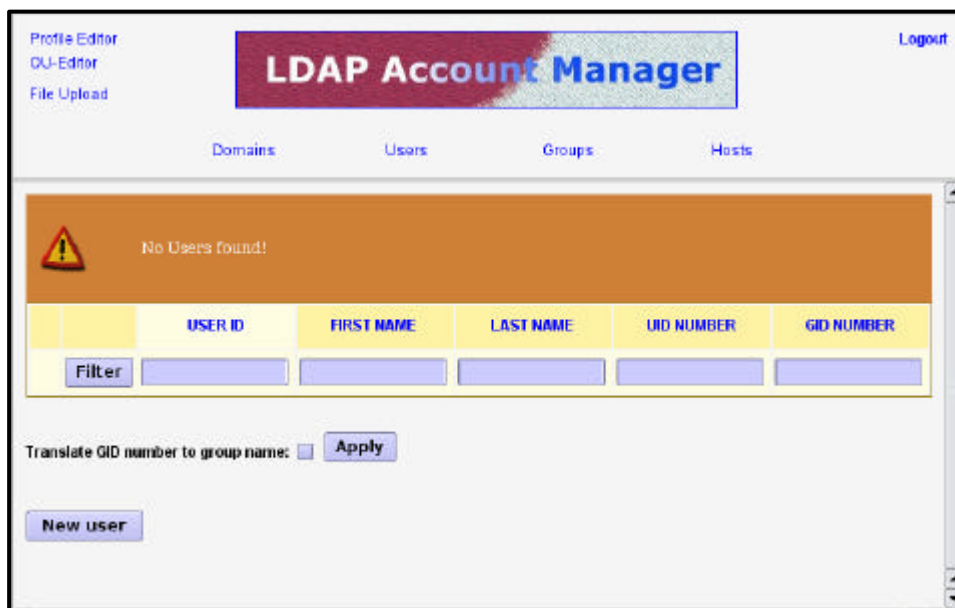
Posteriorment un cop creats els grups, ens sortirà una pantalla mostrant tota la informació que s'ha emmagatzemat al perfil *PROJECTE* que acabem de crear. A continuació regressarem a la pantalla de *Login*.

Com utilitzarem per defecte sempre el perfil creat anteriorment, haurem de canviar la variable default del fitxer de configuració de *LAM /etc/ldap-account-manager/config.cfg* i posar-li el valor *PROJECTE*, del nom del nostre perfil. Així cada cop que entrem a la pantalla de autenticació de *LAM*, ens sortirà el nostre perfil.

Un cop a la pantalla d'autenticació posem la clau de l'usuari administrador de *LDAP* i entrem dins de *LAM*, com podem veure a continuació *LAM* no té una detallada qualitat gràfica, però és una eina molt fàcil de utilitzar, tindrem quatre menú principals per accedir: usuaris, grups, màquines i dominis.

Veurem pas per pas cadascuna d'elles:

Un cop autenticat, ens trobem amb la pantalla d'usuaris, encara que ens diu que no tenim cap usuari creat. També podem entrar al menú d'usuaris clicant sobre el link *User*. Per tal de crear un nou usuari haurem de clicar la opció *New User*.



Un cop entrem a la pantalla de creació de un nou usuari entrem dins de les propietats generals per la creació de l'usuari, però al costat esquerra tenim botons que ens permetran entrar dins de les diferents pantalles de configuració.

La pantalla de configuració general tindria el següent aspecte:

The screenshot shows the LDAP Account Manager web interface. At the top, there are links for 'Profile Editor', 'OU-Editor', and 'File Upload' on the left, and 'Logout' on the right. The main title is 'LDAP Account Manager'. Below the title, there are tabs for 'Domains', 'Users', 'Groups', and 'Hosts'. The 'Users' tab is selected. On the left, there is a 'Please select page:' menu with options: 'General' (selected), 'Unix', 'Samba', 'GnuPG', 'Personal', and 'Final'. The main content area is titled 'General properties' and contains the following fields:

Username*	<input type="text" value="usuari"/>	Help
UID number	<input type="text"/>	Help
First name*	<input type="text" value="Usuari"/>	Help
Last name*	<input type="text" value="Prora"/>	Help
Primary group*	<input type="text" value="domainusers"/>	Help
Additional groups	<input type="button" value="Edit groups"/>	Help
Home directory*	<input type="text" value="/home/samba/users/\$user"/>	Help
Gecos	<input type="text" value="Usuari de Prora"/>	Help
Login shell*	<input type="text" value="/bin/bash"/>	Help
Suffix	<input type="text" value="ou=people,dc=projecte,dc=ldap"/>	Help

Values with * are required

At the bottom, there is a 'Load profile' section with a dropdown menu set to 'default', a 'Load Profile' button, and a 'Help' link.

Els valors que ens demana són els següents:

- *Username* : Nom del nou usuari
- *UID* : Identificador de l'usuari, no fa falta que ho posem *LAM* s'encarregarà automàticament.
- *First Name* , *LastName* : Nom i cognom real de l'usuari.
- *Primary Group* : Indiquem a quin grup volem que pertanyi l'usuari. Ens donarà a escollir entre els tres grups anteriorment creats, *Domain Users* , *Domain Admins* i *Domain Guest*.
- *Additional Groups*: Podem fer que l'usuari pertanyi a més d'un grup.
- *Home directory* : Directori on tindrà el *home* l'usuari, com podem veure utilitzem la *home* creada per *Samba* */home/samba/users* i amb la variable *\$users* li diem de quin usuari es tracta.
- *Gecos* : Descripció de l'usuari.
- *Login shell* : Shell que utilitzarà l'usuari.
- *Suffix* : Sufix a on emmagatzemarem l'usuari, sempre ha de ser el sufix *ou=people* a on emmagatzemarem els usuaris.

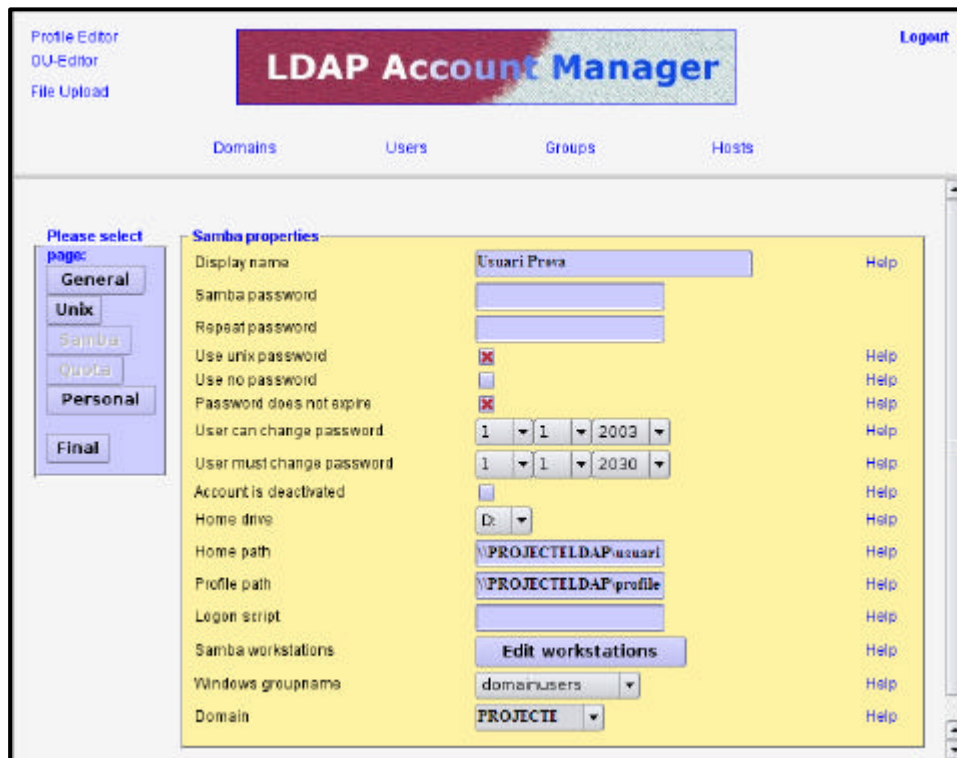
Per continuar haurem de clicar el botó *Unix*, però abans d'accedir *LAM* ens informa que ha completat automàticament el valor *UID*, clicarem de nou sobre *Unix*, per entrar al menú d'opcions *Unix* per l'usuari que estem creant, que tindrà el següent aspecte:

The screenshot shows the LDAP Account Manager web interface. At the top, there are navigation links: Profile Editor, OU-Editor, File Upload, and Logout. The main title is "LDAP Account Manager". Below the title, there are tabs for Domains, Users, Groups, and Hosts. The "Users" tab is selected. On the left, there is a "Please select page:" menu with buttons for General, Unix, Samba, Quota, Personal, and Final. The "Unix properties" section is highlighted in yellow and contains the following fields and options:

Property	Value	Help
Password	*****	Generate password
Repeat password	*****	
Use no password	<input type="checkbox"/>	Help
Password warn	10	Help
Password expire	10	Help
Maximum password age	365	Help
Minimum password age	1	Help
Expire date	31 / 12 / 2030	Help
Account deactivated	<input type="checkbox"/>	Help

Values with * are required

En aquesta pantalla haurem de posar la clau de l'usuari, les altres opcions que ens dona el menú de propietats *Unix* les haurem de deixar amb el valor per defecte que dona *LAM*. Un cop posada la clau a l'opció Password i tornar-la a posar a Repeat Password, per comprovar que no hi hagi cap error al escriure la clau, li donarem al botó *Samba*, per tal d'anar a la pantalla de propietats *Samba* de l'usuari, que tindrà l'aspecte de la figura que tenim a continuació.



Les opcions que ens demana LAM seran les següents:

- *Display Name* : Nom que li sortirà a l'usuari *Samba* a l'hora d'autenticar-se.
- *Samba Password*: No haurem de posar cap clau ja que activarem la opció *Use unix password* que agafarà la clau anteriorment entrada a la pantalla de configuració d'*Unix*. La clau mai expirarà i l'usuari podrà canviar-la sempre, però haurà de fer-ho obligatòriament a partir de la data que nosaltres fixem.
- L'opció *Account is deactivated* ha d'estar desactivada.
- *Home Drive* : Serà la lletra que assignarem a *Windows* de la nostra *home*.
- *Home path* : Ruta on tenim la nostra *home*, aquí no podem posar la notació de directoris i haurem de posar la notació *Windows* pels recursos compartits. És a dir, en el nostre cas, posarem [\\PROJECTELDAP%user](#) per tal de que agafi el nom de l'usuari.
- *Profile path*: Ruta on tenim els perfils mòbils dels usuaris, en aquest pas la connotació serà igual que a l'opció *Home path*. Per tal de que l'usuari pugui carregar els seus perfils mòbils, escriurem [\\PROJECTELDAP\profiles%user](#) per tal que vagi a la carpeta on guardem els perfils de l'usuari.

- *Logon script* : Podem dir-li un cop s'ha autenticat executi un *script* d'inici de sessió. Tal i com hem vist quan hem configurat *Samba*, això és possible gràcies al recurs *netlogon*. En el nostre cas, no precisem d'aquesta opció.
- *Samba Workstation*: Aquest botó és molt important, amb aquest botó li estem dient al servidor *Samba* amb qui estableix una relació de confiança l'usuari. Només a aquelles màquines que estiguin acceptades dintre de la opció *Samba WorkStations* , serà on l'usuari es podrà autenticar.
- *Windows groupname* : Ens dona a escollir entre els diferents grups creats anteriorment, haurem d'escollir el millor per cada usuari, tenint present les restriccions de seguretat d'alguns grups.
- *Domain* : Domini del nostre servidor *Samba*, en el nostre cas, i com ja sabem, es tractarà de *PROJECTE*.

Un cop tenim totes les opcions de *Samba* correctament, pitjarem sobre el botó *Personal*, al fer-ho ens sortirà la següent pantalla:

The screenshot shows the LDAP Account Manager web interface. At the top, there is a navigation bar with links for 'Profile Editor', 'OU-Editor', and 'File Upload' on the left, and 'Logout' on the right. The main title is 'LDAP Account Manager'. Below the title, there are tabs for 'Domains', 'Users', 'Groups', and 'Hosts'. The 'Users' tab is selected. On the left side, there is a 'Please select page:' menu with buttons for 'General', 'Unix', 'Samba', 'Quota', 'Personal', and 'Final'. The 'Personal' button is highlighted. The main content area is titled 'Personal properties' and contains a form with the following fields: Title (filled with 'Usuari de Prova'), Employee type, Street, Postal code, Postal address, Telephone number, Mobile number, Fax number, and eMail address. Each field has a 'Help' link next to it.

Com podem veure a aquesta pantalla podem inserir molta informació personal del nostre usuari, des de l'email fins al carrer. Cap dels camps són obligatoris, de tal manera que podem passar a l'últim pas de creació d'usuari. Per fer-ho, pitjarem sobre el botó *Final*, al donar-li ens sortirà la pantalla que trobem a continuació.



En aquest punt només ens farà falta donar-li al botó *Create Account* per tal de crear l'usuari. Un cop creat i sense cap error, si entrem al menú *Users*, l'usuari creat ens sortirà com a un usuari del directori *LDAP*.

Els menús de *Domains*, *Groups* i *Hosts* no faran falta tocar-los, degut a que anteriorment, al configurar *LAM*, ja hem creat el domini, i els grups (*LAM* crea automàticament els grups) automàticament. Al menú *Hosts* apareixeran les màquines al crear la relació de confiança a *Samba* per la línia de comandes amb la instrucció:

```
$ smbpasswd -a -m màquina.
```

Per tal de crear un altre usuari haurem de seguir els mateixos punts, variant en les opcions escollides.

10.2.2 phpLDAPadmin

Com hem vist *LDAP-Account-Manager* és una eina d'administració web dels usuaris *LDAP* molt senzilla i còmoda, però a vegades i depenen del tipus de xarxa, pot no arribar a tenir totes les opcions necessàries que ens pot aportar *LDAP*. Per aquest tipus de xarxes on busquem més opcions de configuració dels usuaris, utilitzarem *phpLDAPadmin*.

Per tal d'instal·lar *phpLDAPadmin* al nostre sistema, haurem d'executar la comanda:

```
$ apt-get install phpLDAPadmin
```

Una altra opció d'instal·lació seria descarregar-se de la pàgina del projecte *phpLDAPadmin*, <http://phpldapadmin.sourceforge.net>.

A partir d'ara veurem els passos necessaris per a configurar *phpLDAPadmin*.

Primer de tot haurem d'adaptar l'arxiu de configuració *config.php* que trobem dins del directori */var/www/phpldapadmin* al nostre directori *LDAP*, per fer-ho editarem l'arxiu i modificarem algunes entrades, les entrades a modificar són les següents:

```
$servers[$i]['name'] = 'PROJECTE';  
    /* A convenient name that will appear in  
    the tree viewer and throughout phpLDAPadmin to  
    identify this LDAP server to users. */  
$servers[$i]['host'] = 'projecte.ldap';  
$servers[$i]['base'] = 'dc=projecte,dc=ldap';  
$servers[$i]['port'] = 636;  
$servers[$i]['auth_type'] = 'session';  
$servers[$i]['login_dn'] = 'cn=admin,dc=projecte,dc=ldap';  
$servers[$i]['login_pass'] = '';  
$servers[$i]['tls'] = true;  
$servers[$i]['default_hash'] = 'md5';  
$servers[$i]['login_attr'] = 'dn';
```

Com podem veure haurem de dir-li on es troba el servei de directori *LDAP*, la base de cerca, el port a on hem d'escoltar que serà el port que utilitza *LDAP* de forma segura, i l'administrador del servei de directori *LDAP*.

Un altres dels arxius a modificar el tindrem al directori `/var/www/phpldapadmin/templates/template_config.php`, a aquest arxiu modificarem alguns aspectes de la configuració de *Samba* i la forma d'afegir els comptes d'usuari al sistema. Les línies a modificar dintre d'aquest arxiu són les següents::

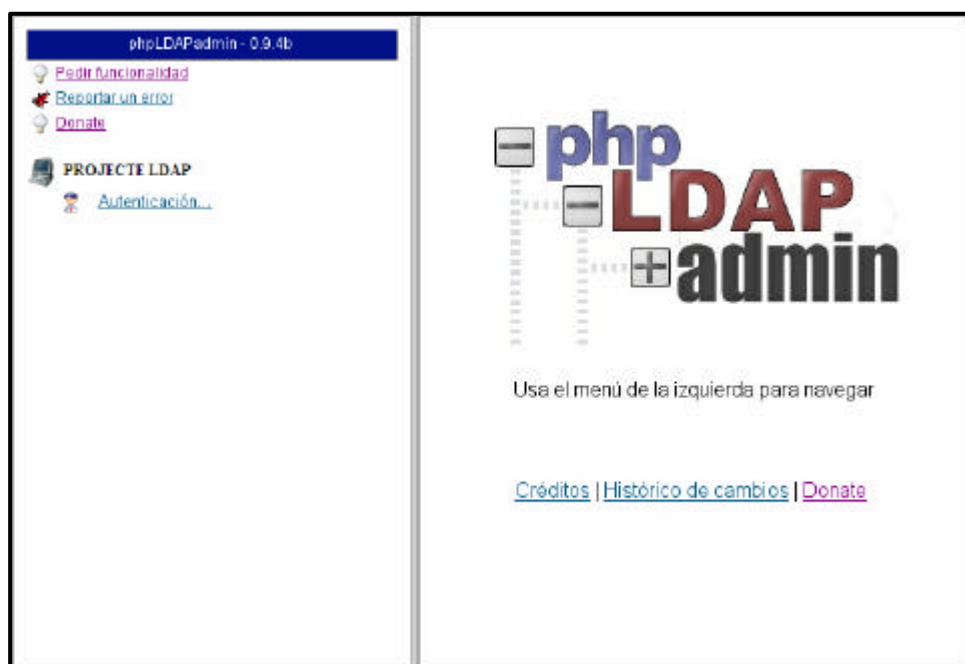
```
$base_posix_groups="ou=groups,dc=projecte,dc=ldap";  
$mkntpwdCommand = "/usr/local/sbin/mkntpwd";  
$default_samba3_domains[] =  
array( 'name' => 'PROJECTE',  
       'sid' => 'S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX' );  
$samba_base_groups = "ou=groups,dc=projecte,dc=ldap";  
$built_in_local_groups = array( "SID" => "Domain Admins",  
                                "SID" => "Domain Users",  
                                "SID" => "Domain Guests",
```

Podem veure que hem de modificar la base de cerca dels grups que tenim al nostre directori *LDAP*, ja que amb la configuració per defecte no estava correctament. També hem canviat el nom del nostre domi *Samba*, així com els grups que utilitza *Samba*.

Un cop realitzades les modificacions anteriors , ja podem accedir a l'aplicació, per fer-ho haurem de teclejar la següent *URL* al nostre navegador web:

<http://projecte.ldap/phpldapadmin>

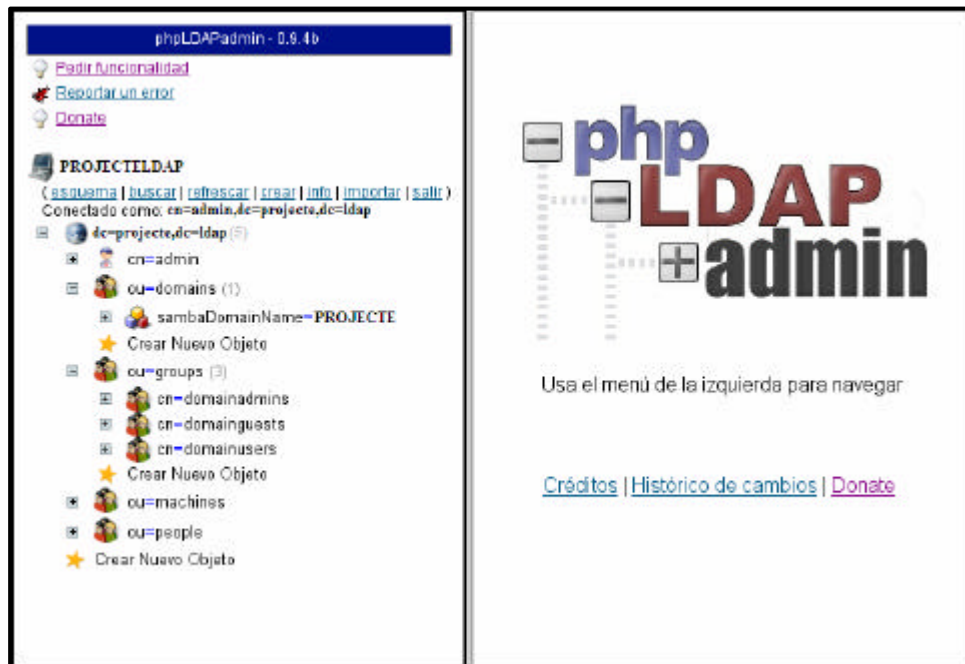
La pantalla principal de *phpLDAPadmin* té el següent aspecte:



Per tal d'autenticar-nos li donarem al link *Autenticación* que ens ofereix l'eina *phpLDAPadmin*. Un cop a la pantalla d'autenticació, ens demanarà l'usuari administrador (com ja sabem es tracta de *cn=admin,dc=projecte,dc=ldap*) i la clau. Si totes dues opcions estan correctes entrarem a la següent pantalla de *phpLDAPadmin*.

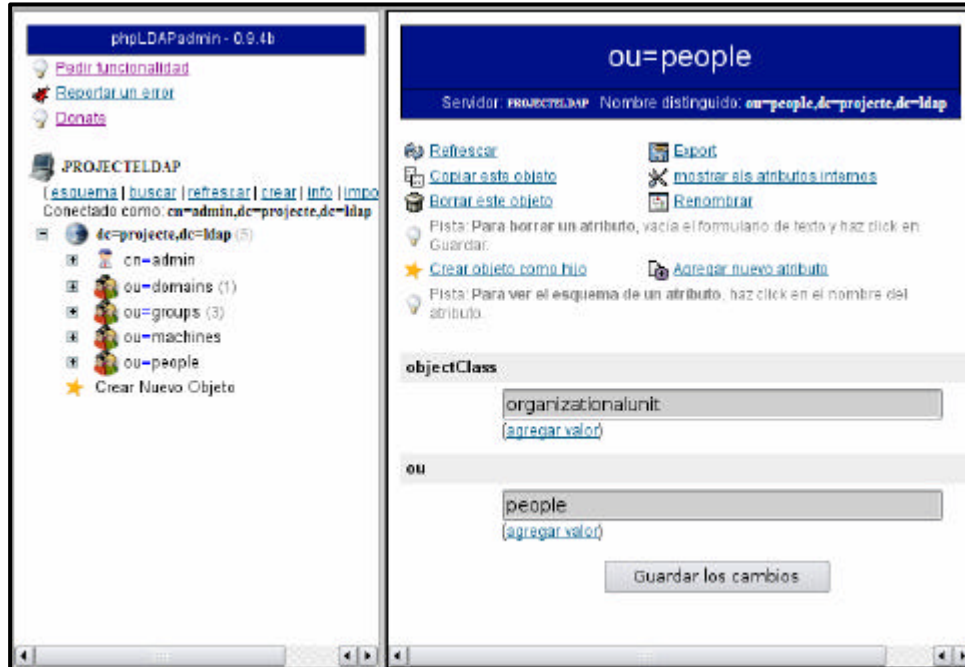
Un cop dins de *phpLDAPadmin*, l'aplicació ens dona una sèrie d'eines per la administració d'un directori *LDAP*. Aquestes comprenen des de el llistat dels esquemes disponibles al servidor *LDAP*, cerques, creació de noves entrades, informació sobre el servidor i fins i tot la possibilitat d'importar arxius *LDIF*. Com veiem les funcionalitats de *phpLDAPadmin* són molt més abundants que les de *LAM*.

A la següent pantalla podem veure el nostre arbre de directori *LDAP*, amb els grups i el domini que varem crear anteriorment amb l'eina *LAM*.



Si polsem sobre el signe + que tenim al costat de cada objecte, podem veure els objectes que depenen d'aquest, així com el número que tenim entre parèntesis al costat de cada branca principal ens indica la quantitat d'objectes dependents que té cada branca.

Si polsem sobre el nom d'un objecte, per exemple, sobre la unitat d'organitzacions *ou=people*, podem veure la informació emmagatzemada dins d'aquesta branca del nostre directori *LDAP*, així com procedir a la seva modificació, com podem veure a la següent pantalla:



phpLDAPadmin també dona la possibilitat de crear una sèrie d'objectes predefinits, ajudant a l'hora d'administrar un servidor *LDAP*. Aquesta pantalla podem observar tots aquells objectes per als que *phpLDAPadmin* té plantilles.



Com podem veure a través d'aquestes plantilles podem crear tot tipus d'usuari i màquines. Per crear un usuari *Samba*, només haurem de seleccionar *Samba 3 User* donar-li al botó *Proceed* i anar seguint una interfície molt intuïtiva de creació d'usuari, a on ens donarem compte de tot el potencial i atributs que pot arribar a tenir un usuari del servei *LDAP*. Podem afegir des de el nostre e-mail fins a imatges *JPEG* de l'usuari. *phpLDAPadmin* automatitzarà aquelles opcions que li sigui possible facilitant-nos encara més el treball d'administració i creació d'un servidor *LDAP*.

Un cop hem finalitzat d'utilitzar *phpLDAPadmin*, haurem desconnectar-nos, per fer-ho pitjarem el link *Salir*.

Un cop donat, ens sortirà la pantalla de desconnexió, en cas de que no hagués cap tipus d'error podem tancar la finestra del navegador web.

11. CUPS

Com hem vist *CUPS* és un sistema d'impressió que permet la impressió en xarxa. A partir d'ara veurem com fer l'instal·lació i configuració de *CUPS*.

L'objectiu al qual volem arribar amb aquest sistema d'impressió, és subministrar un mecanisme per a que els clients puguin imprimir, estiguin on estiguin, i utilitzant el sistema operatiu que sigui.

El clients *Unix* no tindran problemes alhora de aconseguir aquest objectiu gràcies al protocol *IPP*, que funciona sobre *CUPS*. Per una altra banda, els clients amb sistemes operatius podran imprimir gracies a la integració de *CUPS* amb *Samba*.

11.1. Instal·lació

La selecció dels paquets a instal·lar, per aconseguir que el sistema d'impressió *CUPS* funcioni, s'efectuarà, observant la descripció del paquet *cupsys*. A partir de les dependències, suggeriments i recomanacions d'aquest paquet, es seleccionaran els paquets més adequats i importants per a aconseguir l'objectiu final del projecte.

En el nostre cas, que tenim impressores definides, instal·larem la majoria dels paquets de controladors d'impressores, en cas contrari podríem fer una selecció dels paquets a instal·lar.

A continuació veurem els diferents paquets a instal·lar per tal de posar en marxa el nostre sistema d'impressió, els paquets són:

- *cupsys*: paquet que ens instal·larà el servidor CUPS.
- *cupsys-client*: Administració d'impressores pels clients CUPS
- *cupsys-bsd*: Instal·lació del backend BSD per interactuar amb CUPS
- *cupsys-driver-gimpprint*.
- *foomatic-bin*.
- *cupomatic-ppd*.
- *Gsfonts*: Fonts per a interprets GhostScript.

- *gs-esp*: Instal·la GhostScript per tal de poder utilitzar l'impressió PostScript.
- *psfontmgr*: Administrador de fonts PostScript que fa ús de l'aplicació Defoma.
- *kdeprint*: Subsistema d'impressió de KDE, farem ús d'aquest per configurar CUPS.
- *gimpprint-locales*.
- *foomatic-db-gimp-print*.
- *foomatic-filters-ppds*: Instal·lació de filtres

A aquesta llista haurem de sumar també el paquet *cups-pdf* que no és més que una impressora *PDF* virtual, tot el treball d'impressió que processi el convertirà a *PDF*. Aquesta impressora serà la utilitzada per fer proves ja que no disposem d'una impressora real.

Un cop tenim presents tots els paquets necessaris, procedirem a instal·lar aquests al nostre sistema, per realitzar l'instal·lació dels paquets executarem aquesta comanda:

```
$ apt-get install cupsys cupsys-client cupsys-bsd \
cupsys-driver-gimpprint foomatic-bin \
cupsomatic-ppd gsfonts psfontmgr \
kdeprint gimpprint-locales \
foomatic-db-gimp-print \
foomatic-filters-ppds
```

Un cop instal·lats, ens sortirà la primera pantalla de configuració de *Debian* per configurar el filtre d'impressió *foomatic* (paquet *foomatic-filters-ppds*).

foomatic permet la creació d'un arxiu de log, sobre el que escriurà tots els informes de depuració. La creació d'aquest arxiu suposa un risc de seguretat al sistema per lo qual no es recomana tenir-ho, *Debian* ens preguntarà si el volem crear, en el nostre cas respondrem que no.

Després la configuració dels filtres d'impressió de *foomatic* ens demanarà quina comanda utilitzarem per convertir els arxius de text a *PostScript*, ens dona la opció de que el propi programa ho agafi automàticament, i aquesta serà la opció que li donarem.

Després ens demanarà l'interpret de *GhostScript* que utilitzarà *foomatic*, entre les diferents alternatives que ens dona, haurem d'escollir *gs*. Si en qualsevol instant volem canviar aquest interpret només haurem d'executar la funció :

\$ *update-alternatives* -config *gs*.

Ens demanarà posteriorment si volem crear quotes d'impressió, per tal que els usuaris no puguin imprimir més d'un cert número de pàgines , però aquest no és l'objectiu del projecte, així que li respondrem negativament

En *IPP* tots els treballs d'impressió tenen un tipus *MIME*. Donat que no totes les fonts assignen correctament algun tipus *MIME*, molts arriben amb el tipus *application/octet-stream* , quan *CUPS* rep un treball amb aquest tipus *MIME* intenta endevinar el seu format, sinó ho aconsegueix el rebutja. És possible fer que *CUPS* faci que tots els treballs no reconeguts amb aquest tipus *MIME* siguin treballs *en brut*, és a dir que s'enviaran directament a la impressora sense processar.

Si rebem treballs d'impressió des de sistemes *Windows* haurem activar aquesta opció ja que *Windows* dona als treballs d'impressió *IPP* el format *application/octet-stream*. La pantalla de configuració actual ens demanarà si volem que *CUPS* imprimeixi *en brut* , en el nostre cas haurem de respondre afirmativament.

Un cop configurat el paquet *foomatic-filters-ppds* , la següent pantalla en donarà l'opció de configurar el paquet *cupsys*. La pantalla de configuració de *cupsys* ens demanarà quins backends utilitzarà *CUPS*, haurem de seleccionar els *backends ipp, lpd, parallel, socket i usb* per poder suportar la majoria de connexions d'impressores.

Posteriorment ens sortirà la pantalla de configuració de *cupsys-bsd*, ens demanarà si volem instal·lar un servidor que accepti treballs d'impressió al estil *BSD*, respondrem afirmativament a aquesta qüestió, ja que al implementar *CUPS* a la xarxa de la universitat tindrem impressores que enviïn treballs d'impressió serveis *BSD*.

Un cop fetes aquestes instal·lacions ja podem dir que tenim instal·lat el nostre sistema d'impressió *CUPS* amb la configuració bàsica, només ens faltaria instal·lar el paquet *cups-pdf*, que instal·larà al nostre sistema un nou *backend*, a partir del qual podem crear impressores virtuals que convertiran els treballs d'impressió en arxius *PDF*. Per tal d'instal·lar el paquet *cupsys-pdf*, executarem la següent comanda:

```
$ apt-get install cups-pdf
```

Un cop instal·lat, només ens faltirà reiniciar el servidor *CUPS* per tal que el nou *backend* estigui disponible al sistema. Per reiniciar el servidor *CUPS* executarem:

```
$ /etc/init.d/cupsys restart  
Restarting printing system service: cupsd.
```

11.2. Configuració

Per començar la configuració del nostre servidor *CUPS*, començarem realitzant una sèrie de comprovacions al sistema relacionades amb *Samba*. Després configurarem alguns aspectes necessaris per la integració de *CUPS* en *LDAP*, la interactuació amb clients *Windows*, etc.

Primer de tot comprovarem que *Samba* ha estat compilat amb suport per a *CUPS*, aquesta comprovació es realitzarà amb la comanda *ldd*, que ens mostra les llibreries compartides que utilitza el dimoni *smbd*, en aquest cas. Si entre aquestes llibreries trobem la de *CUPS*, vol dir que *Samba* ha estat compilat amb suport per *CUPS*.

Per fer la comprovació executarem:

```
$ ldd `which smbd` | grep "cups"  
libcups.so.2 => /usr/lib/libcups.so.2 (0x40129000)
```

Podem comprovar que *Samba* ha estat compilat amb suport *CUPS*, el següent pas serà el reinici del nostre servidor *Samba* per a comprovar que ja no tenim l'error que donava el log del dimoni *smbd* a l'hora de configurar *Samba* (podem trobar l'error a la pàgina 102 del nostre projecte), per fer-ho editarem l'arxiu */var/log/samba/log.smbd* i comprovem que ja no dona aquests errors.

```
[2005/06/15 13:32:20, 0] smbd/server.c:main(757)
```

```
smbd version 3.0.4-Debian started.
```

```
Copyright Andrew Tridgell and the Samba Team 1992-2005
```

Per tal que *CUPS* pugui utilitzar usuaris emmagatzemats al nostre directori *LDAP*, haurem de afegir l'arxiu *cupsys* al directori d'aplicacions que utilitzen *PAM*. Per tal de portar a terme aquesta opció haurem crear l'arxiu *cupsys* al directori */etc/pam.d/* del clients, de tal forma que cridi als arxius *common-auth* i *common-session* que havíem creat anteriorment.

L'arxiu */etc/pam.d/cupsys* quedaria de la següent forma

```
@include common-auth
```

```
@include common-account
```

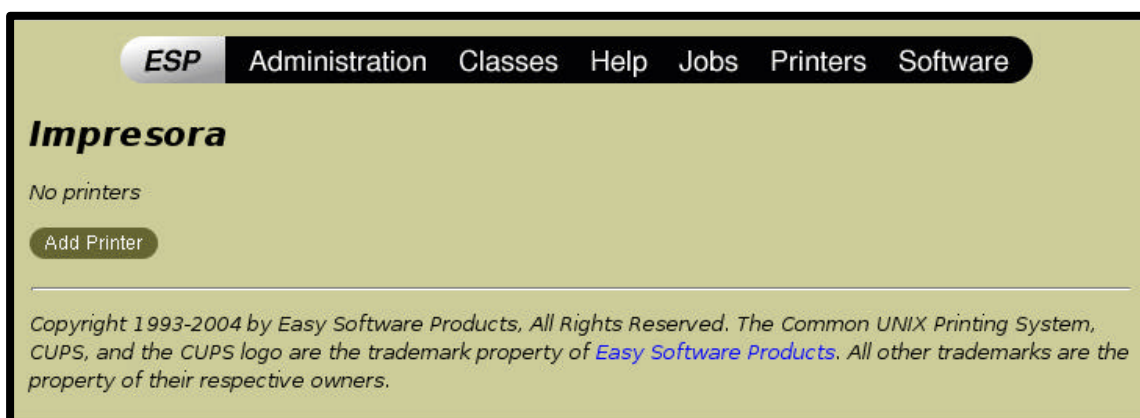
Un cop realitzats aquests canvis ja podem dir que *CUPS* està preparat per actuar conjuntament amb *LDAP* i *Samba*. A continuació veurem com instal·lar impressores en clients *Windows* i *Linux*.

11.3. Instal·lació d'impressores en xarxa

Per tal d'instal·lar les impressores utilitzarem l'interface d'administració web de *CUPS*. Per tal de poder entrar a la interface web de *CUPS*, haurem entrar a un navegador web i posar la següent adreça: <http://projecte.ldap:631> (recordem que *projecte.ldap* és l'adreça on tenim el nostre servidor *LDAP* i *Samba*), això ens carregarà la pàgina principal de l'administrador. La pàgina principal té el següent aspecte:



Un cop dins, si clicquem l'opció **Manage Printers**, no ens donarà cap resultat ja que en aquets moment no tenim cap impressora instal·lada al nostre sistema d'impressió, tal com veiem a la figura:



Per tal d'afegir una nova impressora seleccionarem l'opció *Add Printer*

Per tal de continuar *CUPS* ens demanarà un usuari i clau que pugui accedir al sistema, els usuaris no haurien de poder instal·lar impressores en la nostra xarxa, només l'administrador del sistema d'impressió. L'usuari administrador és *root*. Un cop posat l'usuari i la clau correctament, *CUPS* ens mostrarà la següent pantalla per poder afegir l'impressora. Aquesta pantalla ens demanarà el nom que li volem donar a l'impressora, la seva localització i una descripció breu. Per nosaltres, l'impressora que instal·larem s'anomenarà *LaserColor*, a la següent figura veiem com fer-ho:

ESP Administration Classes Help Jobs Printers Software

Admin

Add New Printer

Name:

Location:

Description:

Copyright 1993-2004 by Easy Software Products, All Rights Reserved. The Common UNIX Printing System, CUPS, and the CUPS logo are the trademark property of Easy Software Products. All other trademarks are the property of their respective owners.

Un cop tenim tota la informació prosseguirem instal·lant l'impressora donant-li al botó *Continue*. La següent pantalla ens demanarà el tipus de dispositiu d'impressió que instal·larem. Escollirem l'opció *Virtual Printer (PDF Printer)* del menú desplegable, per tal de crear la nostra impressora virtual *PDF*.

ESP Administration Classes Help Jobs Printers Software

Admin

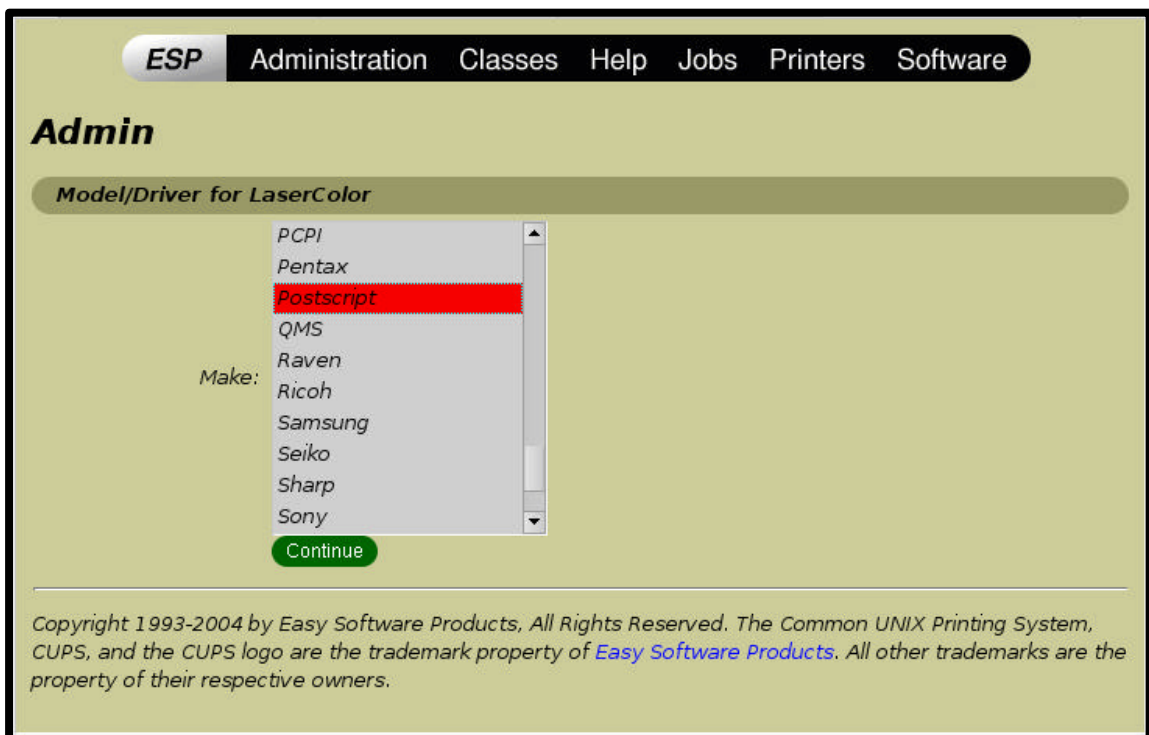
Device for LaserColor

Device:

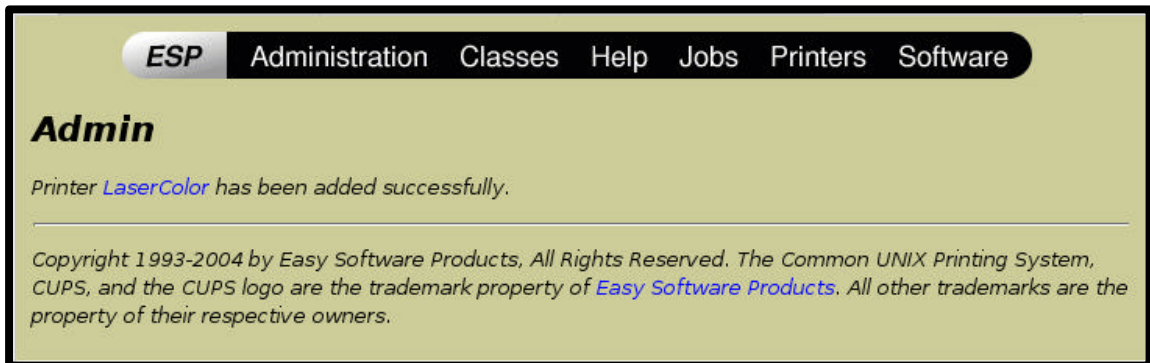
- USB Printer #9
- USB Printer #10
- USB Printer #11
- USB Printer #12
- USB Printer #13
- USB Printer #14
- USB Printer #15
- USB Printer #16
- Virtual Printer (PDF Printer)**
- Windows Printer via SAMBA

Copyright 1993-2004 by Easy Software Products, All Rights Reserved. The Common UNIX Printing System, CUPS, and the CUPS logo are the trademark property of Easy Software Products. All other trademarks are the property of their respective owners.

Un cop escollit, prenem el botó *Continue*, la següent pantalla ens demanarà el model d'impressora que instal·larem, en el nostre cas, seleccionem l'opció *PostScript* i pitjarem el botó *Continue*.



La següent pantalla ens informará que la nostra impressora s'ha instal·lat correctament.



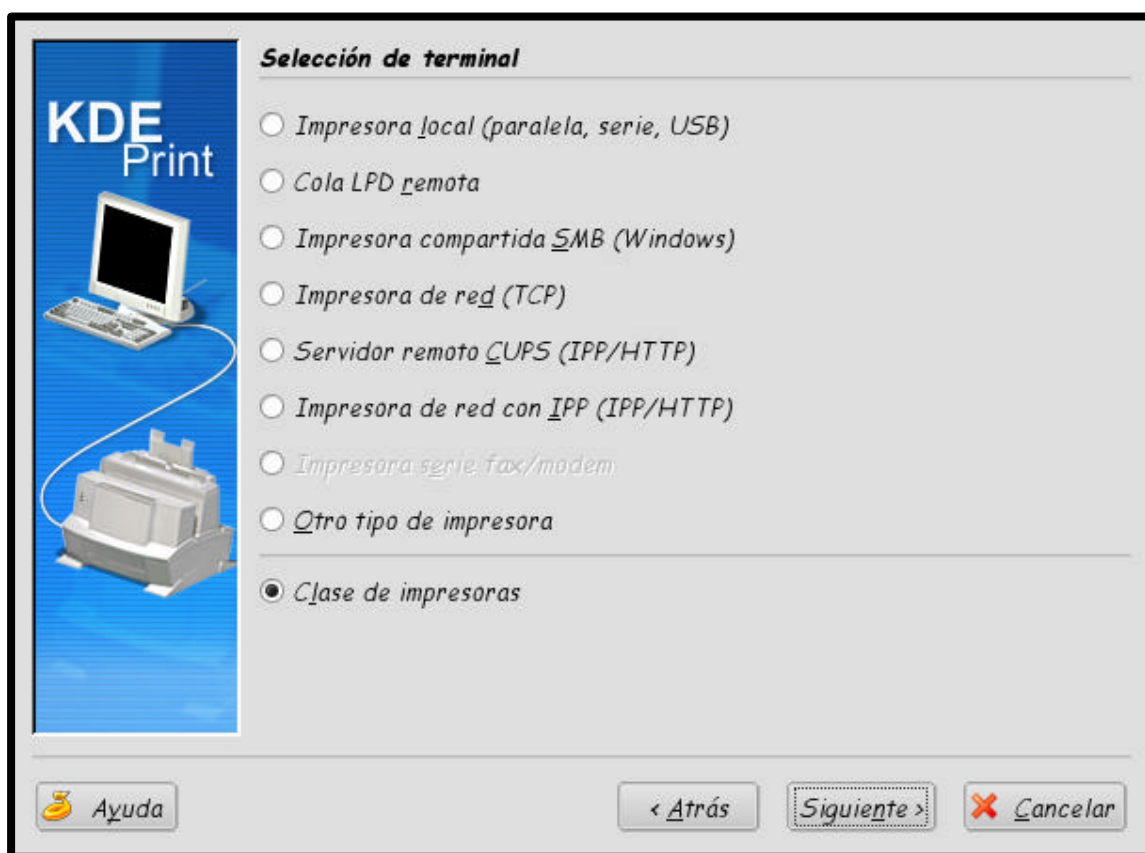
Si cliquem al link *LaserColor*, ens mostrarà una descripció de la impressora instal·lada tal com veiem a la següent figura:



11.3.1. Instal·lació a sistemes operatius Linux

Per tal de veure com podem instal·lar una impressora compartida a un client *Linux*, utilitzarem una altre interfície gràfica que suporta el sistema d'impressió de *CUPS*, es tracta de l'administrador d'impressió de *KDE*, que hem instal·lat prèviament, gràcies al paquet *kdeprinter*.

Un cop dins de l'administrador d'impressió, li donarem a l'opció d'afegir impressora, un cop donat ens sortirà l'assistent d'impressió de *KDE*, amb una interfície molt intuïtiva, ens donarà l'opció d'instal·lar tot tipus d'impressores, tal com veiem a la figura:



Per tal d'instal·lar l'impressora creada al servidor *CUPS*, haurem de escollir l'opció *Impresora de red (TCP)*, un cop escollit li donem a *Següent* i ens sortirà la pantalla per cercar les impressores de la nostra xarxa. En aquest moment, podem inserir l'adreça de la nostra impressora o cercar-la per més comoditat. Escollirem l'opció per cercar-la, i com a resultat ens sortirà la nostra impressora *LaserColor*, la escollirem i anirem continuant donant a *Següent* fins que finalitzi l'assistent.

Un cop finalitzat l'assistent ja tenim al client instal·lat la impressora en xarxa.

11.3.2 Instal·lació a sistemes operatius Windows

Com hem comentat anteriorment *CUPS* no dona suport, directament, als clients *Windows*, per això haurem d'utilitzar *Samba*. La forma de fer-ho és compartint les impressores gestionades per *CUPS* a *Samba*.

A continuació veurem com exportar els controladors d'impressió a equips *Windows*. Els controladors s'emmagatzemen a la instal·lació de *CUPS*, i es comparteixen, via *Samba*, amb els clients *Windows*. Per realitzar aquesta tasca utilitzarem l'eina *cupsaddsmbd* que ens ofereix *CUPS*.

cupsaddsmbd mou els controladors d'impressió al recurs *Samba* [*print\$*]. Hem de recordar que els clients sempre esperen tenir els controladors emmagatzemats a aquest recurs, al qual accediran al moment de fer l'instal·lació de les impressores.

cupsaddsmbd facilita la compartició de qualsevol impressora *CUPS* instal·lada al sistema.

Per tal de que els usuaris de *Windows* tinguin els controladors necessaris per la instal·lació de la nostra impressora, haurem tenir els controladors *PostScript* de *Adobe* o els controladors *PostScript* de *CUPS* per a *Windows NT/2000/XP*.

Els controladors d'impressió de *CUPS* els podem obtenir de la seva pàgina web www.CUPS.org. El nom del paquet es denomina *CUPS-samba-[version].tar.gz*, en el nostre cas la versió que disposem serà la 5.0rc3

Actualment els controladors de *CUPS* només accepten clients *Windows NT/2000/XP*, per als clients de *Windows 95, 98, Me* hauran d'utilitzar els controladors d'*Adobe*. En el nostre cas, totes les màquines *Windows* tindran versions avançades, ja sigui *Windows 2000* o *XP*.

Abans de poder exportar els controladors d'impressió, aquest s'han d'ubicar al directori */usr/share/CUPS/drivers/*.

Un cop tenim el nostre paquet *CUPS-samba-5.0rc3.tar.gz* descarregat al directori */tmp* procedirem a descomprimir-ho amb la comanda

```
$ tar -xvzf /tmp/CUPS-samba-5.0rc3.tar.gz -C /tmp
CUPS-samba.install
CUPS-samba.license
CUPS-samba.readme
CUPS-samba.remove
CUPS-samba.ss
```

El paquet de controladors *CUPS* per a sistemes *Windows* disposa de l'script d'instal·lació *CUPS-samba.install*, però no l'utilitzarem ja que el procés d'instal·lació d'aquests controladors és molt senzill.

L'arxiu *CUPS-samba.ss* no és més que un arxiu *tar* a on tenim els controladors. Per tant desempaquetarem l'arxiu al directori */usr/share/CUPS/drivers*, on hem dit abans que haurem ubicar els drivers. Si el directori no està creat el crearem. Executant les següents comandes podrem crear el directori i desempaquetar l'arxiu.

```
$ mkdir -m 755 /usr/share/CUPS/drivers/
$ tar xvf /tmp/CUPS-samba.ss -C /
/usr/share/CUPS/drivers/cups5.hlp
/bin/tar: Removing leading `/' from member names
/usr/share/CUPS/drivers/cupsdrv5.dll
/usr/share/CUPS/drivers/cupsui5.dll
```

A partir d'aquest moment ja tenim disponibles els controladors *PostScript* de *CUPS* per *Windows NT/2000/XP*, ara només ens quedarà exportar-los a *Samba* amb l'eina *cupsaddsmb*.

Si li passem com paràmetre a `cupsaddsmb` l'opció `-a` li direm que ens afegixi totes les impressores que tenim al sistema a *Samba*, com nosaltres només en tenim instal·lada una, li passarem aquesta opció. Per tal d'executar `cupsaddsmb` escriurem:

```
$ cupsaddsmb -U root -a
```

```
Password for root required to access localhost via SAMBA: [Clau]
```

Que tindrà la següent sortida:

```
Running command: smbclient //localhost/print/$ -N -U'root%1' \
```

```
-c 'mkdir W32X86;put /var/tmp/40d05d9b3e1a0 W32X86/LaserColor.ppd;put \
/usr/share/CUPS/drivers/cupsdrv5.dll \
W32X86/cupsdrv5.dll;put \
/usr/share/CUPS/drivers/cupsui5.dll \
W32X86/cupsui5.dll;put \
/usr/share/CUPS/drivers/cups5.hlp \
W32X86/cups5.hlp'
```

```
Domain=[PROJECTE] OS=[Unix] Server=[SAMBA-LDAP]
```

```
NT_STATUS_OBJECT_NAME_COLLISION making remote directory W32X86
```

```
putting file /var/tmp/40d05d9b3e1a0 as W32X86/LaserColor.ppd \
```

```
(1309,5 kb/s) (average 1309,6 kb/s)
```

```
putting file /usr/share/CUPS/drivers/cupsdrv5.dll as W32X86/cupsdrv5.dll \
```

```
(2709,9 kb/s) (average 2631,4 kb/s)
```

```
putting file /usr/share/CUPS/drivers/cupsui5.dll as W32X86/cupsui5.dll \
```

```
(2614,6 kb/s) (average 2624,1 kb/s)
```

```
putting file /usr/share/CUPS/drivers/cups5.hlp as W32X86/cups5.hlp \
```

```
(3475,0 kb/s) (average 2641,7 kb/s)
```

```
Running command: rpcclient localhost -N -U'root%1' \
```

```
-c 'adddriver "Windows NT x86" \
"LaserColor:cupsdrv5.dll:LaserColor.ppd:\
cupsui5.dll:cups5.hlp:NULL:RAW:NULL"
```

Printer Driver LaserColor successfully installed.

```
Running command: rpcclient localhost -N -U'root%1' \
```

```
-c 'setdriver LaserColor LaserColor'
```

Successfully set LaserColor to driver LaserColor.

Com podem veure, li passem amb el paràmetre `-U` un usuari administrador del sistema d'impressió, en el nostre cas `root`, i `cupsaddsmb` ens demanarà la clau. Un cop posada correctament la clau `cupsaddsmb` procedirà a exportar els controladors d'impressió. Un cop exportats i si no hem tingut cap tipus d'error, comprovarem que la nostra impressora estan presents a *Samba*, per fer-ho executarem l'eina `smbclient` amb passant-li com a paràmetre qualsevol usuari que tinguem al sistema, per fer-ho escriurem a la nostre `shell`:

```
$ smbclient -L PROJECTELDAP -U usuari
Password: [Clau]
Domain=[PROJECTE] OS=[Unix] Server=[SAMBA-LDAP]
  Sharename      Type      Comment
  -----      ---      -
  netlogon       Disk      Network Logon Service
  print$         Disk      Printer Drivers
  tmp            Disk      Temporal
  cdrom          Disk      Samba server's CD-ROM
  IPC$           IPC       IPC Service (SAMBA-LDAP PDC server)
  ADMIN$         IPC       IPC Service (SAMBA-LDAP PDC server)
  LaserColor     Printer   Impresora Laser a Color
  usuari         Disk      Home Directories
```

```
Domain=[PROJECTE] OS=[Unix] Server=[Samba 3.0.4-Debian]
```

```
  Server          Comment
  -----          -
  PROJECTELDAP    SAMBA-LDAP

  Workgroup       Master
  -----          -
  PROJECTE        PROJECTELDAP
```

Com podem apreciar, la nostra impressora *LaserColor*, surt com a un recurs compartit de *Samba*, per tant podem dir que el sistema ja està preparat per a que els clients *Windows* puguin fer ús de les impressores administrades per *CUPS* a sistemes *Unix*.

Per tal d'instal·lar l'impressora en xarxa a *Windows*, haurem cridar a l'assistent per agregar impressores, dir-li que volem instal·lar una impressora de xarxa i cercar l'impressora o donar-li la ruta per tal de procedir amb la seva instal·lació. Un cop cercada o definida la ruta, *Windows* instal·larà l'impressora amb els controladors que varem exportar amb l'eina *cupsaddsmb*.

12. Temps implantació Sistemes LDAP-Samba-CUPS

Aquest projecte ha intentat ser un guia per la integració de les tecnologies *OpenLDAP*, *Samba* i *CUPS*, per la construcció d'una xarxa heterogènia, en la qual cada client, independentment del Sistema Operatiu que disposi, pugui bàsicament, autenticar-se , accedir a la seva *home* i imprimir documents.

La integració de les tecnologies *OpenLDAP*, *Samba* i *CUPS*, la seva instal·lació i configuració requereix molt de temps per tal de realitzar-la per primer cop.

En el nostre cas, hem estat instal·lant, configurant i redactant el projecte durant aproximadament un any. Durant el transcurs del projecte hem tingut diversos problemes a l'hora de configurar *LDAP* i *Samba*, en alguns casos aquests problemes ens a fet invertir molt de temps, i fins i tot, ens ha calgut refer el projecte des de el principi.

Aquest projecte vol ser la base per integrar els diferents Sistemes Operatius que utilitzem a la nostra universitat, facilitant a l'alumne el seu treball i permetent que aquest tingui el seu propi espai per emmagatzemar informació independentment del sistema operatiu que estigui utilitzant, i que pugui autenticar-se als sistemes operatius *Microsoft* amb el mateix nom d'usuari utilitzat a *Linux*.

Seguint pas a pas aquest projecte per la realització d'una xarxa heterogènia, en un espai de temps de dos dies, podríem tenir actuant *LDAP* com el nostre servidor de directori, *Samba* com a controlador primari de la xarxa per a clients *Microsoft*, i *CUPS* com a servidor d'impressió. Hem de tenir en compte que a més de la configuració i instal·lació dels diferents servidors, hem de crear els diferents usuaris, o fer una migració dels usuaris que ja teníem a l'anterior servidor configurat amb *NIS*, mitjançant les eines *MigrationTools*, màquines que puguin accedir al servidor , etc.

La instal·lació i configuració en cada client, no ens comportarà invertir més de dues hores. I fins i tot, en el cas que programem diferents *scripts* per facilitar la configuració i instal·lació, el temps d'implementació és pot reduir notablement.

Cal tenir en compte que a la nostra universitat els sistemes operatius *Windows* estan gestionats per *Novell*. Dins del nostre projecte no hem tingut en compte els sistemes operatius gestionats per aquesta eina degut a que no hem tingut la possibilitat de comprovar el seu comportament amb *LDAP* per no tenir accés al sistema Novell utilitzat a la universitat. Tot i això, podem trobar a Internet diferents documents que verifiquen la integració del servei de directori *LDAP* amb *Novell*.

La implementació total d'aquest projecte en una xarxa com pot ser la de la nostra universitat, no comportaria invertir més d'una setmana de temps.

13. Annexos

13.1. Fitxer implementació servidor Samba-LDAP

- Arxiu de configuració /etc/ldap/slapd.conf:

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.
# Schema and objectClass definitions
include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
include      /etc/ldap/schema/nis.schema
include      /etc/ldap/schema/inetorgperson.schema
include     /etc/ldap/schema/samba.schema
# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck  on
# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile      /var/run/slapd/slapd.pid
# List of arguments that were passed to the server
argsfile     /var/run/slapd.args
# Read slapd.conf(5) for possible values
loglevel     0
# Where the dynamically loaded modules are stored
modulepath   /usr/lib/ldap
moduleload   back_ldbm
#####
# Specific Backend Directives for ldbm:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend     ldbm
#####
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
#backend     <other>
#####
# Specific Directives for database #1, of type ldbm:
# Database specific directives apply to this database until another
# 'database' directive occurs
```



```

database      ldbm
# The base of your directory in database #1
suffix       "dc=projecte,dc=ldap"
# Where the database file are physically stored for database #1
directory      "/var/lib/ldap"
# Indexing options for database #1
#index        objectClass eq
index sambaSID  eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq
index objectClass,uid,uidNumber,gidNumber,memberUid eq
index cn,mail,surname,givenname eq,subinitial
# Save the time that the entry gets modified, for database #1
lastmod       on
# Where to store the replica logs for database #1
# relogfile   /var/lib/ldap/repllog
# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attrs=userPassword by dn.regex="cn=admin,dc=projecte,dc=ldap" write by anonymous
auth by self write by * none
# Ensure read access to the base for things like
# supportedSASLMechanisms. Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read
# The admin dn has full write access, everyone else
# can read everything.
access to * by dn.regex="cn=admin,dc=projecte,dc=ldap" write by * read
access to attrs=sambaLMPassword,sambaNTPassword by
dn.regex="cn=admin,dc=projecte,dc=ldap" write by * none
# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to

```

```
#access to dn="*.*,ou=Roaming,o=morsnet"
#   by dn="cn=admin,dc=projecte,dc=ldap" write
#   by dnattr=owner write
#####
# Specific Directives for database #2, of type 'other' (can be ldbm too):
# Database specific directives apply to this database until another
# 'database' directive occurs
#database    <other>
# The base of your directory for database #2
#suffix      "dc=debian,dc=org"
```

- Arxiu de configuració /etc/ldap/ldap.conf:

```
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.9 2000/09/04 19:57:01 kurt Exp $
# LDAP Defaults
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
HOST XXX.XXX.XXX
BASE dc=projecte,dc=ldap
rootbinddn cn=admin,dc=projecte,dc=ldap
PORT 636
ssl no
#SIZELIMIT 12
#TIMELIMIT 15
#DEREF never
```

- Arxiu de configuració /etc/default/slapd

```
# Default location of the slapd.conf file
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="slapd"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="slapd"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.conf)
SLAPD_PIDFILE=

# Configure if the slurpd daemon should be started. Possible values:
# - yes: Always start slurpd
# - no: Never start slurpd
# - auto: Start slurpd if a replica option is found in slapd.conf (default)
SLURPD_START=auto

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
SLAPD_SERVICES="ldap://projecte.ldap:389/"

# Additional options to pass to slapd and slurpd
SLAPD_OPTIONS=""
SLURPD_OPTIONS=""
```

- Arxiu de configuració /etc/samba/smb.conf:

```
===== Global Settings =====  
[global]  
# Change this to the workgroup/NT-domain name your Samba server will part of  
workgroup = PROJECTE  
netbios name = PROJECTELDAP  
# server string is the equivalent of the NT Description field  
server string = SAMBA-LDAP  
# Windows Internet Name Serving Support Section:  
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server  
wins support = yes  
# This will prevent nmbd to search for NetBIOS names through DNS.  
dns proxy = no  
# What naming service and in what order should we use to resolve host names  
# to IP addresses  
name resolve order = lmhosts host wins bcast  
##### Debugging/Accounting #####  
# This tells Samba to use a separate log file for each machine  
# that connects  
log file = /var/log/samba/log.%m  
# Put a capping on the size of the log files (in Kb).  
max log size = 1000  
# If you want Samba to only log through syslog then set the following  
# parameter to 'yes'.  
; syslog only = no  
# We want Samba to log a minimum amount of information to syslog. Everything  
# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log  
# through syslog you should set the following parameter to something higher.  
syslog = 0  
# Do something sensible when Samba crashes: mail the admin a backtrace  
panic action = /usr/share/samba/panic-action %d  
##### Authentication #####  
# "security = user" is always a good idea. This will require a Unix account  
# in this server for every user accessing the server. See  
# /usr/share/doc/samba-doc/htmldocs/ServerType.html in the samba-doc  
# package for details.
```

```

security = user
os level = 34
local master = yes
preferred master = yes
domain master = yes
domain logons = yes
logon path = \\%L\profiles\%u
logon drive = F:
logon home = \\%L\%u\profile
logon script = netlogon.bat
# You may wish to use password encryption. See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
encrypt passwords = true
# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
passdb backend = ldapsam:ldap://projecte.ldap/
# obey pam restrictions = yes
;guest account = guest
;invalid users = root
# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
unix password sync = yes
;username map = /etc/samba/smbusers
# For Unix password sync to work on a Debian GNU/Linux system, the following
# parameters must be set (thanks to Augustin Luton <aluton@hybrigenics.fr> for
# sending the correct chat script for the passwd program in Debian Potato).
passwd program = /usr/sbin/smbldap-passwd -u %u
passwd chat = *Enter\snewsUNIX\spassword:* %n\n *Rtype\snewsUNIX\spassword:* %n\n .
# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
; pam password change = no
ldap admin dn = cn=admin,dc=projecte,dc=ldap
ldap ssl = off
ldap delete dn = no
ldap suffix = ou=people,dc=projecte,dc=ldap
ldap machine suffix = ou=machines
ldap user suffix = ou=people
ldap group suffix = ou=groups

```

ldap idmap suffix = ou=people

;ldap domain suffix = ou=domains

Printing

If you want to automatically load your printer list rather

than setting them up individually then you'll need this

load printers = yes

lpr(ng) printing. You may wish to override the location of the

printcap file

; printing = bsd

; printcap name = /etc/printcap

CUPS printing. See also the cupsaddsmb(8) manpage in the

cupsys-client package.

printing = CUPS

printcap name = CUPS

When using [print\$], root is implicitly a 'printer admin', but you can

also give this right to other users to add drivers and set printer

properties

printer admin = @domainprintoperators

File sharing

Name mangling options

; preserve case = yes

; short preserve case = yes

Misc

Using the following line enables you to customise your configuration

on a per machine basis. The %m gets replaced with the netbios name

of the machine that is connecting

; include = /home/samba/etc/smb.conf.%m

Most people will find that this option gives better performance.

See smb.conf(5) and /usr/share/doc/samba-doc/html/docs/speed.html

for details

You may want to add the following on a Linux system:

SO_RCVBUF=8192 SO_SNDBUF=8192

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

```
# The following parameter is useful only if you have the linpopup package
# installed. The samba maintainer and the linpopup maintainer are
# working to ease installation and configuration of linpopup and samba.
; message command = /bin/sh -c '/usr/bin/linpopup "%f" "%m" %s; rm %s' &
```

```
# Domain Master specifies Samba to be the Domain Master Browser. If this
# machine will be configured as a BDC (a secondary logon server), you
# must set this to 'no'; otherwise, the default behavior is recommended.
;domain master = yes
```

```
# Some defaults for winbind (make sure you're not using the ranges
# for something else.)
```

```
idmap uid = 10000-20000
```

```
idmap gid = 10000-20000
```

```
add user script = /usr/sbin/smbldap-useradd -m %u
```

```
template shell = /bin/bash
```

```
#===== Share Definitions =====
```

[homes]

```
comment = Home Directories
```

```
path = /home/samba/users/%u
```

```
;read only = no
```

```
browseable = yes
```

```
writeable = yes
```

```
create mask = 0700
```

```
directory mask = 0700
```

```
# By default, the home directories are exported read-only. Change next
# parameter to 'yes' if you want to be able to write to them.
```

```
# writable = no
```

```
# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
```

```
# create mask = 0700
```

```
# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
```

```
# directory mask = 0700
```


*# Un-comment the following and create the netlogon directory for Domain Logons
(you need to configure Samba to act as a domain controller too.)*

[netlogon]

*comment = Network Logon Service
path = /home/samba/netlogon
;guest ok = yes
;public = no
writable = no
time server = yes
;browseable = no
write list = @domainadmins
;share modes = no*

[profiles]

*path = /home/samba/profiles
writeable = yes
;read only = no
create mask = 0600
directory mask = 0700
browseable = no
;guest ok = yes
;profile acls = yes
;csc policy = yes
;force user = %U*

[printers]

*# comment = All Printers
browseable = no
#path = /tmp
path = /var/spool/samba
printable = yes
; public = no
writable = no
create mask = 0700
use client driver = no
printer admin = root, @domainprintoperators
guest ok = no
; printable = yes
Windows clients look for this share name as a source of downloadable*

```
# printer drivers
write list = root, @domainprintoperators
```

[print\$]

```
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# Replace 'ntadmin' with the name of the group your admin users are
# members of.
write list = root, @domainadmins
```

```
# A sample share for sharing your CD-ROM with others.
```

[tmp]

```
comment = Temporal
writeable = yes
path = /tmp
guest ok = no
```

[cdrom]

```
comment = Samba server's CD-ROM
writable = no
locking = no
path = /cdrom
public = yes
guest ok = yes
# The next two parameters show how to auto-mount a CD-ROM when the
# cdrom share is accessed. For this to work /etc/fstab must contain
# an entry like this:
# /dev/scd0 /cdrom iso9660 defaults,noauto,ro,user 0 0
# The CD-ROM gets unmounted automatically after the connection to the
#
# If you don't want to use auto-mounting/unmounting make sure the CD
# is mounted on /cdrom
#
; preexec = /bin/mount /cdrom
; postexec = /bin/umount /cdrom
```

```

- Arxiu de configuració /etc/libnss-ldap.conf:
###DEBCONF###
# the configuration of this file will be done by debconf as long as the
# first line of the file says '###DEBCONF###'
#
# you should use dpkg-reconfigure libnss-ldap to configure this file.
#
# @(#) $Id: ldap.conf,v 2.35 2005/03/03 21:06:34 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# PADL Software
# http://www.padl.com
#

# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).

host XXX.XXX.XXX.XXX

# The distinguished name of the search base.
base dc=projecte,dc=ldap
# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
uri ldap://projecte.ldap/
#uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.

```

```

# The credentials to bind with.
# Optional: default is no credential.
# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=projecte,dc=ldap
#rootbinddn cn=admin

# The port.
# Optional: default is 389.
port 389

nss_base_passwd ou=people,dc=projecte,dc=ldap?one
nss_base_shadow ou=people,dc=projecte,dc=ldap?one
nss_base_group ou=groups,dc=projecte,dc=ldap?one

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
ssl no
# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is "no"
tls_checkpeer no
# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
# Client certificate and key
# Use these, if your server requires client authentication.

```

- Arxiu de configuració: /etc/pam_ldap.conf:

host XXX.XXX.XXX.XXX

The distinguished name of the search base.

base dc=projecte,dc=ldap

Another way to specify your LDAP server is to provide an

uri with the server name. This allows to use

Unix Domain Sockets to connect to a local LDAP Server.

uri ldap://projecte.ldap/

The LDAP version to use (defaults to 3

if supported by client library)

ldap_version 3

The distinguished name to bind to the server with

if the effective user ID is root. Password is

stored in /etc/ldap.secret (mode 600)

rootbinddn cn=admin,dc=projecte,dc=ldap

The port.

Optional: default is 389.

port 389

nss_base_passwd ou=people,dc=projecte,dc=ldap?one

nss_base_shadow ou=people,dc=projecte,dc=ldap?one

nss_base_group ou=group,dc=projecte,dc=ldap?one

OpenLDAP SSL mechanism

start_tls mechanism uses the normal LDAP port, LDAPS typically 636

ssl start_tls

ssl off

OpenLDAP SSL options

Require and verify server certificate (yes/no)

Default is "no"

tls_checkpeer yes

CA certificates for server certificate verification

At least one of these are required if tls_checkpeer is "yes"

tls_cacertfile /etc/ldap/ssl/cacert.pem

tls_cacertdir /etc/ssl/certs

Seed the PRNG if /dev/urandom is not provided

tls_randfile /var/run/egd-pool

SSL cipher suite

See man ciphers for syntax

- Arxiu de configuració /etc/nsswitch.conf:

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

```
passwd:      compat ldap
group:       compat ldap
shadow:     compat ldap
```

```
hosts:      files ldap dns
networks:   files
```

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

```
netgroup:   nis
```

- Arxiu de configuració /etc/nscd.conf:

```
# /etc/nscd.conf
# An example Name Service Cache config file. This file is needed by nscd.
# Legal entries are:
# logfile          <file>
# debug-level     <level>
# threads         <#threads to use>
# server-user     <user to run server as instead of root>
#   server-user is ignored if nscd is started with -S parameters
# stat-user       <user who is allowed to request statistics>
# enable-cache    <service> <yes|no>
# positive-time-to-live <service> <time in seconds>
# negative-time-to-live <service> <time in seconds>
# suggested-size  <service> <prime number>
# check-files     <service> <yes|no>
# Currently supported cache names (services): passwd, group, hosts
# logfile        /var/log/nscd.log
# threads        6
# server-user    nobody
# stat-user      somebody
# debug-level    0
# enable-cache   passwd    yes
# positive-time-to-live passwd    600
# negative-time-to-live passwd    20
# suggested-size passwd    211
# check-files    passwd    yes
# enable-cache   group     yes
# positive-time-to-live group    3600
# negative-time-to-live group    60
# suggested-size group     211
# check-files    group     yes
# enable-cache   hosts     yes
# positive-time-to-live hosts    3600
# negative-time-to-live hosts    20
# suggested-size hosts     211
# check-files    hosts     yes
```

13.2. Fitxer implementació servidor Samba-LDAP Segur

Per tal de no ampliar desmesuradament el nostre projecte, els següents arxius per la implementació del servidor Samba-LDAP en mode segur, només tindrem en compte, aquells registres que han estat modificats en relació amb els arxius de configuració per l'implementació del servidor Samba-LDAP que podem veure al punt 13.1 del nostre projecte.

- Arxiu de configuració /etc/ldap/slapd.conf:

```
TLSCipherSuite HIGH:MEDIUM:+SSLv2  
TLSCACertificateFile /etc/ldap/ssl/cacert.pem  
TLSCACertificatePath /etc/ldap/ssl/  
TLSCertificateFile /etc/ldap/ssl/servercrt.pem  
TLSCertificateKeyFile /etc/ldap/ssl/serverkey.pem  
TLSVerifyClient never
```

- Arxiu de configuració /etc/ldap/ldap.conf:

```
PORT 636  
ssl yes  
TLS_CACERT /etc/ldap/ssl/cacert.pem  
TLS_KEY /etc/ldap/ssl/serverkey.pem  
TLS_REQCERT demand
```

- Arxiu de configuració /etc/default/slapd

```
SLAPD_SERVICES="ldaps://projecte.ldap:636/"
```

- Arxiu de configuració /etc/samba/smb.conf:

```
passdb backend = ldapsam:ldaps://projecte.ldap/  
ldap ssl = on
```


- Arxiu de configuració /etc/libnss-ldap.conf:

```
uri ldaps://projecte.ldap/  
port 636  
ssl yes  
tls_checkpeer yes  
tls_cacertfile /etc/ldap/ssl/cacert.pem  
tls_ciphers HIGH:MEDIUM:+SSLv2  
tls_cert /etc/ldap/ssl/servercrt.pem  
tls_key /etc/ldap/ssl/serverkey.pem
```

- Arxiu de configuració: /etc/pam_ldap.conf:

```
uri ldaps://projecte.ldap/  
port 636  
ssl on  
tls_ciphers HIGH:MEDIUM:+SSLv2  
tls_cert /etc/ldap/ssl/servercrt.pem  
tls_key /etc/ldap/ssl/serverkey.pem
```

14. Bibliografia

Documentació sobre LDAP

Using OpenLDAP For Authentication, Vincent Danen, 18/06/2002.

- <http://www.mandrakesecure.net/en/docs/ldap-auth.php>

Using OpenLDAP For Authentication; Revision 2, Vincent Danen, 06/05/2003.

- <http://www.mandrakesecure.net/en/docs/ldap-auth2.php>

Security with LDAP, Andrew Findlay.

- <http://www.skills-1st.co.uk/papers/security-with-ldap-jan-2002/security-with-ldap.html>

LDAPv3, Turbo Fredriksson, 04/11/2003, 2001.

- <http://www.bayour.com/LDAPv3-HOWTO.html>

The SLAPD and SLURPD Administrators Guide, Tim Howes, Mark Smith, Gordon Good, Lance Sloan, Steve Rothwell, 30/04/1996, 1992-1996.

- <http://www.umich.edu/~dirsvcs/ldap/doc/guides/slapd/>

System Authentication using LDAP, Brad Marshall.

- http://quark.humbug.org.au/publications/system_auth/sage-au/system_auth.html

LDAP Authentication for Linux, metaconsultancy, 2002.

- <http://www.metaconsultancy.com/whitepapers/ldap-linux.htm>

OpenLDAP 2.2 Administrator's Guide, The OpenLDAP Project, 31/12/2003, 2004.

- <http://www.openldap.org/doc/admin22/>

OpenLDAP Faq-O-Matic, The OpenLDAP Project, 2004.

- <http://www.openldap.org/faq/index.cgi?file=1>

OpenLDAP Faq-O-Matic How do I use TLS/SSL, The OpenLDAP Project, 2004

- <http://www.openldap.org/faq/data/cache/185.html>

Instalación y configuración de OpenLDAP, Jesús Roncero, 30/05/2002.

- <http://bulmalug.net/body.phtml?nIdNoticia=1343>

Autenticación de un cliente linux a través de LDAP, Jesús Roncero, 13/06/2002.

- <http://bulmalug.net/body.phtml?nIdNoticia=1371>

OpenLDAP SSL/TLS How-To, D. Kent Soper, 05/06/2003.

- http://www.openldap.org/pub/ksoper/OpenLDAP_TLS_howto.html

LDAP Implementation HOWTO, Roel van Meer, Giuseppe Lo Biondo, 30/03/2001, 2001.

- <http://www.tldp.org/HOWTO/LDAP-Implementation-HOWTO/>

Documentació sobre Samba

Cómo configurar SAMBA, Joel Barrios Dueñas, 1999, 2000, 2001, 2002, 2003.

- <http://www.linuxparatodos.com/linux/13-como-samba.php>

SAMBA Setup I (Client), Tom Berger, 05/06/2002, 1999-2002.

- <http://www.mandrakeuser.org/docs/connect/csamba.html>

SAMBA Setup II (Server), Tom Berger, 28/06/2002, 1999-2002.

- <http://www.mandrakeuser.org/docs/connect/csamba2.html>

SAMBA Setup III, Tom Berger, 05/06/2002, 1999-2002.

- <http://www.mandrakeuser.org/docs/connect/csamba3.html>

SAMBA V: Domain Membership, Buchan Milne, 15/10/2001, 1999-2002.

- <http://www.mandrakeuser.org/docs/connect/csamba5.html>

SAMBA VI: As a Domain Controller, Buchan Milne, 18/12/2001, 1999-2002.

- <http://www.mandrakeuser.org/docs/connect/csamba6.html>

Implementing Linux in your Network using Samba, Jakob Carstensen, Ivo Gomilsek, Lenz Grimmer, Jay Haskins, y Joe Kaplenk, Noviembre de 1999, 1999.

- <http://www.redbooks.ibm.com/redpapers/pdfs/redp0023.pdf>

Replacing Windows NT Server with Linux, Quinn P. Coldiron, 1997.

- <http://citnews.unl.edu/linux/LinuxPresentation.html>

Recopilación de información sobre Samba., Carlos Cortes Cortes, 05/11/2001.

- <http://bulma.net/body.phtml?nIdNoticia=967>

Usando Samba, primera edición, Robert Eckstein, David Collier-Brown, y Peter Kelly, 1-56592-449-5, Noviembre de 1999.

Using Samba, 2nd Edition, Jay Ts, Robert Eckstein, y David Collier-Brown, 0-596-00256-4, Febrero 2003, 2003.

HowTo, los primeros pasos para Instalar Samba, Gabriel, 08/01/2002 a las 00:12.

- <http://bulma.net/body.phtml?nIdNoticia=1123>

Understanding the Network Neighborhood - How Linux Works With Microsoft Networking Protocols, Christopher R. Hertel, Mayo de 2001, 2001.

- http://www.linux-mag.com/2001-05/smb_01.html

Samba: An Introduction, Christopher R. Hertel, 27/11/2001 a las 21:50:29 GMT.

- <http://www.samba.org/samba/docs/SambaIntro.html>

Samba FAQ, Samba Team, Octubre de 2002.

- <http://www.samba.org/faq/samba-faq.html>

Just what is SMB?, Richard Sharpe, 08/10/2002, 1996, 1997, 1998, 1999, 2001, 2002.

- <http://samba.anu.edu.au/cifs/docs/what-is-smb.html>

Using Samba as a PDC, Tom Syroid.

- <http://www-106.ibm.com/developerworks/eserver/tutorials/samba.html>

Samba HOWTO Collection, Jelmer R. Vernooij, John H. Terpstra, Gerald (Jerry) Carter.

- <http://www.samba.org/samba/devel/docs/html/Samba-HOWTO-Collection.html>

SMB HOWTO, David Wood, 20/04/2000, 2000.

- <http://www.tldp.org/HOWTO/SMB-HOWTO.html>

Documentació sobre CUPS

F.A.Q., 1993-2003.

- <http://www.cups.org/faq.php>

CUPS Software Administrators Manual, 1997-2003.

- <http://www.cups.org/sam.html>

Printing With CUPS - Setup And Configuration II, Till Kampeter, 15/11/2000, 1999-2002.

- <http://www.mandrakeuser.org/docs/hardware/hcups3.html>

Troubleshooting-CUPS-and-Asking-for-Help HOWTO, Kurt Pfeifle, Febrero de 2002.

- <http://www.cups.org/cups-help.html>

An Overview of the Common UNIX Printing System, Version 1.1, Michael Sweet, 10/07/2000, 1998-2003.

- <http://www.cups.org/overview.html>

Pàgines del manual de Debian

man, Durant el desenvolupament d'aquest projecte, es van consultar nombroses pàgines del manual, sobretot aquelles relacionades amb les eines utilitzades. Degut a que la llista de pàgines consultades ha estat molt gran, es deixa com a referència el fet que s'ha consultat en múltiples ocasions.

15. Glossari

API = *Application Program Interface*. Una API compren les especificacions de les operacions que un programa ha d'invocar para comunicar-se a través de la xarxa.

CA = *Certificate Authority*. Entitat certificadora.

CIFS = *Common Internet File System*. Mateix protocol que SMB, però que Microsoft va canviar de nom per tal que aparegués la paraula Internet.

CUPS = *Common UNIX Printing System*. CUPS és el més modern sistema de impressió per UNIX i GNU/Linux, donant serveis d'impressió també a clients Apple MacOS i Microsoft Windows.

DAP = *Directory Access Protocol*. DAP és un protocol d'accés al directori de la pila OSI.

DHCP = *Dynamic Host Configuration Protocol*. Protocol que utilitza un determinat equip per obtenir tota la informació de configuració necessària, incloent l' adreça IP.

DN = *Distinguished Name*. DN es utilitzat per referir-se a una entrada d'un directori LDAP sense ambigüitats. Està formada pel nom de la pròpia entrada, o RDN, i la concatenació dels noms de les entrades que li procedeixen.

DNS = *Domain Name System*. DNS és un estàndard per traduir noms de dominis en direccions IP, o a l'inrevés, sol·licitant la informació a una base de dades centralitzada.

GID = *Group IDentification*. Nombre únic que identifica a un grup dins d'un sistema Unix o a un domini NIS.

IP = *Internet Protocol*. Unitat d'informació que dona el servei bàsic per la entrega de paquets en connexions no orientades a connexió.

IPC = *InterProcess Communication*. IPC fa referència als mecanismes de comunicació entre processos del System V: cues de missatges, conjunts de semàfors i segments de memòria compartida.

IPP = *Internet Printing Protocol*. Protocol per la impressió en xarxa, que transmet les dades mitjançant HTTP 1.1.

IPv4 = *Internet Protocol versió 4*. IPv4 es el nom oficial de la versió actual d'IP.

IPv6 = *Internet Protocol versió 6*. IPv6 es el nom de la següent versió d'IP.

IPX = *Internetwork Packet eXchange*. IPX es un protocol de la capa de xarxa no fiable similar a IP.

LDAP = *Lightweight Directory Access Protocol*. LDAP és un protocol estàndard i obert per accedir als serveis de directori X.500. El protocol s'executa sobre els protocols de transport d'Internet, coneguts com TCP.

LGPL=*Lesser General Public License*. Llicència Pública General del projecte GNU.

LPD =*Line Printer Daemon*. LPD el dimoni d'impressió en línia de Berkeley, que històricament s'ha utilitzat com sistema d'impressió en els sistemes Unix.

MIME =*Multipurpose Internet Mail Extensions*. Els tipus MIME s'utilitza per descriure un format de dades independent de la plataforma.

NBNS =*NetBIOS Name Service*. Como el seu propi nom indica, NBNS fa referència a un servidor de noms basats en NetBIOS.

NBT =*NetBios over TCP/IP*. Protocol NetBios sobre el conjunt de protocols TCP/IP.

NFS =*Network File Sharing*. Protocol que fa ús del protocol IP per permetre a un conjunt d'ordinadors l'accés als sistemes d'arxius de cada un d'aquests com si fossin locals.

NetBEUI =*NetBIOS Extended User Interface*. NetBEUI es un protocol de baix cost dissenyat per petites xarxes, que permet a cada ordinador de la xarxa utilitzar un nom que encara no estigui en ús.

NetBIOS =*Network Basic Input Output System*. NetBIOS es la interfície estàndard per xarxes a PCs IBM i ordinadors personals compatibles.

NIS =*Network Information Services*. NIS és molt utilitzat per permetre a varies màquines d'una xarxa compartir la mateixa informació dels comptes d'usuari.

NSCD =*Name Service Cache Daemon*. nscd es un dimoni que administra les cerques de claus, grups i hosts dels programes que estan en execució.

OSI =*Open Systems Interconnection*. OSI és la referència pels protocols desenvolupats per ISO com competidor de TCP/IP. Actualment ja no es desenvolupa ni té suport.

PAM =*Pluggable Authentication Modules*. Suite de llibreries compartides que permeten a l'administrador local del sistema la elecció del mètode que utilitzaran les aplicacions per autenticar als usuaris.

PDC =*Primary Domain Controller*. Un PDC és un servidor Windows encarregat d'autenticar als usuaris dins d'un domini Windows així com establir els permisos associats.

PDF =*Portable Document Format*. Acrònim de Format de Documentació Portable.

POSIX =*Portable Operating System for unIX*. La interfície de sistema operatiu portàtil per UNIX.

PPD =*PostScript Printer Description*. Arxiu ASCII que emmagatzema tota la informació sobre les capacitats especials d'una impressora.

PS =*PostScript*. PostScript és l'estàndard en el sistema d'impressió del món UNIX.

RDN =*Relative Distinguished Name*. RDN correspon al nom d'una entrada al servei de directori LDAP.

RID = *Relative Identifier*. RID és un nombre únic dins d'un domini Windows que identifica a un usuari, un grup, un ordinador o qualsevol altre objecte.

RPC=*Remote Procedure Call*. Tecnologia per la qual un programa invoca serveis a través de la xarxa fent diferents crides a procediments.

Samba=Samba és una suite d'aplicacions Unix que "parla" el protocol SMB (*Server Message Block*).

SID=*Security Identifier*. Els SIDs s'utilitzen per identificar objectes a un domini de sistemes Windows. Aquests objectes poden ser els usuaris, els grups, els ordinadors i els processos.

SMB = *Server Message Block*. SMB es un protocol de compartició d'arxius, impressores, ports sèrie i abstracció de comunicacions (com *pipes* i *slots* de correu) entre ordinadors.

SSL = *Secure Socket Layer*. SSL és un mètode de xifrat propietari per la transmissió de dades a través del protocol HTTP, que va ser desenvolupat per Netscape.

TCP = *Transmission Control Protocol*. Protocol de la capa de transport de l'estàndard TCP/IP que dona servei fiable i *full duplex* del qual depenen molts protocols d'aplicació.

TCP/IP = *Suite protocolar de Internet TCP/IP*. Nom oficial dels protocols TCP/IP.

TLS = *Transport Layer Security*. TLS és el successor del protocol SSL, creat per IETF.

UDP = *User Datagram Protocol*. Protocol que permet a un programa a determinada màquina enviar un datagrama a una altre aplicació executant-se en altre màquina.

UID = *User Identification*. Nombre únic que identifica a un usuari dins d'un sistema Unix o domini NIS.

UNC = *Universal Naming Convention*. UNC fa referència a la notació empleada per Windows per referir-se als recursos compartits d'una xarxa (\\màquina\directori).

Unicode = Conjunt de caràcters de 16 bits estàndard, dissenyat i mantingut per Unicode Inc.

URI = *Universal Resource Identifier*.

URL = *Uniform Resource Locators*.

VFS = *Virtual File System*.

WINS = *Windows Internet Name Service*. WINS és el nom de la implementació NBNS de Microsoft.

X.500 = Directory Access Protocol (DAP)

16 Agräiments

