Integració de sistemes operatius

Jordi Cárdenas Guia i Juan José López Zamorano

Sistemes operatius en xarxa

Índex

Introducció 5

Resultats d'aprenentatge 7

1 Sistemes heterogenis. Integració de sistemes amb Windows 9
1.1 Sistemes heterogenis . . . 9
1.1.1 Integració de sistemes heterogenis . . . 10
1.2 Integració de sistemes lliures i propietaris amb Windows 2008 Server . . . 12
1.2.1 Subsistema per aplicacions UNIX . . . 12
1.2.2 Gestió d'identitats per a UNIX . . . 13
1.3 Utilització d'NFS en Windows Server 2008 . . . 15
1.3.1 Instal·lar NFS . . . 15
1.3.2 Component d'NFS . . . 16
1.3.3 Configuració de l'ús compartit d'NFS . . . 16
1.3.4 Administració de la funció de serveis d'arxius . . . 17
1.3.5 Configuració de l'accés a impressores . . . 18
1.3.6 Configuració d'Active Directory per autenticar màquines UNIX . . . 19
1.4 Interoperabilitat amb equips Mac . . . 21
1.4.1 Equips Mac i Windows dins d'una mateixa xarxa . . . 21
1.4.2 Connexió a volums NFS . . . 22
1.4.3 Mac OS X i Active Directory . . . 22
1.4.4 Mac OS X i Open Directory . . . 23
1.4.5 Emmagatzematge en xarxa . . . 24
1.4.6 Mac i PC: impressores compartides en LAN . . . 24
1.5 Utilització dels diferents servidors de fitxers . . . 25

2 Integració de sistemes amb GNU/Linux 27
2.1 Integració de sistemes lliures i propietaris amb Samba . . . 27
2.1.1 Utilitats de Samba . . . 29
2.2 Domini Windows NT . . . 30
2.3 Grups de treball Windows . . . 31
2.4 Tipus de configuracions d'un servidor Samba . . . 31
2.5 Instal·lació servidor i client Samba . . . 33
2.6 Configuració de Samba a un grup de treball . . . 33
2.6.1 Compartició de recursos a un grup de treball heterogeni . . . 34
2.7 Navegació a les xarxes Windows . . . 40
2.7.1 Configuració del Browsing a Samba . . . 41
2.7.2 Configuració de Samba com a Local Master Browser . . . 42
2.7.3 Configuració com a Domain Master Browser . . . 42
2.8 Gestió de l'autenticació amb Samba en sistemes heterogenis . . . 43
2.8.1 Identificació d'usuaris GNU/Linux i Windows . . . 44
2.8.2 Procés d'autenticació en Samba . . . 46
2.9 Configurar Samba com a Controlador Primari de Domini . . . 48

2.9.1 Configuració bàsica de TCP/IP i dels paràmetres de xarxa de Windows 49
2.9.2 Configuració de la resolució de noms de NetBIOS (WINS) 50
2.9.3 Configuració les opcions de Logon 51
2.9.4 Scripts de gestió d'usuaris 57
2.9.5 Afegir clients al domini amb Samba com a PDC 59
2.10 Samba amb LDAP 61
2.10.1 Configuració d'un PDC Samba amb OpenLDAP 63

Introducció

La integració de sistemes és un fet habitual avui dia en el món informàtic. Considerem completament normal que sistemes propietari i lliures convisquin en una mateixa xarxa i, encara més, comparteixin recursos.

No tindria sentit estudiar les característiques i els components dels sistemes propietari i els sistemes lliures si no s'uneixen les vies d'estudi en algun punt. En aquesta unitat convergeixen els dos tipus de sistemes. Cal avaluar com s'accepten mútuament i quins problemes en generen. Heu d'aconseguir desenvolupar un ull crític que us permeti aprofitar els avantatges que cadascun dels sistemes us ofereix.

Aquesta unitat presenta els mecanismes actuals de compartició de recursos entre els sistemes propietari i lliure i entre els sistemes lliures i propietari. S'ha centrat l'estudi en distribucions lliures basades en UNIX i les versions més actuals dels sistemes operatius servidor de Microsoft.

És molt recomanable disposar de, com a mínim, un sistema operatiu propietari i un sistema operatiu lliure que es puguin comunicar per poder treballar els continguts aquí presentats. Al llarg del text es mostren situacions i exercicis que us ajudaran molt a assolir els objectius del crèdit. Les activitats i els exercicis d'autoavaluació s'han dissenyat en la línia de treball del material escrit i, per tant, es recomana treballar-los en paral·lel a l'estudi teòric.

En l'apartat "Sistemes heterogenis. Integració de sistemes amb Windows", es descriu en què consisteixen els sistemes heterogenis i com estan presents en gairebé tots els àmbits de treball actual. A més, s'hi mostra, mitjançant eines com SNIS i NFS, la integració de diferents sistemes operatius des del punt de vista dels sistemes propietaris, concretament utilitzant Windows 2008 Server.

En l'apartat "Integració de sistemes amb GNU/Linux" es mostra, mitjançant eines com Samba i LDAP, la integració dels sistemes operatius GNU/Linux, concretament Ubuntu, dins de la estructura dels sistemes operatius Windows.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumna/e:

1. Identifica la necessitat de compartir recursos en xarxa entre diferents sistemes operatius.
2. Comprova la connectivitat de la xarxa en un escenari heterogeni.
3. Descriu la funcionalitat dels serveis que permeten compartir recursos en xarxa.
4. Instal·la i configura serveis per compartir recursos en xarxa.
5. Utilitza eines gràfiques per a la gestió de recursos compartits en escenaris heterogenis.
6. Accedeix a sistemes d'arxius en xarxa des d'equips amb diferents sistemes operatius.
7. Accedeix a impressores des d'equips amb diferents sistemes operatius.
8. Gestiona usuaris i grups.
9. Estableix nivells de seguretat per controlar l'accés dels usuaris i grups als recursos compartits en xarxa.
10. Comprova el funcionament dels serveis instal·lats.
11. Documenta les tasques d'integració fetes, les incidències aparegudes i les solucions aportades.
12. Cerca i interpreta documentació tècnica en les llengües oficials i en les de més ús al sector.

1. Sistemes heterogenis. Integració de sistemes amb Windows

En aquesta unitat desenvolupem el concepte de sistema heterogeni i la importància de la integració dels sistemes existents en aquest tipus d'escenari. Així mateix, es mostren les diverses possibilitats d'integració entre diferents tipus de sistemes operatius i introduïm els mecanismes d'integració proporcionats pel sistema Windows 2008 Server.

Microsoft Windows és el sistema operatiu amb llicència propietària de programari més important del món, mentre que les diferents distribucions Linux són els sistemes operatius amb llicència lliure més distribuïts arreu del món. És clara, doncs, la importància de fer treballar junts tots dos sistemes i aprofitar al màxim les respectives característiques.

El codi obert dels sistemes Linux i la seva gratuïtat es contraposen al codi tancat i de pagament dels sistemes Windows. Segons Microsoft, els seus sistemes són realment més barats que els sistemes Linux, ja que són més fàcils d'utilitzar i això implica a llarg termini un abaratiment del producte, mentre que els sistemes Linux requereixen una "mà" més experta, cosa que encareix un producte que en un principi era gratuït.

1.1 Sistemes heterogenis

La gran majoria d'organitzacions existents actualment, degut a les tendències del món de la informàtica i les telecomunicacions, fan servir gran quantitat de maquinari i programari amb característiques, arquitectures o fabricants diferents. Aquestes diferències conformen un sistema o escenari heterogeni, que podem definir com:

> Un **sistema heterogeni** és aquell que es troba compost per maquinari amb característiques físiques distintes entre si, i programari amb característiques operatives distintes entre si, però que es poden comunicar utilitzant mitjans comuns.

Molts dels àmbits referents a la comunicació i la compatibilitat entre equips amb diferent maquinari i programari estan estandarditzats, per exemple protocols de comunicacions, estàndards de maquinari, etc. Però existeixen altres àmbits, com són el del funcionament i gestió dels sistemes operatius, en el qual cada distribució o empresa té implementacions, comportaments o funcionalitats diferents. Aquestes implementacions no estandarditzades o no consensuades fan que en molts casos els diferents sistemes operatius siguin incompatibles entre ells. Aquestes

diferències són majors sobretot entre sistemes operatius lliures i propietaris, ja que la filosofia de negoci de cadascú dificulta de vegades el desenvolupament d'estàndards comuns i, per tant, la integració dels sistemes.

El fet que existeixen diferents màquines amb sistemes operatius en una mateixa organització indica que cada màquina gestionarà una quantitat d'informació i una sèrie de recursos com ara impressores, discos durs, unitats de CD-ROM que pot ser necessari que siguin compartits amb la resta de màquines de la xarxa o l'organització.

Així resulta necessari l'ús de serveis o aplicacions que permetin i facilitin l'intercanvi de recursos i informació en les organitzacions i que generin un entorn de xarxa comú entre els diferents sistemes operatius.

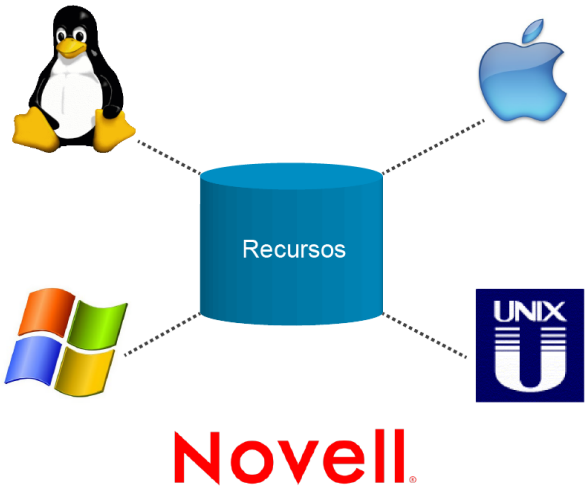
Independència

Quan utilitzem el terme *independència* no volem dir que les aplicacions que implementen els serveis de xarxa siguin independents del sistema operatiu, sinó que quan els sistemes utilitzen un determinat servei, per exemple accedir a un fitxer en un servidor FTP, és indiferent que la màquina on es troba funcionant el servei tingui instal·lat un sistema operatiu o un altre, davant de l'usuari.

Existeixen gran varietat de serveis que ens permeten fer la compartició de recursos de manera transparent a l'usuari i amb independència del sistema operatiu que utilitzem a través de la xarxa. Aquesta independència es deu al fet que aquests serveis utilitzen protocols de comunicació estandarditzats, per exemple FTP, HTTP, DNS, etc. Però si el que volem és generar un entorn de xarxa comú en el qual integrem el sistema d'autenticació d'usuaris en una xarxa local, amb la compartició de recursos i la gestió de la informació de les màquines connectades a la xarxa, necessitem fer servir altres tipus de serveis com són els serveis de directori, serveis d'autenticació centralitzada, serveis de compartició de fitxers, serveis d'impressió, etc. que funcionin de manera conjunta i integrada.

La figura 1.1 il·lustra la idea de sistema heterogeni. Es pretén fer conviure sistemes molt diferents en un mateix espai.

FIGURA 1.1. Un sistema heterogeni



1.1.1 Integració de sistemes heterogenis

Una vegada entenem en què consisteix un sistema heterogeni i la importància de la compartició de recursos dins de les organitzacions, podem adonar-nos de la necessitat d'integrar els diferents sistemes operatius perquè puguin funcionar en

conjunt en àmbits comuns i utilitzar els recursos de què es disposa.

> Definim la integració de sistemes com la creació d'estructures formades per ordinadors de diferent tipus i amb sistemes operatius diferents que interoperin entre si de manera transparent per a l'usuari.

Existeixen diferents possibilitats d'integració entre sistemes lliures i propietaris per a la compartició de recursos, la possibilitat més comuna és mitjançant dominis Windows. Per implementar un domini Windows tenim diferents opcions:

- Utilitzar una màquina Windows com a controlador de domini.
- Utilitzar una màquina GNU/Linux com a controlador de domini.

En els dos casos anteriors els clients podran ser màquines amb sistemes Windows o GNU/Linux.

En el cas d'utilitzar una màquina Windows com a controlador de domini, les màquines clients Windows no tindran cap problema per accedir al domini. Per a les màquines clients GNU/Linux, ens caldrà especificar un mecanisme d'autenticació i proporcionar la manera d'obtenir els atributs específics (UID; GID; shell, etc.) per a usuaris i grups. D'aquesta manera podem optar per dues solucions:

1. No utilitzar Directori Actiu, fent servir winbind, aquesta opció ens permet:
    - Resoldre l'autenticació i l'obtenció d'atributs comuns mitjançant mecanismes Windows (Kerberos + LDAP).
    - Integrar el client GNU/Linux com a membre del domini Windows.
    - Proporcionar atributs UNIX des del mateix client GNU/Linux quan sigui necessari.
2. Utilitzar Directori Actiu, fent servir IDMU, aquesta opció ens permet:
    - Modificar l'esquema d'*Active Directory* per incloure atributs UNIX.
    - Resoldre l'autenticació i l'obtenció d'atributs comuns mitjançant mecanismes Windows (Kerberos + LDAP).
    - No integrar el client GNU/Linux com a membre del domini Windows.
    - Configurar el client GNU/Linux perquè pugui accedir al Directori Actiu.

Independentment de l'opció que utilitzem haurem de configurar el client GNU/-Linux per utilitzar NSS (especificació de la base de dades d'usuaris), PAM (autenticació de comptes) i, si cal, windbind (integració de clients GNU/Linux en dominis Windows).

En el cas d'utilitzar una màquina GNU/Linux com a controlador de domini, la màquina haurà de tenir instal·lat el paquet Samba i estar configurada com a controlador primari de domini. Aquesta solució permet emular un domini Windows

NT amb una màquina GNU/Linux, la qual cosa suposa utilitzar programari lliure, evitant així, haver de pagar llicències per la seva utilització. Els clients Windows podran accedir al domini i als recursos accessibles des del domini sense cap problema. Els clients GNU/Linux podran accedir als recursos del domini, si els usuaris existents als clients estan donats d'alta també com a usuaris Samba. Si volem que els clients GNU/Linux, a més, s'autentiquen al domini creat pel servidor Samba, haurem d'utilitzar i configurar eines com NSS, PAM, i windbind o LDAP.

Existeix una altra opció molt més senzilla per a la simple compartició de recursos entre màquines Windows i GNU/Linux, sense necessitat d'implementar un domini. Aquesta opció consisteix a utilitzar Samba a les màquines GNU/Linux i crear un grup de treball comú entre les màquines amb sistemes Windows i les màquines amb sistemes GNU/Linux.

1.2 Integració de sistemes lliures i propietaris amb Windows 2008 Server

Tot i que Microsoft domina clarament el mercat domèstic, cada vegada més el sistema Linux està present a les llars compartint màquina amb una versió Windows. En el món de les supercomputadores les dades canvien: Microsoft és el segon sistema utilitzat per darrere de Linux.

Des del punt de vista tècnic, el més important és saber identificar les febleses de cadascun dels sistemes i cobrir-les amb un altre sistema operatiu. És aquí on té un paper molt important saber integrar diferents sistemes operatius.

Microsoft Windows Server 2008 ofereix diverses opcions d'integració vers diferents sistemes operatius, com ara les distribucions Linux o els sistemes operatius d'Apple.

1.2.1 Subsistema per aplicacions UNIX

En les distribucions Linux existeixen paquets que permeten executar en Linux aplicacions dissenyades per a Windows. L'empresa Microsoft no tenia la possibilitat d'executar aplicacions basades en UNIX, cosa que es podia interpretar com una situació de desavantatge, fins que es va presentar el SUA (*Subsystem Unix Applications*).

SUA ofereix la infraestructura bàsica per executar aplicacions i scripts UNIX en Microsoft Windows Server 2008.

El SUA resideix sobre el nucli, igual que el subsistema win32. Contempla la semàntica i les crides del sistema UNIX completes.

Per utilitzar el *SUA* l'haureu d'instal·lar com una característica de Windows Server 2008.

Utilitats del subsistema d'aplicacions UNIX

El *SUA* inclou una sèrie d'utilitats que el posicionen com una eina molt potent i amb un ampli camp d'aplicació. Algunes de les utilitats que inclou el *SUA* són:

- **Shells**: Korn i C.
- **Jobs**: ps, nice i kill.
- **Batchs**: at, cron i batch.
- **Desenvolupament**: gcc, gdb i make.
- **Processament de text**: grep, less, awk, sed, pr i tr.
- **Gràfics**: xterm, xrdb, xset i xclock.
- **Connectivitat**: bind, sendmail i ftp.

El SUA també inclou un ampli suport d'APIs que permeten dur a terme la portabilitat d'aplicacions UNIX sense haver de fer gaires canvis en el codi font, com ara C, C++, Fortran, Perl, Math, RPC, Socket, Curse, Crypt, Termcap, Lex, Yacc, Pthread, X11R6.6 i suport a Dynamic linking/shared object.

Portabilitat d'aplicacions

De manera similar a com es fan les portabilitats d'aplicacions entre diferents distribucions de Linux, *SUA* s'encarrega de portar a Windows *scripts* i aplicacions d'UNIX. Els *scripts* els copia a *scripts* per a Windows Server i els executa, mentre que les aplicacions les ha de recompilar.

La portabilitat es fan de manera segura en un gran nombre de casos, tot i que us podeu trobar amb problemes durant la compilació de les aplicacions. En determinats casos es produeixen petits canvis en l'aspecte que presenten les aplicacions deguts a les diferències en les llibreries d'ambdós sistemes.

1.2.2 Gestió d'identitats per a UNIX

La gestió d'identitats s'instal·la com una part del *Role* de *Directory Services* de Windows Server 2008.

SNIS (*Server for NIS*) integra les xarxes de Windows i la de *Network Information Service* (*NIS*).

Un controlador de domini Windows té la possibilitat d'actuar como un NIS mestre per a un o diversos dominis NIS. SNIS emmagatzema les dades dels *NIS maps* en el *Directorio Activo* utilitzant un esquema compatible amb l'RFC 2307.

Altres característiques pròpies són:

- La gestió d'identitats pot utilitzar *NIS maps* com estàndard, per exemple hosts, group, protocols, o com no estàndard.
- Els clients UNIX i Linux accedeixen a *AD* utilitzant *LDAP*.
- *SNIS* pot instal·lar-se en altres *DC* del domini per a que actuïn com a subordinats.
- Els servidors *NIS* UNIX poden seguir actuant com a subordinats del domini *NIS*.

Eines i utilitats SNIS

SNIS agrupa una sèrie d'eines i utilitats que faciliten molt les tasques de l'usuari. En resum, SNISS ofereix:

- Un assistent de migració i utilitats en la línia d'ordres per migrar i gestionar els *NIS maps* d'UNIX al servidor executant SNIS: nis2ad, nisadmin, nismap, ypcat, ypclear, ypmatch, yppush.
- Els clients poden utilitzar moltes funcions i crides de procediment remot per connectar al servei de xarxa: yp_match, yp_first, yp_next, yp_all, yp_order, yp_master, yperr_string, and ypprot_err.
- Un llarg etcètera com: yppoll, ypset, domainname.

Sincronització de contrasenyes

La possibilitat de sincronitzar les contrasenyes tant en un sistema UNIX com en un sistema Windows facilita molt la tasca de l'administrador i la dels usuaris.

La sincronització de contrasenyes:

- S'instal·la com una part del *Role* de *Directory Services* de Windows Server 2008.
- Permet als usuaris mantenir un únic parell usuari/contrasenya per a tot el domini Windows i els equips UNIX, i sincronitzar les contrasenyes quan es canvien en algun dels sistemes.

- La sincronització pot ser en un o en els dos sentits.
- Sincronitza les contrasenyes en equips Windows *Stand-Alone* o per a un domini de Windows.
- Gestiona les contrasenyes d'equips UNIX individuals o de tots els equips d'un domini *NIS*.

1.3 Utilització d'NFS en Windows Server 2008

Windows Services For UNIX

Windows Services For UNIX és un paquet que conté utilitats per reproduir diverses *Shell* de UNIX, emular el seu comportament i proporcionar un entorn operatiu similar al d'UNIX o Linux dins de Windows Server 2003.

Resulta de gran utilitat utilitzar un client *NFS* per migrar arxius d'una màquina UNIX a un servidor Windows Server 2008. Utilitzant el client per a *NFS* podreu accedir sense gaires problemes a una màquina UNIX.

Característiques que heu de tenir en compte a l'hora d'utilitzar *NFS* són:

- S'instal·la com a part del *Role* de servidor de fitxers amb el *Server Manager*.
- Té suport per treballar amb màquines de 64 bits.
- Proporciona millores de rendiment.
- Ofereix suport a dispositius UNIX especials (mknod).
- Heu de tenir en compte que determinades característiques de SFU 3.5 no estan suportades en Windows Server 2008 (ni en Windows Server 2003 R2).
- Proporciona *Gateway for NFS*.
- Conté *Server for PCNFS*.
- Conté tots els components PCNFS del client per NFS.

1.3.1 Instal·lar NFS

Per fer la instal·lació de l'NFS Microsoft Windows utilitza *Microsoft Installer*.

Podeu instal·lar mòduls individuals o tot el producte sencer. Heu de tenir en compte que si s'han instal·lat components anteriors de *Servicios de Windows* per UNIX, haureu d'incloure aquests components en el paràmetre *addlocal* de la línia d'ordres d'instal·lació, separats per una coma (,). Si no ho feu, aquests productes s'eliminaran durant la instal·lació del client per a NFS.

Per instal·lar el client per a NFS des de la línia d'ordres haureu de seguir els passos següents:

1. Inicieu una sessió en l'equip amb un compte del grup dels administradors.

2. Obriu una finestra de línia d'ordres.
3. Introduïu al lector de DVD el disc que contingui *Windows Services for UNIX*.
4. Escriviu a la línia d'ordres: *msiexec /I D:\sfusetup.msi /qb addlocal="NFSClient" [targetdir="install path"]*.
5. Incloeu la clau del producte agregant *PidKey= la vostra clau*.

1.3.2 Component d'NFS

Els components que podeu trobar per a serveis per UNIX lligats a NFS estan directament relacionats amb els processos d'autenticació o bé en depenen. A continuació es descriuen breument aquests components:

- **User Name Mapping Server**: mapa els usuaris UNIX que estan a Windows i els usuaris Windows que estan a UNIX. Si es donés el cas que un usuari té un compte d'usuari en UNIX i un en Windows, el component conté un mecanisme per relacionar-los amb una única persona.
- **Server for NFS Authentication**: no es tracta d'un servidor, sinó d'un component necessari perquè les màquines Windows puguin fer el procés d'autenticació amb NFS.
- **Server for PCNFS**: aquest servidor el pot utilitzar qualsevol altre NFS que necessiti accedir a PCNFS.
- **Client for NFS**: es tracta del component client d'SFU per a NFS. El client per NFS ha d'estar a la màquina que utilitzarà el recurs NFS a la xarxa.
- **Gateway for NFS**: es tracta d'un client NFS especial. Proporciona l'accés a recursos a altres màquines Windows que no tenen instal·lat cap component SFU.
- **Server for NFS**: el servidor per a NFS s'instal·la en aquells equips que han de proporcionar el servei NFS a la xarxa.

1.3.3 Configuració de l'ús compartit d'NFS

És possible configurar NFS per compartir carpetes locals en volums NTFS utilitzant l'explorador de Windows o mitjançant d'administració d'emmagatzematge i recursos compartits. Mitjançant l'explorador de Windows podreu activar i configurar l'ús compartit d'NFS si seguiu els passos següents:

1. Cliqueu amb el botó dret del ratolí a sobre del recurs compartit que vulgueu administrar.

2. Seleccioneu *Propietats*.
3. Dins el quadre de diàleg *Us compartit avançat d'NFS* marqueu l'opció *Compartir aquesta carpeta*.
4. Escriviu el nom del recurs compartit en el quadre de text *Recurs compartit*.
5. Marqueu la casella *Permetre accés anònim*si voleu permetre l'accés anònim a aquest recurs.

Els noms dels recursos compartits mitjançant *NFS* han de ser únics per a cada sistema. El nom del recurs que indiqueu és el nom de la carpeta a la qual es connectaran els usuaris UNIX.

Per defecte, els equips UNIX només disposen d'accés de lectura al recurs compartit mitjançant *NFS*. Per canviar els permisos d'accés heu de clicar, dins el quadre de diàleg *Ús compartit avançat d'NFS*, a sobre del botó *Permisos*.

Si el que necessiteu és desactivar els recursos compartits amb *NFS* heu de seguir els passos següents:

1. Cliqueu amb el botó dret del ratolí a sobre del recurs compartit que vulgueu desactivar.
2. Premeu a sobre de *Propietats*.
3. Dins de la fitxa*Ús compartit avançat d'NFS* elimineu la marca de la casella *Compartir aquesta carpeta*.
4. Accepteu per tancar.

1.3.4 Administració de la funció de serveis d'arxius

El servidor d'arxius és un equip que resulta imprescindible en moltes configuracions de xarxa. És imprescindible configurar almenys un servidor de fitxers si molts usuaris necessiten accedir als mateixos fitxers i dades d'aplicació. Microsoft Windows Server 2008 està preparat per donar aquest accés a màquines que funcionin sobre sistemes UNIX i distribucions Linux.

En sistemes anteriors a Windows Server 2008 es tenia la possibilitat d'instal·lar un servidor de fitxers bàsic, però amb l'actual sistema operatiu és necessari configurar un servidor perquè actuï com a servidor de fitxers afegint la funció Serveis d'arxiu.

En la taula 1.1 es mostren els serveis de funció per a servidors de fitxers.

TAULA 1.1. Descripció dels serveis de funció per a servidors de fitxers.

Servei de funció	Descripció
Administració de recursos compartits i emmagatzemament	Permet que els administradors s'ocupin de les carpetes compartides i permet que els usuaris accedeixin a les carpetes compartides mitjançant la xarxa.
Servei de cerca de Windows	Permet buscar fitxers ràpidament en el servidor des de màquines client.
DFS, sistema de fitxers distribuït	Proporciona eines i serveis per als espais de noms i la replicació DFS.
Espais de noms DFS	Permet agrupar carpetes compartides ubicades en diferents servidors dins d'una estructura lògica formada per un o més espais de noms.
Replicació DFS	Permet sincronitzar carpetes de diversos servidors mitjançant les connexions de xarxa d'àrea local o extensa.
FSRM, administrador de recursos del servidor de fitxers	Agrupa un conjunt d'eines que els administradors poden utilitzar per gestionar les dades emmagatzemades.
Serveis per a NFS	Permet compartir fitxers en entorns mixtos. Els usuaris podran transferir fitxers entre Windows Server 2008 i UNIX o distribucions Linux.
Serveis d'arxiu de Windows Server 2003	Proporciona serveis de fitxer compatibles amb Windows Server 2003.
FRS, serveis de replicació d'arxius	Permet sincronitzar carpetes amb servidors d'arxius que utilitzin FRS en comptes de DFS.
Serveis d'Index Server	Permet la indexació d'arxius i carpetes per poder trobar-los ràpidament.

Per afegir la funció *Serveis de fitxer* i poder treballar seguiu els passos següents:

1. Obriu l'administrador del servidor.
2. Dins el node *Funcions* cliqueu a *Afegir funcions*.
3. Quan estigueu a *Seleccionar funcions del servidor* seleccioneu *Serveis de fitxer* i progresseu amb *Següent*.
4. Marqueu *Serveis per a Network File System* per poder treballar amb sistemes UNIX.
5. Completeu els passos opcionals i cliqueu a *Següent*.
6. Confirmeu l'inici de la instal·lació amb *Confirmar seleccions d'instal·lació*.
7. Cliqueu a *Instal·lar* per iniciar el procés d'instal·lació.

1.3.5 Configuració de l'accés a impressores

Una impressora accessible des de la xarxa pot concentrar un gran número de tasques d'impressió que poden venir tant de sistemes Windows com de sistemes

UNIX. L'alta càrrega de treball fa que calgui fer un treball d'administració força acurat.

Els treballs que s'acumulen a la cua d'impressió es copien a la carpeta *%SystemRoot%\system32\spool\PRINTERS*. Els usuaris que hagin d'accedir a la impressora hauran de tenir permisos per modificar aquesta carpeta.

Reviseu els permisos de la carpeta seguint els passos següents:

1. Obriu el servidor d'impressió.
2. Cliqueu a *Propietats*.
3. Seleccioneu la fitxa *Opcions avançades*.
4. La carpeta a revisar està descrita com *Carpeta de cua d'impressió*.
5. Utilitzeu l'explorador de Windows per accedir a la carpeta descrita en el punt anterior.
6. Cliqueu amb el botó dret a sobre de la carpeta i premeu *Propietats*.
7. Dins la fitxa *Seguretat* comproveu que els permisos són els adients.

1.3.6 Configuració d'Active Directory per autenticar màquines UNIX

Abans de l'aparició de Microsoft Windows Server 2000 els controladors de domini de Windows NT proporcionaven serveis d'autenticació per a clients utilitzant *NTLM* (gestor de xarxes d'NT). Aquest protocol era capaç de mantenir duplicats de comptes d'usuari en diversos servidors de xarxa, tot i que tenia importants problemes de seguretat.

És a partir de Microsoft Windows Server 2000 que Microsoft decideix deixar de banda el protocol *NTLM* i començar a treballar amb *Active Directory* i els serveis d'autenticació integrats d'autenticació Kerberos.

Kerberos és un sistema molt més segur que NTLM i que gestiona millor l'escalabilitat. Els sistemes Linux i UNIX també utilitzen Kerberos, per tant es converteix en molt real la possibilitat d'integrar els diferents sistemes operatius.

Existeix un problema amb l'autenticació d'usuaris de Linux i UNIX amb *Active Directory*: els identificadors d'usuaris i grups. Internament, ni Linux ni Windows fan referència als usuaris pel nom, sinó que utilitzen els identificadors interns únics.

Els sistemes Microsoft utilitzen el *SID* (identificador de seguretat), que és una estructura de longitud variable que identifica sense marge d'error els diferents usuaris dins d'un domini de Windows. El *SID* també conté un identificador únic de domini per tal que el sistema operatiu pugui distingir entre els usuaris en diferents dominis.

En sistemes UNIX i distribucions Linux cada usuari té un identificador d'usuari (*UID*) que és un nombre enter de 32 bits únic en el sistema. L'àmbit de l'*UID* està limitat en l'equip, sense que es garanteixi que un altre usuari en una màquina diferent pugui tenir el mateix nombre enter. Això fa que un usuari ha d'iniciar sessió en cada equip on hagi de tenir accés.

Aquest problema se soluciona proporcionant autenticació de xarxa amb el sistema d'informació de xarxa (*NIS*) o un directori compartit d'*LDAP*. El sistema d'autenticació de xarxa proporciona l'*UID* per a l'usuari i tots els equips Linux o UNIX utilitzen aquest sistema d'autenticació compartint el mateix usuari i els identificadors de grup.

És recomanable utilitzar *Active Directory* per proporcionar un usuari únic i els identificadors de grup. Es pot crear un *UID* per a cada usuari i grup i emmagatzemar aquest identificador amb l'objecte corresponent en *Active Directory*, així, quan un usuari s'autentica pot cercar l'UID per a l'usuari i proporcionar-lo per al sistema operatiu com l'identificador de l'usuari intern.

Aquesta solució, però, té un inconvenient. És necessari proporcionar un mecanisme per garantir que cada usuari i grup tenen un identificador i que aquests identificadors són únics en el bosc.

Una altra estratègia per assignar identificadors és utilitzar l'identificador relatiu (*RID*). L'identificador relatiu és un número enter de 32 bits que identifica l'usuari dins el domini. El *RID* forma part del *SID*. La solució consisteix en extreure el *RID* quan l'usuari inicia la sessió i fer-lo servir com a *UID* intern únic. Només cal remarcar que no podreu utilitzar aquesta estratègia en aquells entorns on existeixin diversos dominis, ja que existeix la possibilitat que els usuaris de diferents dominis tinguin el mateix valor *RID*.

És necessari proporcionar els identificadors de Linux o UNIX per a tots els usuaris, i els grups als quals pertanyen, que poden iniciar sessió. S'han de definir valors per als atributs *uidNumber* i *gidNumber* dels usuaris i grups. No oblideu que:

- Els sistemes UNIX i distribucions Linux necessiten un UID para a cadascun dels usuaris que autentiquen. Cada compte d'usuari que iniciarà una sessió en un equip Linux o UNIX ha de tenir un atribut *uidNumber* únic. El valor específic que utilitzi per a un *uidNumber* no és important, però ha de ser únic entre tots els usuaris que poden iniciar sessió en l'equipo de Linux o UNIX.

- Cada usuari de Linux també ha de tenir un identificador de grup predeterminat, per a cada usuari d'*Active Directory* que s'iniciarà en una sessió en un equipo Linux o UNIX requereix un valor per a l'atribut *gidNumber*. Aquest valor no ha de ser únic entre tots els usuaris, però ha d'identificar el grup.

- Cada grup en *Active Directory* ha de tenir un valor únic per a l'atribut *gidNumber*.

1.4 Interoperabilitat amb equips Mac

És possible intercanviar arxius i compartir impressores i la connexió a Internet dins una xarxa amb equips Mac.

L'adopció del d'Ethernet i el protocol TCP/IP com estàndard en els últims PC i Mac ha simplificat enormement la interoperativitat entre les dues plataformes.

Els sistemes Macintosh es poden connectar a totes les principals plataformes de servidor, com ara AppleShare, Unix, Linux i Windows (NT/2000/XP/2003/Vista/2008). El sistema operatiu Mac OS X és compatible amb:

- Els protocols d'arxius compartits estàndard AFP (*Apple Filing Protocol*).
- SMB / Samba (*Service Message Block*).
- WebDAV.
- Unix NFS (*Network File System*).

Per connectar-se a xarxes, Mac OS X disposa d'un client AFP, un altre SMB per connectar-se a servidors de fitxers Windows i també un NFS per als servidors Unix. La integració de clients Macintosh en aquestes plataformes de servidor és senzilla i molt intuïtiva.

1.4.1 Equips Mac i Windows dins d'una mateixa xarxa

El sistema operatiu Mac OS X disposa d'un client i un servidor SMB incorporat, fet que permet a l'equip que està funcionant amb Mac OS X pertànyer a la xarxa exactament igual que qualsevol PC per als usuaris de Windows i viceversa. A l'equip amb Mac OS X, heu de seleccionar *Connectar al servidor ...* al menú *Anar* per navegar per diversos ordinadors de grups de treball i dominis Windows.

Amb aquesta implementació de client i servidor SMB, els usuaris de Mac OS X poden compartir les carpetes i impressores connectades per USB a una xarxa Windows.

Des d'una estació de treball Windows s'accedeix de la mateixa manera a tots els recursos ubicats en un servidor Mac OS X.

Mac OS X Server és un sistema operatiu per a servidor d'última generació. Gràcies al seu alt rendiment. Heu de tenir en compte que el sistema operatiu Mac OS X Server pot atendre un gran nombre d'estacions de treball, tant Mac com PC amb Windows o estacions de treball Unix.

El programari inclòs en el sistema operatiu Mac proporciona serveis per compartir arxius Macintosh (AFP sobre IP), Windows (SMB / CIFS) i Unix (NFS). També inclou eines d'administració per a ordinadors Macintosh anteriors i les aplicacions necessàries per implantar un servidor d'Internet complet (DNS, web, correu i un llarg etcètera). A més, el programari proporciona una interfície d'administració unificada per organitzar els privilegis d'accés dels usuaris.

Mac OS X Server és compatible amb els arxius compartits Windows des de qualsevol punt d'accés definit, no solament les carpetes compartides i públiques del directori d'inici de l'usuari. També és compatible amb el protocol WINS (*Windows Internet Naming Service*), que permet a clients Windows de diverses subxarxes negociar noms i adreces.

La interoperavilitat amb Novell també és possible. Novell sempre ha treballat per proporcionar als seus servidors Netware solucions de compatibilitat amb Macintosh (des de la versió 4.x. Netware inclou Netware per a Macintosh, una extensió del programari que permet compartir arxius i impressores amb Macintosh). Des de Mac OS X, els servidors Netware 5.xi 6 es veuen com un veritable servidor AppleShare sobre IP.

1.4.2 Connexió a volums NFS

Si la xarxa on pertany l'equip Mac té servidors NFS, podeu utilitzar l'opció *Connectar al servidor ...* del menú *Anar* per accedir als arxius compartits. A diferència dels servidors SMB, haureu d'indicar el camí NFS fins als arxius en qüestió.

La sintaxi correcta per l'URL de servidors NFS és: nfs: / / nomdelservidor.com / ruta /.

Cal tenir molt en compte que no podeu utilitzar les utilitats de la línia d'ordres ni *Serveis per a NFS* per administrar versions anteriors.

Utilitzeu *Servidor per a NFS* per controlar l'accés dels usuaris i dels grups als recursos de *Serveis per a NFS* mitjançant *Active Directory*. Per aconseguir-ho, us caldrà l'identificador d'usuari o l'identificador de grup segons quin sigui el cas.

Si agregueu una nova unitat en l'equip que és el servidor d'NFS, tingueu en compte que haureu de modificar permisos. El directori arrel de la unitat haurà de tenir els permisos adequats perquè no tothom hi pugui escriure.

1.4.3 Mac OS X i Active Directory

El sistema operatiu Mac OS X és compatible amb *Active Directory*, cosa que permet integrar més fàcilment els Mac a les xarxes basades en Windows. És

possible adoptar el mateix sistema d'autenticació mitjançant contrasenya que s'utilitza en els sistemes Windows, i emmagatzemar el vostre directori d'inici en un servidor Windows remot.

Un aspecte a tenir molt en compte és utilitzar un nom de màquina i contrasenya correctes. Aquestes dades han de contenir caràcters vàlids per a Windows i no tenir una longitud de més de setze caràcters. Amb la utilitat *dsconfigad* podeu utilitzar noms de màquines i contrasenyes no vàlids per a *Active Directory*. Amb *dsconfigad* es canvien de forma automàtica les dades per tal que siguin vàlides per a *Active Directory*.

Per poder utilitzar recursos de Windows Server 2008 en màquines amb sistemes operatius Mac, caldrà que el protocol *AppleTalk* estigui funcionant correctament. Per activar el protocol *AppleTalk* seguiu els passos següents:

1. Seleccioneu *Preferències del sistema* al menú *Apple*.
2. Cliqueu a sobre de la icona *Xarxa*.
3. Al menú *Mostrar* seleccioneu *Ethernet integrada* o bé *Airport*.
4. Cliqueu a la fitxa *AppleTalk*.
5. Marqueu la casella *Activar AppleTalk*.
6. Cliqueu a *Aplicar ara*.

1.4.4 Mac OS X i Open Directory

Apple ha integrat Samba i *Open Directory* per l'autenticació d'usuaris. No és necessari mantenir bases de dades de serveis de directori separades per als sistemes Windows, de manera que els usuaris poden accedir als seus arxius de xarxa des de sistemes tant Windows com Macintosh amb el mateix nom d'usuari i contrasenya.

Des del punt de vista del manteniment, resulta de gran utilitat treballar amb *Open Directory*, ja que el tècnic només ha de preocupar-se de mantenir un únic directori, independentment de les plataformes que es trobin dins la xarxa informàtica.

Els passos per crear un domini basat en *Open Directory* són:

1. Obrir la utilitat *MacOS X Server Admin*.
2. Al menú *Ordinadors i serveis*, que trobareu a l'esquerra de la pantalla, seleccioneu *Open Directory*.
3. A la part central de la pantalla, dins la fitxa *General*, seleccioneu el rol *Open Directory*.
4. Amb el botó *Configuració*, que trobareu a la part inferior de la pantalla, podreu fer-ne la configuració a mida.

5. Per finalitzar, haureu de crear un compte d'usuari local no compartit que permeti la gestió administrativa d'*Open Directory*.

1.4.5 Emmagatzematge en xarxa

Actualment s'utilitzen servidors d'emmagatzematge en xarxa per a emmagatzemar els arxius d'un grup de treball o d'un departament. Aquest sistema es pot usar amb transparència pels Mac.

La majoria dels servidors d'emmagatzemament en xarxa de nivell bàsic són compatibles amb diversos protocols d'arxius compartits, com ara AppleShare. Això vol dir que l'equipament pot utilitzar-se per a compartir arxius sense esforç en entorns heterogenis constituïts per ordinadors Mac OS X / PC. La majoria tenen una interfície web d'administració i poden configurar i administra-se des d'un equip Mac.

Quan els servidors d'emmagatzematge no són compatibles amb AppleShare, el sistema Mac OS X ofereix diverses alternatives igual d'efectives mitjançant sistemes d'arxiu NFS d'Unix i de web estàndard WebDAV. El sistema operatiu Mac OS X garanteix l'accés a l'emmagatzematge en xarxa, fins i tot a servidors com els de Network Appliance o EMC.

1.4.6 Mac i PC: impressores compartides en LAN

L'ús compartit d'impressores és una de les tasques més desitjades en els escenaris heterogenis.

Amb Mac OS X, les opcions d'impressió s'han ampliat considerablement. Aquest sistema operatiu és compatible amb totes les impressores PostScript del mercat. Les impressores gestionades i compartides amb Mac OS X Server es veuen des de les estacions Windows com impressores de PC i com impressores Mac per les estacions amb Mac OS X. Des de Windows, les cues d'impressió de Mac OS X Server es veuen com cues SMB/CIFS estàndard. Amb el controlador adient, apareixen com impressores compartides en l'entorn de xarxa Windows.

Les estacions de treball Mac imprimeixen a través de Mac OS X Server amb les seves eines habituals (el *Centre d'impressió*). Els serveis d'impressió de Mac OS X també estan a l'abast de les estacions de treball Unix via LPD/LPR. De la mateixa manera, no cal utilitzar servidors d'impressió compatibles amb AppleTalk, ja que es pot utilitzar el sistema d'impressió LPD/LPR d'Unix.

1.5 Utilització dels diferents servidors de fitxers

És molt important que comproveu la possibilitat d'utilitzar determinats sistemes de fitxers en el sistema operatiu en xarxa que necessiteu implantar. Heu de saber els problemes de compatibilitat que es poden manifestar en els vostres dissenys abans d'implementar cap solució.

En la taula 1.2 es presenta un resum on es relacionen alguns dels sistemes operatius en xarxa dels servidors més comuns amb els diferents sistemes de fitxers que us podeu trobar, i s'indica si és possible utilitzar-los.

Taula 1.2. Possibilitat s'ús de diferents servidors de fitxers segons el sistema operatiu.

Sistema operatiu	AFP en AppleTalk	AFP sobre IP	SMB/CIFS	NFS
Mac OS X Server	Sí	Sí	Sí	Sí
Windows 2008 Server	Sí	Sí	Sí	Sí
Netware 6	Sí	Sí	Sí	Sí
Linux	Sí	Sí	Sí	Sí
Solaris	Sí		Sí	Sí

2. Integració de sistemes amb GNU/Linux

Per a l'assoliment dels objectius, és imprescindible que l'alumne conegui el procés d'instal·lar i configurar les aplicacions que s'utilitzen per compartir recursos com carpetes, impressores, etc. entre màquines amb diferents sistemes operatius instal·lats. L'aplicació més utilitzada per a la compartició de recursos entre sistemes operatius diferents és Samba. Així doncs, cal que l'alumne aprengui i practiqui la instal·lació i configuració del paquet Samba perquè funcioni tant en un grup de treball amb màquines Windows i GNU/Linux i com a controlador primari de domini de sistemes Windows NT.

Un altre punt interessant que tractarem és la integració entre els usuaris, grups i permisos dels sistemes Windows i GNU/Linux que es fa utilitzant Samba. Cal tenir clar la manera en què Samba permet garantir la seguretat a l'hora d'accedir als recursos des de diferents plataformes. La millor manera d'entendre el funcionament del mecanisme de compartició de recursos amb Samba és mitjançant alguns exemples de compartició de recursos instal·lats en diferents sistemes operatius. També és molt interessant saber com funciona la integració entre Samba i LDAP per tal de garantir la seguretat, fiabilitat, escalabilitat i robustesa en un escenari de xarxa heterogeni.

2.1 Integració de sistemes lliures i propietaris amb Samba

Samba és un paquet de programes que implementa en sistemes basats en Unix (GNU/Linux) una dotzena de serveis i una dotzena de protocols, els quals ens permeten compartir fitxers i impressores entre els equips d'una xarxa local.

Samba té com a característica principal que ens permet compartir recursos entre màquines Windows i GNU/Linux connectades en xarxa, per tant possibilita compartir recursos en un escenari heterogeni.

Veiem els protocols implementats pel paquet Samba:

- NetBIOS sobre TCP/IP (NetBT).
- SMB (reanomenat CIFS).
- DCE/RPC o MSRPC: el paquet de protocols de xarxes veïnes *The Network Neighborhood suite of protocols*.
- WINS: també conegut com a *NetBIOS name server* (NBNS).
- *NT Domain* i el seu conjunt de protocols:
  - *NT domain logons*.

  - *Secure accounts manager* (SAM) base de dades.
  - *Local security authority* (LSA) servei.
  - *NT-style printing servei* (SPOOLSS).
  - *Active directory logon* (Kerberos i LDAP).
  - Protocols de compartició d'impressores.

Tot aquest conjunt de protocols són necessaris per a la integració entre màquines Windows i GNU/Linux.

NetBIOS

NetBIOS és necessari per al funcionament de Samba, excepte en el cas d'una xarxa amb *Active Directory on SMB* pot treballar directament sobre TCP/IP sense utilitzar NetBIOS.

El paquet Samba instal·lat sobre una màquina amb un sistema GNU/Linux permet que la màquina ofereixi una sèrie de serveis i ocupi una sèrie de rols dins d'una xarxa integrada, similars als que oferiria una màquina amb un sistema Windows NT instal·lat. Així doncs, veiem els serveis que ofereix i el rols que pot ocupar un servidor Samba i els que no.

Entre les tasques que **pot fer** un servidor Samba hi ha:

- Servidor de fitxers.
- Servidor d'impressores.
- Servidor DFS de Microsoft.
- Controlador de domini principal.
- Autenticació de màquines amb Windows 95/98/Me.
- Autenticació de màquines amb Windows NT/2000/XP
- *Local master browser* i *backup*.
- *Domain master browser*.
- Servidor primari de WINS.

Entre les tasques que **no pot fer** un servidor Samba es troben:

- Controlador de domini secundari (*backup*) quan el servidor primari és Windows.
- Controlador de domini *active directory*.
- Servidor secundari de WINS.
- No ofereix *group policy objects* (d'*active directory*).
- No proporciona *machine policy objects*.
- No conté els *logon scripts* d'*active directory*.
- No proporciona el control de les aplicacions de programari que té *active directory*.

Single sign-on (SSO)

SSO és un procediment d'autenticació que habilita l'usuari per accedir a diversos sistemes amb una sola instància d'identificació. Exemples d'aquest procediment són Kerberos o OpenID.

El paquet Samba es troba actualment en la versió 3 i entre els avantatges podem destacar:

- Reduir el cost total de propietat.
- Ens proporciona suport global.

- Es pot executar més d'un servidor SMB/CIFS per cada sistema GNU/Linux. (*dynamic SMB servers*).
- Creació de fitxers d'inici de sessió *logon on-the-fly*.
- Creació de directives *on-the-fly*.
- Gran estabilitat, fiabilitat, rendiment i disponibilitat.
- Control del servidor amb SSH.
- Flexibilitat a l'hora d'escollir *backends* (tdbsam, ldapsam...).
- Habilitat per implementar una solució SSO real (no solament per a Windows).
- Habilitat per tenir sistemes d'autenticació distribuïts amb un mínim ús de trànsit de xarxa WAN.

2.1.1 Utilitats de Samba

Principalment Samba permet que màquines GNU/Linux i Windows coexisteixin en la mateixa xarxa, a més d'altres funcions utilitzades en sistemes homogenis (és a dir, en conjunts de màquines connectades en xarxa amb el mateix sistema operatiu). D'aquesta manera ens proporciona una de les eines bàsiques per entendre i compartir recursos entre dos dels sistemes operatius més utilitzats en l'actualitat. Des del punt de vista d'un escenari heterogeni, Samba pot ser útil per al següent:

- Substituir un servidor Windows, si és necessita de les seves funcionalitats però no és pot pagar.
- Evitar el pagament de les llicències que requereix Microsoft per cada client Windows que es connecta al servidor (Client Access Licenses CALs). Aquestes llicències són massa cares i ens les podem estalviar.
- Proveir una àrea de dades comuna per fer una transició de Windows a GNU/Linux.
- Compartir impressores entre xarxes Windows i xarxes GNU/Linux.
- Integrar l'autenticació d'usuaris tant en GNU/Linux com en Windows.

- Integrar a la xarxa altres sistemes operatius.

El fet que un servidor Samba pugui adquirir diversos rols i treballar en combinació amb altres serveis ens permet situar-lo en diferents escenaris heterogenis. És molt important conèixer els possibles escenaris en què podem utilitzar el servei Samba per integrar màquines Windows i GNU/Linux i compartir recursos entre elles.

2.2 Domini Windows NT

Un **domini Windows NT** és una agrupació lògica de màquines de xarxa que comparteixen un directori centralitzat. Aquest model segueix una arquitectura de xarxa client/servidor on múltiples clients comparteixen una base de dades centralitzada localitzada en un o més servidors de domini.

La base de dades d'un domini Windows NT pot contenir:

- Comptes d'usuari.
- Informació de seguretat dels recursos del domini per tal de garantir el control d'accés dels usuaris als recursos.

La base de dades des de Windows 2000 s'anomena *Active Directory*, està basada en LDAP, i treballa de forma diferent a les versions anteriors.

Les màquines que emmagatzemen la base de dades del domini s'anomenen **Controladors de domini** (*Domain Controllers*).

Entre els avantatges de la utilització d'un domini Windows NT podem destacar:

- Les estacions Windows i les aplicacions relacionades poden gaudir de Single Sign On (SSO).
- Els usuaris membres del domini i els seus permisos poden ser gestionats de forma centralitzada des d'una sola base de dades *Security Account Manager* (SAM) anomenada Domain SAM.
- Cal indicar que només poden utilitzar dominis les versions NT4/200x i XP Professional (no XP *Home Edition*) del sistema Windows.
- Les estacions de treball del domini poden ser controlades utilitzant *policy files* (NTConfig.POL) i perfils d'escriptori.
- Se centralitza la feina dels administradors de xarxa.

Aquest tipus de sistemes normalment s'utilitzen en empreses o organitzacions mitjanes/grans.

Un servidor Samba pot substituir servidors Windows en diferents rols dins d'un domini Windows NT. De fet la versió actual del servidor Samba s'integra totalment en dominis Windows NT.

2.3 Grups de treball Windows

Els **grups de treball Windows** són un model d'agrupació lògica de màquines en xarxa que segueix un paradigma d'igual a igual (*peer-to-peer*). És a dir, en una xarxa amb grups de treball no hi ha servidors principals, sinó que totes les màquines tenen entre si una relació d'igual a igual. Les màquines són independents (*Stand-Alone*) i no comparteixen una base de dades com en el cas dels dominis.

Els grups de treball són utilitzats sobretot per a la compartició de recursos entre les màquines pertanyents al mateix grup de treball. Els grups de treball són considerats més útils per a xarxes petites.

Les màquines amb sistemes GNU/Linux i Samba, poden formar part dels grups de treball i compartir recursos a través d'ells amb màquines Windows.

Els grups de treball es consideren difícils de manejar més enllà d'una dotzena de clients, i els manquen algunes característiques com SSO, escalabilitat, capacitat de recuperació de desastres, i diverses característiques més de seguretat.

Dominis mixtos

El servei Samba es pot combinar amb altres serveis com LDAP per generar una cosa similar a *Active Directory* que integri màquines Windows i GNU/Linux amb programari lliure de manera segura, potent i escalable. A més, Samba també permet que màquines GNU/Linux puguin accedir a un domini *Active Directory* amb un controlador de domini Windows.

2.4 Tipus de configuracions d'un servidor Samba

Samba s'integra totalment en dominis de Windows NT4. En aquests entorns Samba pot dur a terme diferents tasques o ocupar diferents rols. Així doncs, per conèixer millor les funcions que pot fer el servei Samba, cal que veiem primer els possibles rols d'un servidor en un domini Windows NT. Així doncs, una màquina amb un sistema Windows NT Server té tres possibles configuracions:

1. Controlador primari de domini o *primary domain controller* (PDC). Un PDC es correspon amb el centre nerviós d'un domini Windows NT. L'objectiu principal d'un controlador de domini és garantir la seguretat, mitjançant el control del procés d'autenticació i proporcionar accés als recursos. La base de dades on el controlador de domini emmagatzema la informació dels usuaris s'anomena SAM (*security account manager*). Només pot haver-hi un PDC per domini.

2. Controlador secundari de domini o *backup domain controller* (BDC). El seu objectiu és tenir una replica de la base de dades, SAM, del PDC com a mesura de seguretat.

Samba pot fer de BDC d'un altre servidor PDC Samba però no d'un servidor PDC Windows.

El fet de tenir un o més BDC en un domini permet millorar la disponibilitat del sistema i la seva escalabilitat. En una xarxa amb molts clients de domini el fet de tenir un sol servidor PDC on s'autentiquin tots els clients pot generar un coll d'ampolla de la xarxa.

El PDC conté la còpia mestra de la base de dades SAM. En el cas que l'administrador vulgui modificar la informació de la base de dades SAM ens podem trobar amb dues opcions:

- La modificació es fa en una zona del domini associada al PDC. Aleshores es modifica directament els fitxers de SAM i són replicats als BDC.
- La modificació és fa en una zona del domini associada al o als BDC: Per tant, no es modifica directament el fitxer SAM. Al BDC es genera un fitxer anomenat fitxer delta que conté les diferències entre el SAM original i el modificat. Aleshores el BDC avisa el PDC per començar un procés de sincronització. Un cop sincronitzat el PDC inicia un procés de sincronització amb la resta de BDC en el cas que n'hi hagi més. Poden haver-hi tants BDC com calgui per domini.

3. Servidor membre de domini o *domain member server* (DMS). Els servidors membres de domini són servidors amb diferents tipus de serveis o recursos compartits que es troben dins d'un domini i s'autentiquen a través d'un PDC. Aquests servidors no són PDC ni BDC i, per tant, no tindran una còpia de la base de dades d'usuaris. Poden haver-hi tants servidors membres com calgui per domini.

Ordre testparm

Podem saber el rol del nostre servidor amb l'ordre testparm:
sudo testparm

....

Server role:
ROLE_STANDALONE

....

Una vegada conegudes les funcions realitzades per un servidor Windows a un domini NT veiem les possibles configuracions d'una màquina amb Samba.

Un servidor Samba pot configurar-se com a:

- *Stand-alone server*. No utilitza dominis, és la configuració normal per als grups de treball.
- *Domain member server* o membre de domini. Samba suporta dos subtipus del tipus membre de domini:
  - *Active directory domain server*.
  - NT4 *Style domain domain server*.
- *Domain controller server*. N'hi ha tres subtipus:
  - *Primary domain controller* (PDC).
  - *Backup domain controller* (BDC).
  - *ADS domain controller*.

Samba no pot (s'està treballant a la versió 4) treballar com a ADS *domain controller* i no pot ser un BDC d'un servidor Windows, però sí d'un servidor Samba.

Una vegada conegudes les funcionalitats d'un servidor Samba, resulta interessant tractar el procés de configuració de les més importants. Abans de passar a la configuració, però, hem de fer el procés d'instal·lació de Samba.

2.5 Instal·lació servidor i client Samba

Per poder treballar amb el servei Samba i configurar-lo en algun dels diferents papers que pot ocupar, primer cal dur a terme el procés d'instal·lació. La instal·lació dels paquets que ens proporcionaran tant el servidor com el client Samba en una màquina GNU/Linux, en concret Ubuntu 9.04, es pot fer fàcilment de dues maneres.

1. Mitjançant la línia d'ordres, utilitzant l'ordre:

```
$sudo apt-get install samba smbclient smbfs
```

2. Mitjançant l'entorn gràfic. Simplement hem de prémer el botó dret sobre una carpeta del nostre equip, que vulguem compartir, i seleccionar l'opció *Opcions de compartició* del menú contextual. A continuació s'obrirà un quadre de diàleg en el qual marquem la casella *Comparteix aquesta carpeta* i premem el botó *Crear compartició*. Automàticament, la primera vegada que fem aquesta acció, ens avisarà que ha d'instal·lar el servei Samba; si acceptem i li posem la contrasenya de superusuari, a continuació ens preguntarà si deixem que Nautilus afegeixi els permisos necessaris per poder compartir la carpeta. Si acceptem començarà la instal·lació dels paquets Samba, smbclient i samba-common, entre d'altres.

2.6 Configuració de Samba a un grup de treball

Podem configurar el servidor Samba per compartir recursos dins d'un grup de treball entre màquines Windows i GNU/Linux. El tipus de configuració o rol que ocuparà Samba serà el d'*Stand-Alone Server*. Els servidors *Stand-Alone* són independents dels controladors de domini de la xarxa. Aquests servidors no són membres del domini, sinó que funcionen com a servidors dins d'un grup de treball. Com hem comentat la filosofia del grup de treball és d'igual a igual (*peer-to-peer*) i per tant existiran tants *Stand-Alone Servers* dins d'un grup de treball com màquines amb recursos per a compartir.

Aquest tipus de configuració és la manera més senzilla i ràpida per compartir recursos entre màquines en un escenari heterogeni, però també és la configuració que presenta més problemes quant a escalabilitat, seguretat i eficiència.

El paper d'un servidor Samba després d'instal·lar-lo és per defecte *Stand-Alone*, per tant no hem de fer res per a configurar-lo com a tal. Així doncs, amb el servidor Samba configurat com a *Stand-Alone Server*, resulta interessant conèixer el procés que s'ha de portar a terme per a la compartició de recursos en un grup de treball amb màquines Windows i GNU/Linux.

2.6.1 Compartició de recursos a un grup de treball heterogeni

La compartició de recursos en un grup de treball heterogeni és el mecanisme que permet l'accés a diferents recursos, principalment directoris i impressores ubicats en màquines amb sistemes operatius diferents, però que, mitjançant la configuració de les eines adequades, com Samba, es troben lògicament dins del mateix grup de treball.

Per poder compartir recursos en un grup de treball entre màquines Windows i GNU/Linux, hem de fer una sèrie de passos a ambdós tipus de màquines. Els passos per a compartir directoris i carpetes són els següents:

- Compartició de directoris.
- Compartició d'impressores.

Compartició de directoris

La compartició de directoris en un grup de treball heterogeni suposa que qualsevol màquina, tingui el sistema operatiu que tingui instal·lat, pot accedir als directoris configurats per compartir i ubicats en una altra màquina amb un sistema operatiu diferent situada lògicament dins del mateix grup de treball.

Per a la compartició de directoris a un grup de treball amb màquines GNU/Linux i Windows, a les màquines GNU/Linux hem de fer els passos següents:

1. Instal·lar el servei i el client Samba.
2. Configurar el nom del grup de treball, el nom netbios de l'equip i les possibles opcions de seguretat a la secció global de fitxer `/etc/samba/smb.conf`. Aquesta configuració la podem fer tant manualment com gràficament.

   Per exemple, per crear el grup de treball *INSTITUT*, anomenar a la nostra màquina *ALFA* i establir el nivell de seguretat d'usuari, el nivell per defecte, amb l'eina SWAT, faríem la configuració que es veu en la figura 2.1.
3. Afegir els directoris que vulguem compartir a la secció corresponent del fitxer de configuració de Samba, `/etc/samba/smb.conf` i especificar el valor de les diferents opcions per a cada recurs.

   Per exemple la configuració per a compartir la carpeta *professors*, amb accés a usuaris convidats, que no sigui de només lectura, que estigui disponible i que es pugui veure quan un client accedeix als recursos compartits de la màquina Swat es faria com en la figura 2.2.

FIGURA 2.1. Creant un grup amb l'eina SWAT

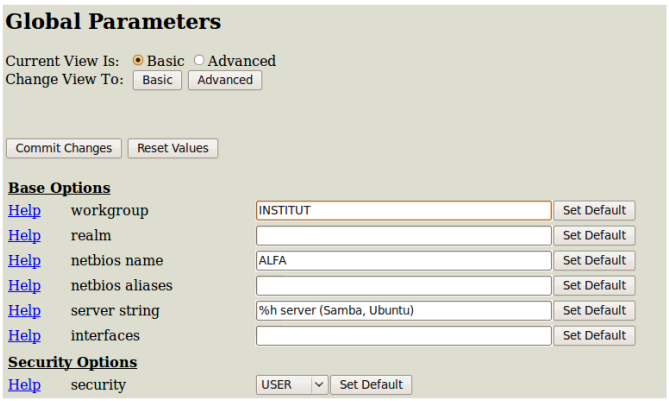
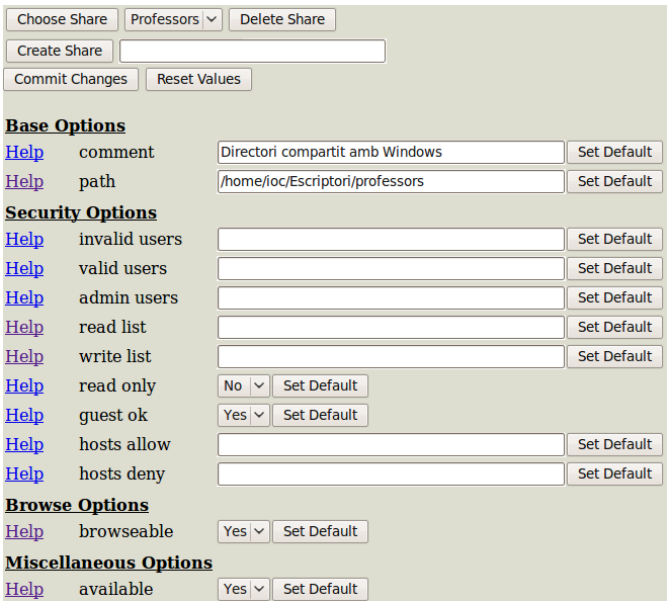


FIGURA 2.2. Compartint una carpeta amb l'eina SWAT



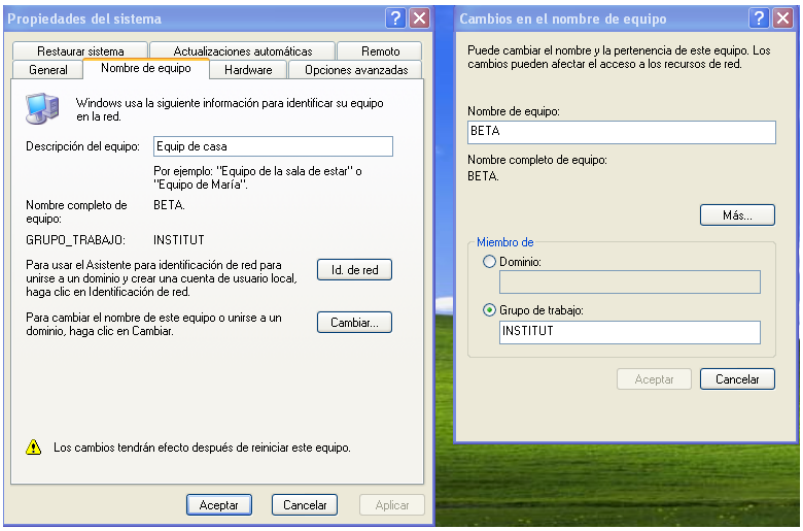
L'únic requisit és que els directoris que configurem a Samba existeixin realment al sistema. Amb aquest pas finalitzaríem la configuració de la màquina GNU/Linux per compartir directoris.

Per a la compartició de directoris a un grup de treball amb màquines GNU/Linux i Windows, a les màquines Windows hem de fer els passos següents:

1. No cal instal·lar cap programa ja que incorporen el protocol SMB per a la compartició de recursos integrat. Només cal tenir totes les opcions de compartició habilitades. Així, el primer pas serà establir el nom del grup de treball que volem crear o al qual volem afegir l'equip, si ja existeix, i especificar el nom amb el qual volem que s'identifiqui l'equip al grup.

Per exemple a Windows XP cal prémer botó dret damunt de la icona *Mi PC* i seleccionar la pestanya *Nom d'equip*. A continuació premem el botó *Canviar* i establim als quadres corresponents el nom de l'equip i el nom del grup de treball del qual volem formar part (figura 2.3). Una vegada fets els canvis hem de reiniciar l'equip.

FIGURA 2.3. Canviant el nom de l'equip a Windows XP

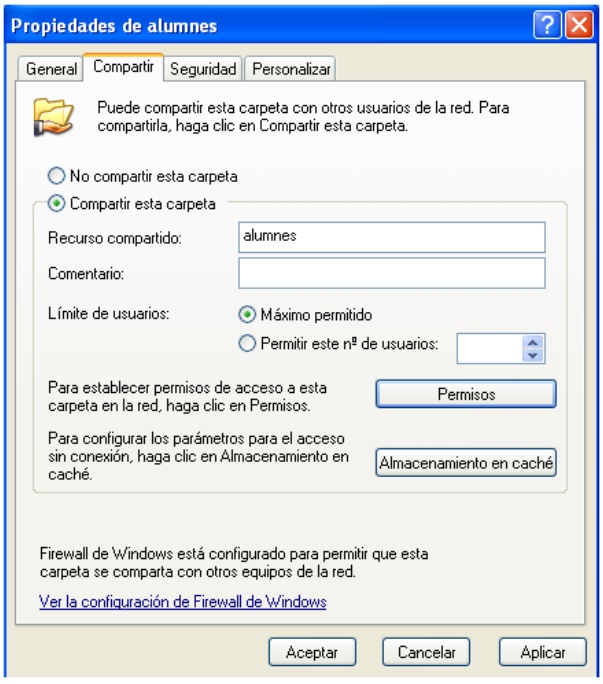


2. Especificar els directoris que volem compartir.

Per exemple, per a compartir una carpeta anomenada *alumnes* premem botó dret damunt de la carpeta i seleccionem *Propietats*, a continuació anem a la pestanya *Compartir* i seleccionem l'opció *Compartir aquesta carpeta* i prenem el botó *Acceptar*. Veiem l'exemple en la la figura 2.4.

Per canviar els permisos de la carpeta en Windows XP, abans hem d'activar la visualització dels permisos. Per fer això dins d'una carpeta anem al menú *Eines*> *Opcions de carpeta*, i a la pestanya *Veure* desmarquem l'ultima opció *Utilitzar ús compartit simple d'arxius*. Així, quan tornem a seleccionar les propietats de la carpeta, ens apareixerà la pestanya *Seguretat* on podrem establir els permisos de cada carpeta per als diferents usuaris.

FIGURA 2.4. Compartint una carpeta amb Windows XP



Així finalitzem la configuració de la màquina Windows per compartir carpetes.

Una vegada configurats els grups de treball i els recursos a compartir a cadascuna de les màquines, podem accedir als recursos d'altres màquines mitjançant el menú *Els meus llocs de xarxa* a Windows i *Llocs> Xarxa* a Ubuntu.

Aquestes dues ubicacions tant a Windows com a Ubuntu contenen un grup d'accessos directes als ordinadors, impressores i altres recursos compartits en una xarxa.

Els accessos directes són creats automàticament en l'equip cada vegada que s'obre un recurs compartit de xarxa, com una nova impressora o una carpeta compartida.

Així, mitjançant aquestes aplicacions el client pot veure, administrar, moure, copiar, guardar i reanomenar fitxers i carpetes, sempre depenent dels permisos que aquestes tinguin, ja que són emmagatzemades en un altre ordinador com si es tractés d'arxius i carpetes emmagatzemats en l'ordinador mateix.

Compartició d'impressores

> La compartició d'impressores en un grup de treball heterogeni suposa que qualsevol màquina, tingui el sistema operatiu que tingui instal·lat, pot accedir a les impressores configurades per compartir i instal·lades en una altra màquina amb un sistema operatiu diferent i situada lògicament dins del mateix grup de treball.

Els sistemes Windows 95, 98 y ME solen tenir problemes per comunicar-se amb Samba a l'hora d'imprimir. Cal afegir uns paràmetres al fitxer /etc/samba/smb.conf per solucionar aquest inconvenient:

```
print command = lpr -P %p -o raw %s -r
 lpq command = lpstat -o %p
 lprm command = cancel %p-%j
 printer admin = fulano, @opers_impresion
```

Suposem que tenim la **impressora instal·lada a una màquina Windows** i volem compartir-la amb una maquina Ubuntu. Aleshores hem de seguir una sèrie de passos:

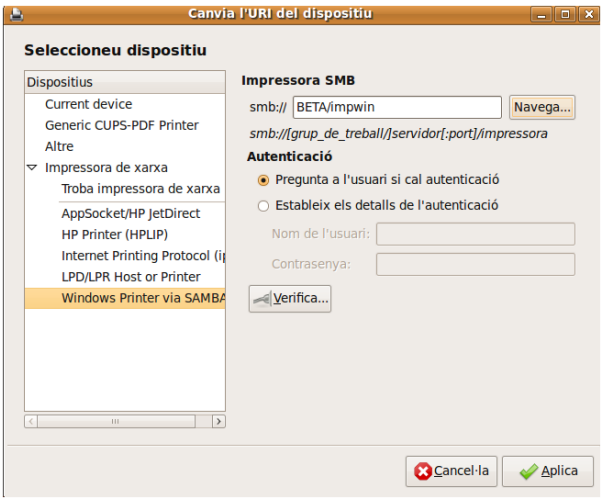
1. Configurar la impressora per compartir-la. Per fer això anem a *Impressores i faxos*, prenem el botó dret damunt de la impressora a compartir i seleccionem *Propietats*. Seleccionem la pestanya *Compartir* i marquem l'opció *Compartir aquesta impressora*.

2. Una vegada configurada la impressora compartida a Windows. Anem a l'equip amb Ubuntu i des del menú *Sistema >Administració> Impressió* obrirem la finestra on seleccionem la icona *Nou >Impressora* i ens cercarà automàticament les impressores que tenim instal·lades tant localment com remotament.

Si no ens apareix la impressora com a detectada, haurem de seleccionar la opció

Windows Printer via Samba i especificar la ruta cap a la màquina Windows que té la impressora compartida com es veu en la figura 2.5.

FIGURA 2.5. Seleccionant una impressora via Samba



A continuació prenem el botó *Aplica* i ens mostrarà una finestra on podem seleccionar entre diverses opcions; escollir el model de la impressora, passar els controladors via fitxer PPD o cercar en la xarxa un controlador per a la impressora. Si escollim la marca de la impressora ens permetrà triar entre els diferents models de la marca per instal·lar els controladors més adients a la impressora. Si continuem *Endavant*, ens preguntarà si volem imprimir una pàgina de prova per a comprovar que la instal·lació s'ha realitzat correctament.

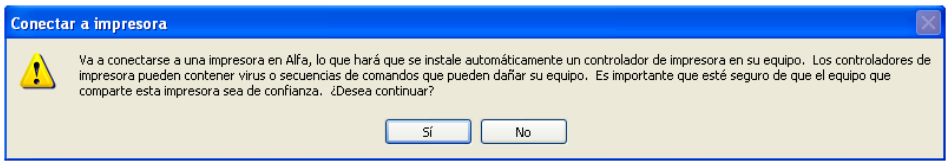
Suposem que tenim la **impressora instal·lada a una màquina Ubuntu** i volem compartir-la amb una màquina Windows. Aleshores hem de seguir una sèrie de passos:

1. Configurar Ubuntu per a compartir la impressora, això ho podem fer amb la interfície web de CUPS. Si tenim l'eina CUPS instal·lada, anem amb l'explorador web a l'adreça http:localhost:631 i marquem les opcions *Show printers shared by other systems* i *Share published printers connected to this system* a la secció *Server* de la pestanya *Administrador*.

A la pestanya *Printers*, podem comprovar les impressores que tenim instal·lades i preparades per a compartir.

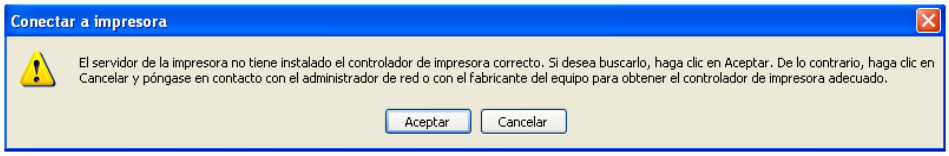
2. Una vegada configurat el servidor d'impressió a Ubuntu, anem a l'equip Windows. Anem a *Els meus llocs de xarxa* i accedim a la màquina amb Ubuntu on hem configurat la impressora per a compartir. Comprovem si ens apareix un accés directe a la impressora. Si es així només cal fer doble clic sobre la icona de la impressora i ens mostrarà el quadre de la figura 2.6.

Figura 2.6. Connectant a una impressora de xarxa des de Windows



Si seleccionem l'opció *Sí*, potser que no reconegui els controladors instal·lats al servidor i ens demani que els instal·lem a l'equip Windows (figura 2.7).

Figura 2.7. Alerta! No es localitzen els controladors



Si acceptem ens mostrarà un quadre on haurem de seleccionar la marca i model de la impressora o instal·lar els controladors des d'un CD (figura 2.8).

Figura 2.8. Instal·lació de controladors amb Windows

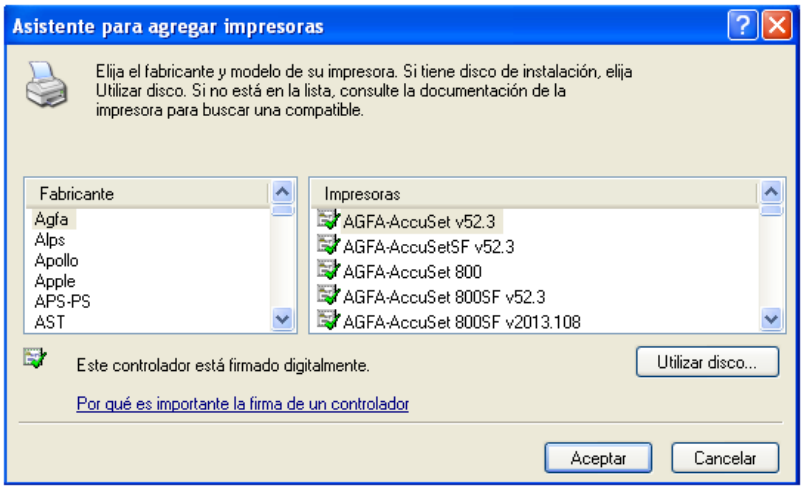
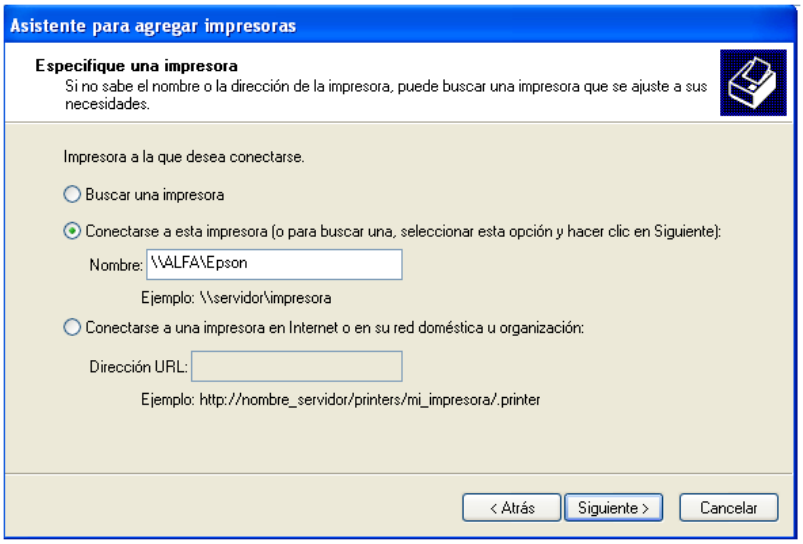


Figura 2.9. Assistent per instal·lar impressores



Si no ens apareix l'accés directe a la impressora a la màquina Ubuntu en *Els meus llocs de xarxa*, haurem de fer servir *Assistent per afegir impressores* (figura 2.9) i seleccionar la ubicació de xarxa on trobar la impressora de la màquina Ubuntu en aquest cas.

La resta de passos una vegada seleccionem la impressora són els comentats anteriorment.

2.7 Navegació a les xarxes Windows

Per cada grup de treball de Windows ha d'haver-hi una màquina que funcioni com a *Browse Master*. Aquesta màquina és la que s'encarrega d'emmagatzemar la informació de màquines de xarxa (noms) i els recursos que comparteixen. Cada cop que s'encén un sistema Windows el primer que fa el programari de xarxa és buscar un *Browse Master* a la xarxa:

1. Si no es troba un *Browse Master* es comença un procés anomenat d'elecció de *Browse Master*.
2. Només un sistema amb l'opció de compartir fitxers i impressores pot ser escollit per a ser un *Browse Master*.
3. Si hi ha diferents tipus de sistemes operatius Windows, se segueix l'ordre següent de preferència a l'hora d'escollir *Browse Master*:
   - Windows NT or 2008 server o qualsevol altra versió de servidor abans que una estació de treball (*workstation*).
   - Windows XP (NT 5.1).
   - Windows 2000 Workstation (NT 5.0).
   - Windows NT4 Workstation.
   - Windows ME.
   - Windows 98.
   - Windows 95.
   - Windows 3.x.

Cada sistema envia la seva llista de recursos disponibles al *Browse-Master*. Cada cop que ens connectem a "Mis sitios de red Red" de Windows es fa una consulta al *Browse-Master* per tal que ens mostri la llista de màquines que comparteixen recursos.

Aquest sistema és molt poc eficient ja que el procés d'elecció d'un *Browse-Master* pot trigar uns minuts un cop activada la màquina. A més, un cop finalitzat el procés d'elecció, si una màquina s'afegeix a la xarxa o surt de la xarxa pot trigar en actualitzar-se la xarxa fins a 15 minuts.

A més del *Browse Master* existent als grups de treball, a una xarxa Windows podem trobar també els *Masters Browsers* dels dominis:

A l'hora de fer servir un DMB cal tenir en compte de totes maneres les normes d'encaminament o els possibles tallafocs dels encaminadors (*routers*).

- ***Domain Master Browser***: Aquest és el *Browser* principal per a un domini. En un domini Windows NT, el controlador de domini primari (PDC) sempre guanya les eleccions per a convertir-se en l'examinador principal de domini. Només pot haver-hi una màquina que ocupi aquest rol per xarxa o domini. A més el DMB necessita del servei WINS per a funcionar correctament.
- ***Local Master Browser*** és *Master Browser* local en un segment de xarxa concret. La seva finalitat és proporcionar llistes de recursos als clients i mantenir el *Domain Master Browser* al dia amb les llistes de recursos. Es tracta normalment d'un controlador de domini de reserva (BDC). Aquest navegador ha de tenir suport per a un protocol enrutable com TCP / IP o IPX / SPX, ja que el *Domain Master Browser* pot trobar-se a una subxarxa diferent. Només hi ha d'haver una màquina que faci de *Local Master Browser* per segment de xarxa.

2.7.1 Configuració del Browsing a Samba

El servidor *Browser* o servidor de navegació d'una xarxa és la màquina que ens permet navegar i localitzar els recursos disponibles a la xarxa. El servidor Samba disposa d'una sèrie d'opcions que permeten configurar-lo com a *Browser* de xarxa. Veiem quins paràmetres són i què signifiquen:

- **os level**: permet tenir més possibilitats de guanyar les eleccions a l'hora d'escollir un *Master Browser*.
- **lm announce**: utilitzat pel client OS/2 d'IBM.
- **lm interval**: utilitzat pel client OS/2 d'IBM.
- **preferred master**: s'utilitza per forçar eleccions.
- **local master**: estableix la màquina com a LMB.
- **domain master**: estableix la màquina com a DMB.
- **browse list**: per defecte yes. No es varia mai.
- **enhanced browsing**: activat per defecte. Implementa una sèrie de millores a Samba que no estan disponibles a Windows(vegeu man smb.conf).

Amb l'ordre nmblookup a GNU/Linux podem cercar qui és el *Master Browser* d'un segment de xarxa.

```
nmblookup –M WORKGROUP
querying WORKGROUP on 192.168.56.255
192.168.56.101 WORKGROUP
```

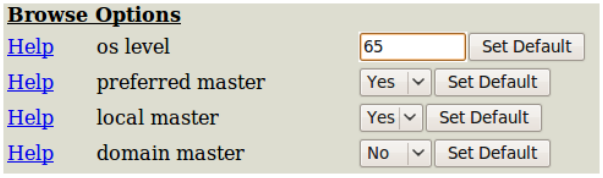
També podem utilitzar l'ordre net a GNU/Linux:

```
net lookup master
192.168.56.101
```

2.7.2 Configuració de Samba com a Local Master Browser

Per tal que el servidor Samba sigui escollit com a *Local Master Browser* d'un segment de xarxa hem d'especificar les opcions següents a la secció global del fitxer /etc/samba/smb.conf (figura 2.10).

Figura 2.10. Secció global del fitxer



etc/samba/smb.conf

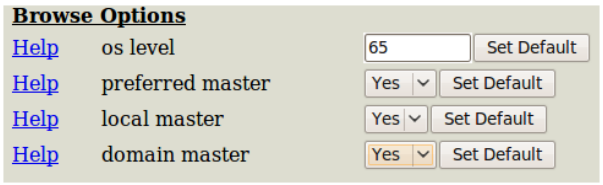
Per defecte, Samba "guanya" totes les eleccions a *Local Master Browser* davant tots els sistemes Windows excepte amb un PDC Windows NT. Això significa que una configuració errònia del servei Samba pot aïllar la xarxa local de les peticions de "Browse" de la resta de la xarxa.

2.7.3 Configuració com a Domain Master Browser

El Domain Master Browser d'un domini ha de ser el Primary Domain Controller del domini. L'opció domain master =yes no especifica que sigui el PDC del domini.

Per tal que el servidor Samba sigui *Domain Master Browser* d'un domini hem d'especificar les opcions que es mostren en la figura 2.11 a la secció global del fitxer /etc/samba/smb.conf:

Figura 2.11. Configuració com a "Domain Master Browser"



Utilitzant la següent ordre:

```
1 nmblookup -S nom_màquina
```

en els sistemes GNU/Linux podem saber el tipus de treball que està fent qualsevol màquina del domini en un moment concret.

La taula 2.1 enumera alguns dels sufixos NetBIOS que empra Microsoft Windows NT. Els sufixos s'enumeren en format hexadecimal ja que, en cas contrari, molts d'ells no podrien imprimir-se.

TAULA 2.1. Sufixos NetBIOS a Windows NT

Nom de l'etiqueta	Número	Tipus	Ús
computername	00	U	Servei d'estació de treball
computername	01	U	Servei Messenger
\\–**MSBROWSE**	01	G	Examinador principal (Master Brower)
computername	03	U	Servei Messenger
computername	20	U	Servei Servidor d'arxius
domain	00	G	Nom de domini
domain	1B	U	Examinador principal de domini (DMB)
domain	1C	G	Controlador de domini(PDC)
domain	1D	U	Examinador principal
domain	1E	G	Eleccions de servei Explorador

Els tipus de nom NetBIOS descriuen la funcionalitat del registre.

- **Únic (U)**: el nom només pot tenir assignada una adreça IP.
- **Grup (G)**: un mateix nom pot existir amb diverses adreces IP.

2.8 Gestió de l'autenticació amb Samba en sistemes heterogenis

Per a més informació sobre els nivells de seguretat de Samba consulteu la unitat "Compartir recursos en xarxa i seguretat en sistemes lliures i propietaris".

Samba incorpora una sèrie de nivells de seguretat, ja coneguts, per tal de controlar l'accés del usuaris als recursos. En tots aquests nivells es porta a terme una autenticació d'usuaris.

L'autenticació en Samba es fa a través del sistema habitual d'usuari/contrasenya. Cada usuari Samba ha d'existir també al sistema GNU/Linux. Samba interactua amb comptes d'usuaris de Windows i GNU/Linux, però el sistema d'encriptació de les contrasenyes en Windows és diferent al sistema d'encriptació de les contrasenyes en GNU/Linux. No existeix un sistema per passar una paraula de pas xifrada en sistema Windows al sistema GNU/Linux. És per aquesta raó que no es poden utilitzar les contrasenyes dels usuaris de GNU/Linux per validar els usuaris Windows. Encara que la informació que s'emmagatzema dels usuaris GNU/Linux és diferent a la dels usuaris Windows, els usuaris, al contrari de les contrasenyes, sí es poden utilitzar per a fer la validació. Per tant, cal emmagatzemar les contrasenyes en algun lloc diferent als fitxers tradicionals del sistema GNU/Linux (/etc/shadow) per garantir el bon funcionament del mecanisme d'autenticació a Samba. Així doncs, Samba té el seu fitxer de paraules de pas, és el /var/lib/samba/passdb.tdb.

En aquest fitxer Samba emmagatzema les contrasenyes segons el *backend* o tipus

de base de dades de contrasenyes especificat al fitxer de configuració.

Així, els tipus de *backends* suportats per Samba són:

- **smbpasswd**. És el *backend* per defecte a Samba. Aquest *backend* es considera obsolet i només es manté per compatibilitat enrere amb versions antigues de Samba.
- **tdbsam**. És el *backend* per defecte en distribucions com Debian o Ubuntu. Aquest *backend* guarda les contrasenyes de l'antic format smbpasswd i també suporta el format extended MS Windows NT/200x SAM. La informació es guarda en un fitxer binari amb extensió tdb (trivial database). Aquest sistema permet implementar tots els sistemes de control dels servidors MS Windows NT4/200x. Tdbsam permet funcionar amb LDAP però no està recomanat per instal·lacions amb més de 250 usuaris, a més no suporta configuracions múltiples de controladors de domini. Per exemple un controlador primari de domini PDC més un o més controladors de *backups* BDC.
- **ldapsam**. Aquest *backend* permet integrar una base de dades LDAP amb Samba. La versió 3 de Samba incorpora un suport estès per LDAP i permet gran quantitat d'opcions de control. Es poden utilitzar configuracions de control d'accés per usuari, perfils, etc. i suporta perfectament sistemes distribuïts. Per exemple controladors primaris de domini amb múltiples controladors de *backups*.

Samba suporta també altres *backends* per tal de ser compatible amb versions anteriors. Aquests *backends* seran eliminats en futures versions:

- **plaintext**: Pot utilitzar els fitxers tradicionals d'UNIX (etc/passwd o /etc/shadow).
- **ldapsam_compat**: suport LDAP per a versions 2 de Samba.

L'opció que determina el *backend* al fitxer de configuració de Samba és **passdb backend**.

2.8.1 Identificació d'usuaris GNU/Linux i Windows

Totes les operacions que es fan en un sistema GNU/Linux requereixen d'un identificador d'usuari (UID). Així, de manera similar totes les operacions de les versions de servidor de Windows MS Windows NT4/200x requereixen també d'un identificador (SID). A continuació veurem el procés d'autenticació dels usuaris tant GNU/Linux com Windows a Samba. Però abans veiem alguns conceptes per tal d'entendre millor aquest procés.

1. SID (Identificador de seguretat). En els sistemes operatius de Microsoft basats en Windows NT, un Security Identifier (SID) es correspon amb una cadena

de caràcters alfanumèrics única que és assignada pel sistema durant el procés d'identificació d'un usuari o un grup d'usuaris en una xarxa de sistemes Windows NT/2000.

Els SID no són portables, la qual cosa vol dir que si canviem de sistema es generarà un nou SID per als usuaris o grups de la xarxa.

El sistema Windows permet l'accés i atorga els privilegis als recursos basant-se en la llista de control d'accés (ACL), que utilitza el SID per identificar unívocament els usuaris i membres del seu grup. Quan un usuari entra en una màquina, es genera un **token d'accés** que conté el nivell de privilegis i la SID de l'usuari o el grup. Quan un usuari sol·licita accés a un recurs, el **token d'accés** és comprovat per l'ACL per a permetre o denegar l'acció particular sobre el recurs.

Els SID son molt útils per a la localització i resolució de problemes amb auditories de seguretat, servidors de Windows i migracions de domini.

Qualsevol grup o usuari que no és creat per defecte tindrà una ID relativa de 1000 o més.

El format del **SID** és el següent:

```
S-1-5-12-7623811015-3361044348-030300820-1013
```

On:

- `S`: Determina que la cadena és un SID.
- `1`: Especifica el nivell de revisió.
- `5`: Marca el valor de l'autoritat d'identificador.
- `12-7623811015-3361044348-030300820`: Es correspon a l'identificador del domini o d'ordinador local.
- `1013`: Es correspon amb el RID (Relative ID), una ID relativa la qual identifica un compte o un grup unívocament (similar a UID o GID dels sistemes GNU/Linux).

2. UID i GID. En els sistemes Unix i derivats com GNU/Linux, els usuaris són representats per un identificador numèric d'usuari, normalment abreujat com UID (*User Identifier*). Les característiques bàsiques d'aquest identificador són:

- El rang dels valors dels UID varia entre els diferents sistemes. Com a mínim els UID han d'estar compresos entre 0 i 32767.
- El superusuari ha de tenir sempre l'UID 0.
- A l'usuari nobody, utilitzat diferents aplicacions i concretament en Samba per accedir anònimament, sempre se li assigna per tradició l'UID més alt possible com a oposició al superusuari.
- Els UID entre 1 i 499 són reservats normalment per a usuaris creats pel sistema.
- La llista de tots els UID dels usuaris existents al sistema es troba en l'arxiu /etc/passwd.

- L'identificador d'usuari és un component necessari en sistemes d'arxius i processos Unix/GNU/Linux.

En els sistemes Unix i derivats els grups d'usuari s'identifiquen mitjançant un identificador numèric anomenat GID (*Group Identifier*). Les característiques bàsiques d'aquest identificador són:

- La gamma dels valors per a un GID varia entre diversos sistemes, un GID pot estar 0 i 32767.
- El grup del superusuari ha de tenir com a GID 0.
- Aquest valor numèric s'utilitza per fer referència a grups en els arxius del sistema /etc/passwd i /etc/group o els seus equivalents.
- Els arxiu de contrasenyes /etc/shadow i el servei informatiu de la xarxa també fan referència a GIDs.
- Per tant, l'identificador del grup és un component necessari d'Unix/GNU/-Linux per al sistema d'arxius i els processos.

2.8.2 Procés d'autenticació en Samba

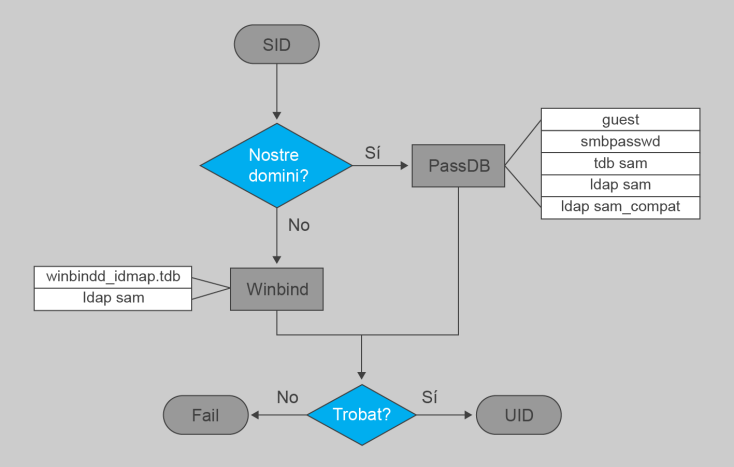
Per al correcte funcionament del l'autenticació dels usuaris en Samba, en escenaris heterogenis, és imprescindible que es faci un procés de mapatge correcte dels identificadors de Samba enfront els identificadors Unix/GNU/Linux. Els esquemes següents mostren aquest procés.

Samba proporciona dos mètodes per mapejar UID a SID:

- Cada usuari de Samba ha de tenir el corresponent usuari local Unix. Samba pot cridar a l'ordre useradd per afegir l'usuari.
- L'altra opció és fer un mapatge de SID enfront UID amb idmap. Això es pot fer amb els paràmetres **idmap uid** i **idmap gid** del fitxer **smb.conf**.

La figura 2.12 mostra el procés d'autenticació d'un usuari Windows.

FIGURA 2.12. Procés d'autenticació d'usuari en el sistema operatiu Windows



Si el sistema Samba rep un **identificador d'usuari de Windows (SID)** el primer que farà serà comprovar si el SID pertany al nostre domini en cas que ens trobem a una màquina que fa de PDC o grup de treball. És a dir, si els UID/GID de l'usuari existeixen localment. En el cas que el SID pertanyi al domini o grup de treball, es buscarà la seva contrasenya al *backend* configurat al servidor. Si la contrasenya es troba al *backend*, aleshores es farà el mapatge amb l'UID corresponent. En el cas que el SID no pertanyi al domini s'utilitzarà el servei windbind el qual ens ajuda a resoldre els problemes d'inici de sessió unificats. Winbind proporciona tres funcions separades:

Windbind

Windbind es pot utilitzar per tal que un client GNU/Linux formi part d'un domini de Windows. És a dir, el client és GNU/Linux però els usuaris i l'autenticació es fa en un domini de Windows.

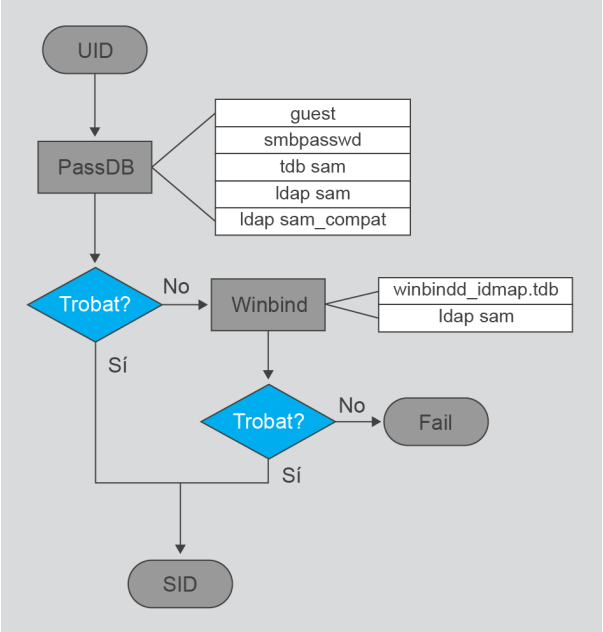
- Autenticació per a credencials d'usuari (via PAM).
- Resolució d'identitat (via NSS).
- Manteniment d'una base de dades cridada winbind_idmap.tdb en la qual emmagatzema les associacions entre usuaris UNIX UID/GID i NT SID. Aquesta associació s'usa només per a usuari i grups que no tenen uns UID/GID locals.

Si l'usuari no es troba a la base de dades del servei windbind o als *backends* de Samba no es validarà.

La figura 2.13 mostra el procés d'autenticació d'un usuari GNU/Linux

Si el sistema Samba rep un **identificador d'usuari de GNU/Linux (UID)** el primer que farà serà comprovar si la contrasenya de l'usuari es troba en el seu *backend*. Si la contrasenya es troba al *backend*, aleshores es farà el mapatge amb el SID corresponent. En el cas que no es trobi es farà servir el servei windbind per veure si es troba a la base de dades utilitzada pel servei. Si l'usuari no es troba a la base de dades del servei *windbind* o als *backends* de Samba, no es validarà.

FIGURA 2.13. Procés d'autenticació d'usuari en un sistema operatiu Linux



Finalment, hem de comentar que en els sistemes anteriors a XP l'autenticació es produïa a nivell de recursos: les carpetes compartides podien ser protegides per contrasenyes. Per accedir al recurs, n'hi havia prou de ser a la xarxa i conèixer la ubicació i la contrasenya del recurs. Aquest mètode d'autenticació es correspon amb el *Share Security Level* de Samba. El funcionament per defecte de Samba es correspon amb el *User Security Level*, és a dir, hem de tenir un usuari vàlid amb contrasenya per poder accedir als recursos compartits.

2.9 Configurar Samba com a Controlador Primari de Domini

Un dels rols més importants que pot fer un servidor Samba és actuar com a controlador primari de domini, ja que un controlador de domini és un servidor SMB/CIFS. Així doncs, resulta molt interessant conèixer el procés de configuració d'un servidor Samba com a controlador primari de domini en un domini heterogeni. És a dir, un domini on s'autenticaran i compartiran recursos màquines Windows i GNU/Linux. Els passos que ha de seguir el servidor Samba són els següents:

- Que es registri com a controlador de domini. Aquest registre es pot fer de tres maneres, utilitzant *broadcasts* de NetBIOS, informant a un servidor de WINS o a través de DNS en el cas d'*Active Directory*.
- Proporcioni el servei de NETLOGON. Aquest servei està format per diferents protocols com el servei d'inici de sessió de Lan Manager, Netlogon service, etc.
- Proporcioni un recurs compartit anomenat NETLOGON.

Per tant, un servidor Samba que compleixi aquestes condicions podrà fer de Controlador Primari de Domini PDC. El procés de configuració consta d'una sèrie d'etapes. Així doncs, les diferents etapes per configurar un servidor Samba com a PDC són les següents:

- Configuració bàsica de TCP/IP i dels paràmetres de xarxa de Windows.
- Configuració de la resolució de noms de NetBIOS (WINS).
- Configuració de les opcions de *Logon*.
- *Scripts* de gestió d'usuaris.
- Afegir clients al domini amb Samba com a PDC.

2.9.1 Configuració bàsica de TCP/IP i dels paràmetres de xarxa de Windows

Normalment no ens cal tocar res de la configuració de TCP/IP al servidor, a no ser que el PDC també sigui un encaminador amb diferents NIC i vulguem que el servei Samba només treballi per a una NIC concreta.

Per configurar els paràmetres de la xarxa de Windows hem d'establir el nom del domini (*workgroup*) i el nom de màquina de NetBIOS al fitxer de configuració /etc/samba/smb.conf. Per exemple, amb Swat quedaria com es mostra en la figura 2.14.

Figura 2.14. Configuració dels paràmetres de xarxa

Si no establim explícitament el nom de NetBIOS, aleshores el nom assignat a l'equip coincideix amb el nom de màquina al sistema operatiu.

El següent pas consisteix a assegurar-nos que el paràmetre security té assignat el valor **user**. L'opció que es mostra en la figura 2.15 és l'opció per defecte:

Figura 2.15. Establint el nivell de seguretat

Valor domain

És molt important no assignar el valor domain a l'opció security. Al contrari del que pot semblar pel seu nom aquest model de seguretat només s'utilitza quan una màquina Samba és membre d'un domini però no és un PDC.

Amb aquesta opció, el client s'identifica a nivell de sessió enviant un usuari i una paraula de pas i el servidor pot acceptar o denegar la sessió. Així doncs, en aquest nivell de seguretat, el servidor pot controlar l'accés als recursos del domini basant-se en:

- L'usuari i la paraula de pas.

- El nom de la màquina client.

Si la sessió és acceptada, el client podrà accedir als recursos del domini sense que li calgui haver de tornar a especificar la paraula de pas. En aquest mètode és imprescindible que els usuaris existeixin com a usuaris de GNU/Linux i com a usuaris de Samba.

Si configurem com a domain l'opció security, el servidor Samba passarà a utilitzar els usuaris del domini del PDC o BDC al qual ens hem unit, igual que qualsevol servidor Windows NT.

2.9.2 Configuració de la resolució de noms de NetBIOS (WINS)

La configuració més convenient de la resolució de noms de NetBios (WINS) és que el servidor Samba com a PDC sigui també un servidor WINS i funcioni com a *Domain Master Browser* del domini.

WINS (*Windows Internet Naming Service*) és la implementació de Microsoft del protocol NetBIOS *name server* (NBNS). El servidor WINS manté una taula amb la correspondència entre adreces IP i noms NetBIOS d'ordinadors. Aquesta llista permet localitzar ràpidament qualsevol ordinador de la xarxa. La utilització d'un servidor WINS evita l'ús de mètodes de recerca més laboriosos, com l'ús de difusió (*broadcast*), i redueix així el trànsit de xarxa. Un servidor WINS pot emmagatzemar també els noms del grup de treball o del domini. Així doncs, un servidor WINS pot donar servei a més d'un grup de treball o domini.

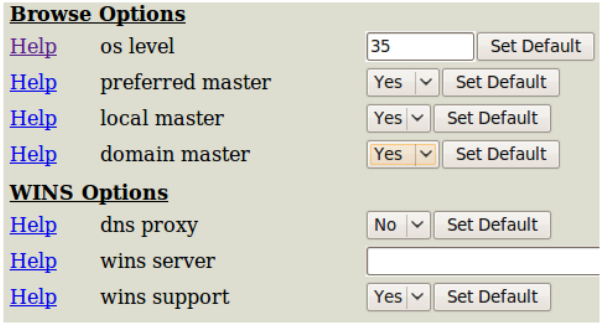
Per a més informació sobre la configuració de la resolució de noms de NetBIOS consulteu la secció "Adreces d'interès" del web.

WINS

WINS no s'ha de confondre amb DNS ni els noms de màquina NetBIOS s'han de confondre amb els noms de màquina TCP/IP. El servidors de DNS són imprescindibles per a Internet mentre que WINS només resol noms de NetBIOS i a la xarxa local, no a Internet.

A partir de Windows 2000, WINS ha estat relegat en favor de DNS i *active directory*, no obstant això, segueix essent necessari per establir serveis de xarxa amb versions anteriors de sistemes Microsoft com Windows NT i en el cas que ens ocupa per a Samba.

FIGURA 2.16. Configurant Samba com a WINS i DMB



Samba pot funcionar com un servidor primari WINS però no pot sincronitzar les seves dades amb altres servidors WINS Així doncs, per configurar el servidor Samba com a WINS i DMB els paràmetres del fitxer de configuració del servidor Samba quedaran com es mostra en la figura 2.16.

També hem de configurar el paràmetre **name resolve order** amb els valors **wins host bcast** Per configurar un servidor Samba com a client WINS hem d'especificar les opcions següents:

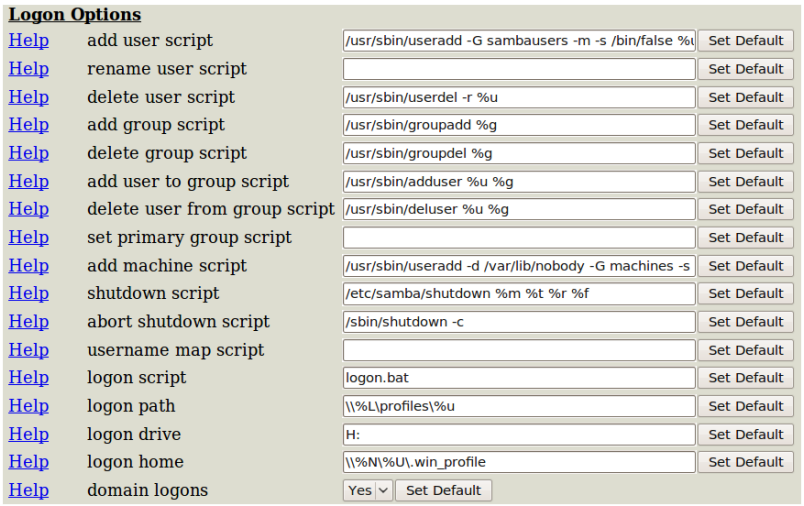
```
wins server = Adreça_IP_Servidor_WINS
name resolve order = wins host bcast
```

2.9.3 Configuració les opcions de Logon

Una vegada s'ha fet la configuració bàsica de TCP/IP i dels paràmetres de xarxa de Windows i la resolució de noms de NetBIOS el pas següent és la configuració de les opcions Logon dels usuaris del servidor Samba. Amb aquestes opcions podem determinar quins seran els *scripts* que s'executaran per gestionar els usuaris i grups GNU/Linux necessaris per als servidor, cosa que permetrà la sincronització automàtica entre els usuaris GNU/Linux i els usuaris Samba. A més, en aquesta secció també podem especificar quin serà l'*script* d'inici (*logon script*) i on s'emmagatzemaran els *scripts* de perfils per als usuaris de les màquines client Windows que s'autentiquin al domini a través del PDC.

A Swat, com ens mostra la figura 2.17, existeix una secció especifica dins de l'apartat GLOBALS, amb l'opció **Advanced** activada, anomenada **Logon Options** on ens permet configurar totes les opcions anteriors.

Figura 2.17. El paràmetre domain logons indica que l'equip és un PDC



En aquesta secció el paràmetre més important és:

```
domain logons = yes
```

Aquest és realment el paràmetre que determina que aquesta màquina és un PDC.

Si no ens interessa executar cap *script* d'inici (*logon script*), ni configurar perfils o gestionar els usuaris remotament, no cal configurar res més a Samba, amb aquesta configuració ja podríem treballar com a PDC sense servei de NETLOGON.

Wizard de Swat

També podem establir el tipus de servidor a l'apartat Wizard de l'eina Swat.

- Swat activa: domain logons = Yes.
- Quan executem tesparm ens indica el tipus de servidor.

Si ens interessa que s'executi un script d'inici cada vegada que un client Windows es validi al PDC haurem d'utilitzar els paràmetres d'inici de sessió següents:

1. **logon script**: aquest paràmetre especifica el fitxer batch (.bat) o el fitxer d'ordres de NT (.cmd) que serà descarregat i executat per cada client un cop s'ha autenticat correctament. Aquests fitxers s'utilitzen generalment per carregar a l'inici recursos compartits com impressores, carpetes, etc.

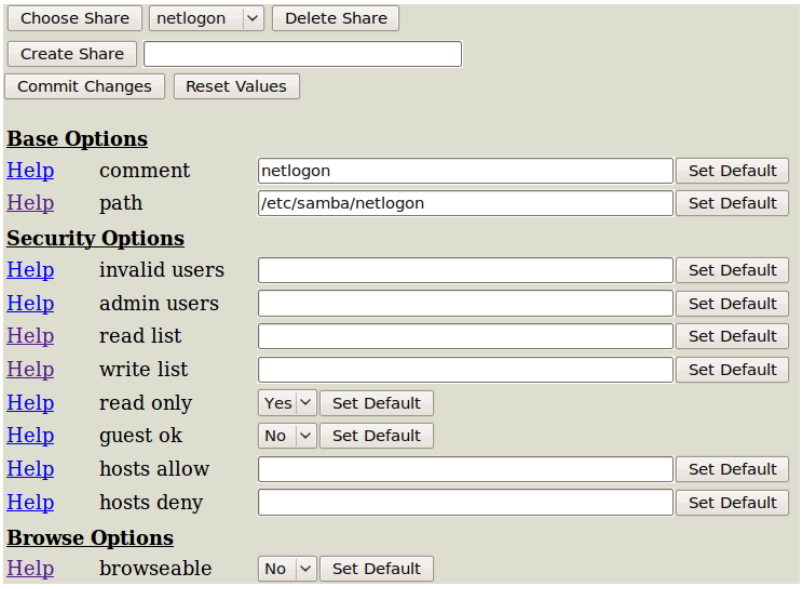
El fitxer ha d'estar en format DOS (les línies han d'acabar en CR/LF) i la seva ubicació depèn del recurs compartit [**netlogon**] el qual ens permet crear un perfil de xarxa comú per a tots els usuari que s'autentiquin al servidor.

Per exemple si el path del recurs [**netlogon**] és /etc/samba/netlogon i el nom del logon script és **logon.bat**, aleshores el camí absolut del fitxer serà **/etc/samba/-netlogon/logon.bat**.

És important destacar que no s'ha de proporcionar permís d'escriptura al recurs netlogon per tal que els usuaris no puguin modificar aquests *scripts*.

Així, els paràmetres del recurs compartit [netlogon] serien els que es mostren a la figura 2.18:

FIGURA 2.18. Paràmetres del recurs [netlogon]



Després de crear el recurs compartit [netlogon], hem de crear el directori corresponent al camí o *path* especificat i donar-li els permisos adients. Això ho podem fer amb les ordres següents:

```
1 sudo mkdir /etc/samba/netlogon
2 sudo chmod 775 /etc/samba/netlogon
```

Ara només ens caldria crear o afegir l'*script* d'inici de sessió al directori corresponent en aquest cas /etc/samba/netlogon/logon.bat

Com a exemple de *script* d'inici de sessió podem fer que, en validar-se, un usuari sincronitzi l'hora del seu sistema amb l'hora del servidor i munti la carpeta remota a una unitat local. Així l'*script* d'exemple seria:

```
sudo nano /etc/samba/netlogon/logon.bat.unix
net time \\ALFA /set /yes
net use p: \\ALFA\professors
```

On ALFA seria el nom del nostre PDC.

Com que el fitxer ha d'estar en format DOS, podem convertir-lo utilitzant l'eina **tofrodos** com a arrel (*root*). Primer haurien d'instal·lar-la i després crear el nou fitxer; el procés seria el següent:

```
sudo apt-get install tofrodos
sudo -i
unix2dos < /etc/samba/netlogon/logon.bat.unix > /etc/samba/netlogon/logon.bat
```

Podem comprovar que els fitxers són diferents amb l'ordre file:

```
file /etc/samba/netlogon/logon.bat.unix
logon.bat.unix: ASCII text, with no line terminators
file /etc/samba/netlogon/logon.bat
logon.bat: ASCII text, with CRLF line terminators
```

2. logon path: indica on estan els perfils mòbils dels usuaris. Els perfils defineixen entre altres coses les característiques de l'escriptori i els programes i fitxers accessibles d'un compte.

A les xarxes Windows NT trobem dos tipus de perfils:

- **Perfils locals (*Local Profiles*)**: en aquests tipus de perfils es manté una copia del perfil a la màquina local, només estan disponibles a l'ordinador local i el control és únicament de l'usuari al qual pertany cada perfil.
- **Perfils mòbils (*Roaming profiles*)**: els perfils mòbils s'emmagatzemen en un servidor centralitzat (PDC) i estan disponibles sobre qualsevol ordinador de la xarxa (amb el SO Windows). Quan un usuari entra en una xarxa, fa logon, el perfil de l'usuari emmagatzemat al servidor es copia a la màquina local per crear un perfil local. Aquest perfil es manté en local, a no ser que s'especifiqui el contrari canviant una clau del registre. Si es fa aquesta modificació el perfil s'elimina de la màquina quan l'usuari finalitza sessió (logout). De perfils mòbils en tenim tres tipus:
  - **Perfils mobils personals (*Personal roaming profiles*)**: Són els normals. Les estacions de treball emmagatzemen una còpia del perfil en local. Aquesta copia es pot utilitzar si al pròxim logon no es pot obtenir el perfil. Generalment poden ser modificats pels usuaris i les modificacions s'emmagatzemaran en local i al servidor.

- **Perfils de grup (*Group profiles*)**: són perfils creats normalment a partir d'una plantilla d'usuari. Poden ser assignats a grups d'usuaris estalviant així feina a l'administrador. Aquestos perfils són carregats des d'un servidor centralitzat.
- **Perfils obligatoris (*Mandatory profiles*)**: els perfils obligatoris es poden crear per a usuaris i per a grups. L'usuari pot fer modificacions durant la sessió però aquestes modificacions no es guardaran al perfil mòbil. Només els usuaris administradors poden modificar.

Consideracions sobre perfils

El tema dels perfils és sempre un compromís entre servei/comoditat i eficiència. Els perfils poden arribar a ocupar Gigas d'espai, el que provoca que una estació de treball Windows pugui arribar a trigar una hora en carregar.

La configuració per defecte de Samba pel que fa als perfils és la d'utilitzar perfils mòbils, encara que es poden desactivar. De fet normalment no cal fer res per activar la qüestió dels perfils amb Samba, ja que el valor per defecte del paràmetre logon path és:

```
logon path = \\%N\%U\profile
```

Aquest valor especifica on es guarden per defecte els perfils d'usuari. El valor **%N**, si no utilitzem el servei NIS, és idèntic a %L i es correspon amb el nom NetBIOS del servidor i **%U** indica el nom d'usuari de sessió.

Per tant els perfils es guarden en una carpeta anomenada **profile** de la *home* de l'usuari. Aquesta carpeta es crea automàticament en el cas de no existir durant el primer accés de l'usuari.

Per qüestions de seguretat, que el perfil estigui a la *home* de l'usuari potser no és el més convenient, ja que l'usuari el pot modificar directament i després tenir problemes. Així doncs, normalment la localització dels perfils es fa fora de les *homes* dels usuaris. Per exemple:

```
logon path = \\%L\profiles\%U
```

Els perfils per a clients Windows 9x/Me funcionen d'una manera lleugerament diferent. Aquests perfils utilitzen el paràmetre:

```
logon home = \\%N\%U
```

Amb aquests tipus de clients els perfils només es poden posar a la *home*. Però hi ha un truc que és fer que la *home* comenci per punt i sigui un fitxer ocult:

```
logon home = \\%L\%U\ . profiles
```

Tots dos paràmetres, logon path i logon home, es poden utilitzar alhora per suportat tots els tipus de clients.

A més de configurar el paràmetre logon path necessitem crear un nou recurs compartit al servidor Samba per treballar amb perfils. Aquest recurs compartit l'anomenem **profile**.

Al directori que vinculem amb el recurs profile no ha de poder accedir cap usuari directament, només el superusuari (*root*) Samba per tant, el recurs no serà

"browseable". Per altra banda aquest directori vinculat amb el recurs profile, no serà de només lectura, ja que la seva funció és que la màquina client pugi carregar al servidor el seu perfil mòbil quan l'usuari surt (*log off*) i descarregar-lo quan l'usuari entri al domini (*log on*).

Així, quan un usuari entra per primera vegada al domini és crea la carpeta profile a la màquina client, en la ubicació que indica el servidor Samba al paràmetre logon path. Quan l'usuari surt (*log off*) el contingut del seu perfil, és a dir, les dades de Inicio, Mis Documentos, Favoritos... s'emmagatzemen en aquesta carpeta i es pugen al servidor Samba, emmagatzemant-se a la carpeta corresponent dins del recurs profile. Quan l'usuari torna a entrar al domini, descarrega les dades del seu perfil, pujades anteriorment, de la carpeta compartida al recurs profile del servidor. Aquesta configuració ens permet modificar, mitjançant l'usuari root, la configuració del perfil de l'usuari.

Recurs compartit [profiles] per a perfils mòbils

El recurs compartit per a perfils mòbils s'utilitza per emmagatzemar els perfils 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 permisos de lectura globals. Els paràmetres més importants d'aquest recurs es mostren a continuació:

- **path = /etc/samba/profile**: Directori on s'emmagatzemaran els perfils mòbils. Sota aquest directori, cada usuari tindrà una carpeta amb el seu nom.
- **read only = no**: Aquesta opció indica que es permet escriure en el recurs compartit.
- **browseable = no**: indica si aquest recurs apareixerà en la llista de recursos compartits o no, en aquest cas, no es mostrarà.
- **create mask = 0600**: màscara de creació d'arxius, el valor d'aquest paràmetre indicarà els permisos que tindran els arxius de nova creació sota el directori.
- **directory mask = 0700**: màscara de creació de directoris, el valor d'aquest paràmetre indicarà els permisos que tindran els directoris de nova creació sota el directori.

Una vegada creat el recurs compartit hem de crear el directori corresponent i assignar els permisos adequats:

```
1 sudo mkdir /etc/samba/profile
2 sudo chmod 775 /etc/samba/profile
```

Perfils obligatoris

> Els **perfils obligatoris** són aquells perfils amb els quals l'usuari pot fer modificacions del seu perfil però aquestes modificacions no s'emmagatzemaran al finalitzar la sessió.

El procés es tan senzill com localitzar el fitxer NTUSER.DAT del perfil de l'usuari i reanomenar-lo a NTUSER.MAN.

Perfils per defecte i perfil de tots els usuaris

Els perfils per defecte i els perfils per tots els usuaris son perfils locals, i per tant s'emmagatzemen a la màquina client del domini.

El perfil d'un usuari concret, ja sigui local o de domini, es forma a partir del perfil per defecte i del perfil per a tots els usuaris de la màquina local.

El perfil per defecte del domini, el podem establir a través del recurs compartit [**netlogon**]. Per exemple:

```
1 \\ALFA\ netlogon\Default user
```

El perfil per a tots els usuaris s'estableix a la màquina local i es carrega des d'aquesta. Per exemple quan s'instal·len aplicacions normalment s'afegeixen al menú Inicio del perfil **All Users**.

Importar perfils

Existeix la possibilitat d'importar fàcilment un perfil de Windows a Samba. Per exemple A XP, hem d'entrar com administrador a la màquina client, posteriorment anem a la icona *Mi PC* i prenem botó dret, escollim *Propietats* i anem a la pestanya *Opcions avançades*, seleccionem l'opció *Configuració* de l'apartat "Perfiles de usuario", seleccionem un usuari del domini i prenem el botó *Copiar a*, ens demanarà la ubicació on el volem copiar, la qual pot ser el PDC Samba, i ja està, podem fer servir el contingut d'aquest perfil per al que necessitem.

Desactivar els perfils mòbils

Hi ha casos en què els perfils mòbils no són la millor opció, per exemple quan no es disposa o no es desitja gastar ample de banda per carregar els perfils dels usuaris, no es vol tenir control dels clients, tenim distints tipus de màquines i distintes configuracions de maquinari, i aquest fet complica que un client entri al domini des de qualsevol lloc amb la seva configuració predeterminada...

Existeixen tres maneres de desactivar els perfils mòbils:

1. Modificant el fitxer **smb.conf**. Cal deixar els paràmetres:

```
logon home =
logon path =
```

Si deixem en blanc aquest paràmetre s'utilitzaran perfils locals.

Atenció

Deixar aquests paràmetres en blanc no és el mateix que no especificar-los. Segons el manual de smb.conf, els valors per defecte són:

```
logon home = \\%N\%U
logon path = \\%N\%U\profile
```

2. Modificant el registre de Windows: Es pot utilitzar l'aplicació gpedit.msc.

3. Canviant el tipus de perfil. Entrar com a Administrador a la màquina client amb XP i des de la icona *Mi PC*, premem botó dret, seleccionem *Propietats* i anem a la pestanya *Opcions avançades*. Aquí seleccionem *Configuració* de l'apartat *Perfils d'usuari* i seleccionem *Canviar tipus*.

- **logon drive**: aquest paràmetre especifica el volum on es muntarà la *home* de cada usuari. Només s'utilitza en servidors Samba PDC. Per exemple:

```
logon drive = H:
```

- **logon home**: aquest paràmetre indica la localització de la *home* per clients Win95/98 o estacions de treball NT.

El valor per defecte és:

```
logon home = \\%N\%U
```

2.9.4 Scripts de gestió d'usuaris

Swat a la secció *Logon Option* proporciona una sèrie d'opcions que ens permeten especificar un conjunt d'*scripts*. Aquests *scripts* s'utilitzaran per gestionar remotament els usuaris del sistema GNU/Linux on es troba el PDC. Quan usuaris de Samba amb permisos de *root* es connecten remotament des de màquines del domini Windows NT, aquests *scripts* permeten crear, esborrar, modificar usuaris i grups al PDC proporcionant així una sincronització automàtica entre els usuaris de GNU/Linux i Samba. Veiem algunes d'aquestes opcions.

Tots els paràmetres utilitzats per indicar els diferents tipus de *scripts* **no** s'han d'utilitzar amb l'opció *security = share*, ja que els *scripts* són executables de GNU/Linux als quals es passa el nom de l'usuari que correspongui utilitzant la variable %u.

- **add user script**: quan un usuari intenta connectar-se a un servidor Samba, en temps de login, el dimoni smbd contacta amb el servidor de contrasenyes, el qual pot ser una màquina remota o ell mateix, i intenta autenticar l'usuari. Si l'autenticació és correcta aleshores smbd intenta buscar un usuari GNU/Linux equivalent. Si aquest usuari no existeix, aleshores

s'executa l'*script* indicat per la variable: aquest *script* s'executa com a root i es l'encarregat de crear l'usuari al sistema GNU/Linux si no existeix.

- **rename user script**: quan un usuari administrador o amb els permisos adequats intenta reanomenar un usuari des d'un client remot s'executarà aquest *script* per tal de modificar l'usuari GNU/Linux corresponent.
- **delete user script**: aquest és l'*script* que s'executarà quan un usuari amb permisos d'administrador elimini des d'un client remot un usuari.
- **add group script**: similar a add user script però per a grups.
- **delete group script**: idèntic a delete user script però per eliminar un grup.
- **add user to group script**: s'utilitza quan un usuari amb permisos al client remot afegeix a un usuari existent a un grup existent.
- **delete user from group script**: idèntic a l'anterior però per eliminar un usuari d'un grup.
- **set primary group script**: estableix el grup principal de l'usuari.
- **add machine script**: utilitzat per a crear un compte de confiança entre màquines.
- **shutdown script**:determina un *script* que permet iniciar un procés d'apagada del servidor. Si l'usuari connectat té els permisos **adequats** podrà executar aquesta ordre.

En la taula 2.2 podem veure el conjunt de variables utilitzades a Samba i el seu significat.

TAULA 2.2. Conjunt de variables utilitzades a Samba

Variable	Significat
%a	Arquitectura del client (p. ex. Samba, WfWg, WinNT, Win95, o UNKNOWN)
%I	Adreça IP de client (p.ex. 192.168.220.100)
%m	Nom NetBIOS del client
%M	Nom DNS del client
%g	Grup primari de %u
%G	Grup primari de %U
%H	Directori "home" de %u
%u	Actual nom d'usuari Unix
%U	Nom d'usuari (no sempre utilitza per Samba)
%p	Automontador de ruta per al recurs, si és diferent de %P
%P	Actual directori root del recurs
%S	Actual nombre del recurs
%d	Actual PID de servidor
%L	Nom NetBIOS del servidor Samba

TAULA 2.2 (continuació)

Variable	Significat
%h	Nom DNS de màquina del servidor Samba
%N	Directori "home" edl servidor, des del mapa automount
%v	Versió de Samba
%R	Nivell de protocol SMB que ha negociat
%T	Data i hora actual

2.9.5 Afegir clients al domini amb Samba com a PDC

Una vegada configurat el servidor Samba com a PDC d'un domini, podem afegir màquines i usuaris que tinguin accés al domini i als recursos compartits d'aquest. Per afegir un client a un domini hem de seguir una seqüència de passos que serien:

1. Configurar l'administrador del domini. Al servidor Samba, hem d'afegir com a usuari Samba el superusuari o root del sistema i posar-li una contrasenya. Utilitzarem la següent ordre:

```
1 sudo smbpasswd -a root
```

Perquè tingui validesa l'ordre anterior, hem d'assegurar-nos que al fitxer /etc/samba/smb.conf no tenim el paràmetre:

```
1 invalid users=root
```

És força comú a Samba utilitzar un mapatge d'usuaris. Aquest mapatge d'usuaris ens serveix per exemple per a poder utilitzar des de Windows l'usuari Administrador.

Per configurar el mapatge d'usuaris creem un fitxer anomenat /etc/samba/smbusers on introduirem la següent línia :

```
1 root=Administrador
```

Després establirem el nou fitxer com a valor del paràmetre username map. Així, a la secció global del fitxer /etc/samba/smb.conf s'afegirà el següent:

```
1 usename map=/etc/samba/smbusers
```

És recomanable no utilitzar la mateixa paraula de pas per a l'administrador Samba que per a l'usuari *root* del servidor.

2. Cal afegir un compte de màquina MTA per cada estació de treball a la base de dades SAM del domini.

Un compte **MTA** (*Machine Trust Account*) és un compte que s'utilitza per autenticar una màquina client en un domini de Windows. La idea és evitar que una màquina es pugui fer passar per un altra utilitzant el mateix nom de NetBIOS.

Cal recordar que Windows NT/200x i XP Professional utilitzen MTA i Windows 9x/Me/XP Home no utilitzen MTA

El PDC del domini és l'encarregat d'emmagatzemar les MTA. A Windows es guarden al registre de Windows, excepte en el cas de *Active Directory* que les guarda a LDAP. En una màquina Samba treballant com a PDC es guarden en dos llocs, igual que els usuaris:

- En un compte de seguretat del domini al passdb backend (smbpasswd, tdbsam, ldapsam).
- En un compte corresponent de GNU/Linux.

Els noms de màquina en els dominis Windows NT acaben en $.

Hi ha tres maneres de crear un compte MTA a Samba:

- De manera manual des de la línia d'ordres del servidor, amb l'ordre net. Exemple:

```
1 sudo addgroup maquines
2 sudo useradd -g maquines -d /var/lib/nobody -c "BETA" -s /bin/false BETA$
3 sudo passwd -l BETA$
4 sudo smbpasswd -a -m BETA$
```

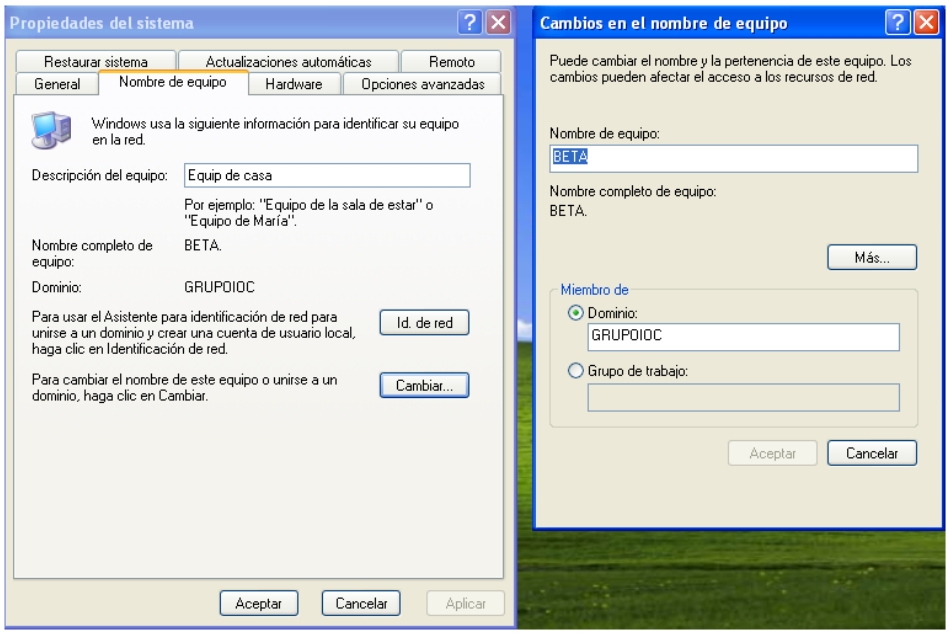
- Utilitzant MS Windows NT4 Server Manager des d'una màquina que sigui membre del domini.
- Creació *on-the-fly*. El compte es crea automàticament per Samba en el moment que el client s'afegeix al domini. La corresponent paraula de pas de GNU/Linux es pot crear automàticament o manualment. Per fer aquest tipus de configuració haurem d'afegir la línia següent al fitxer /etc/samba/smb.conf en la secció *Logon Options de Swat*.

```
1 add machine script = /usr/sbin/useradd -d /var/lib/nobody\
2  -G maquines -s /bin/false -m %u
```

- Cal afegir les estacions de treball al domini. Aquesta operació s'anomena **join**, i es fa des de cadascun dels clients. El procés és el següent: premem botó dret a la icona *Mi PC* de la màquina client, seleccionem *Propietats*, anem la pestanya *Nom d'equip* i premem el botó *Canviar*. En el nou quadre que ens apareix seleccionem *Domini* dins de la secció *Miembro de* i especifiquem el nom del domini al qual volem afegir la màquina, el mateix que al servidor Samba, tal com veiem en la figura 2.19. Quan acceptem ens

demanarà un usuari i una contrasenya, la primera vegada que entrem hem d'utilitzar com a usuari root, o, administrador si hem fet el fitxer de mapatge, i com a contrasenya la que hem establert per a l'administrador de Samba. Si els valors son correctes, ens apareixerà un missatge de benvinguda al domini i ens demanarà que reiniciem. Així, el *join* ja estarà completat.

FIGURA 2.19. Afegint una màquina en un domini



2.10 Samba amb LDAP

Quan en una organització han de conviure diferents sistemes operatius, s'ha de facilitar als usuaris la manera d'accedir als recursos independentment de la plataforma que aquests decideixin utilitzar.

Unes credencials úniques facilitaran a l'usuari l'accés a la xarxa i implicarà una major seguretat i control del funcionament de la mateixa. La utilització de credencials úniques comporta la creació d'un dipòsit únic on s'emmagatzema la informació de cada element de la xarxa. Màquines, usuaris i serveis podran ser fàcilment creats, modificats i eliminats si disposem d'un únic punt d'administració. La implantació d'un domini de xarxa que ens permeti implementar els objectius anteriors, ens obliga a escollir les eines programari que siguin capaces de dur aquest repte a bon port. Així, l'elecció del programari condiciona el model de domini que es pot oferir.

El servei Samba pot funcionar en conjunt amb el servei LDAP per tal de combinar la potència d'ambdós serveis i oferir un punt central d'autenticació i accés als recursos compartits tant per a màquines Windows com GNU/Linux.

Samba pot funcionar amb qualsevol tipus de servidor que respecti l'estàndard LDAP, però el servidor de referència utilitzat per Samba és OpenLDAP.

LDAP és un protocol del nivell d'aplicació utilitzat per accedir a un servei de directori.
OpenLDAP és el projecte de codi obert que ens proporciona tant client com el servidor LDAP per gestionar, accedir i organitzar el servei de directori.
Samba com a PDC, ens permet crear amb una màquina GNU/Linux un **controlador de domini Windows NT** que manté la base de dades centralitzada del domini i permet controlar el procés d'autenticació i accés als recursos.

A partir de la versió 2000, els sistemes Windows incorporen *Active Directory*, el qual funciona amb LDAP i Kerberos entre altres protocols. Amb *Active Directory* desapareixen els conceptes de PDC i BDC, ja que tots els controladors de domini actuen igual. Tanmateix, la finalitat continua essent idèntica, ja que *Active Directory* permet compartir de manera centralitzada informació de recursos i usuaris de la xarxa o domini Windows. A més de funcionar com autoritat d'autenticació controlant els accessos dels usuaris al domini.

Així doncs, què obtenim de combinar Samba amb LDAP o més concretament un PDC Samba amb OpenLDAP? Doncs obtenim els avantatges següents:

- El principal avantatge que ens aporta la combinació de Samba amb LDAP és la potencia i escalabilitat del sistema. Amb la combinació de Samba i LDAP podem gestionar major quantitat d'usuaris d'una manera més ràpida i organitzada.
- La combinació d'un PDC Samba amb OpenLDAP permet implementar, amb un servidor GNU/Linux, un sistema similar a l'*Active Directory* de Windows, en el qual poden treballar màquines Windows i GNU/Linux al mateix temps, sense cap mena de problema.
- El fet d'utilitzar el servei LDAP sempre augmenta les capacitats d'SSO (*single sign on*) ja que gran quantitat d'aplicacions utilitzen o suporten aquest mecanisme d'autenticació.
- Utilitzar LDAP ens permet implementar un servidor Samba com a BDC (*backup domain controller*) d'un domini Windows NT.
- Utilitzar la combinació d'aquestes eines ens permet treballar i implementar serveis molt potents amb programari lliure i de qualitat, cosa que sempre suposa un avantatge.

Escalabilitat

L'escalabilitat no només depèn del *backend* (cal analitzar les necessitats de disc dur, memòria RAM, etc. i els patrons de carrega). Com a norma cal un PDC (o BDC) per cada 30-150 clients.

Un dels inconvenients que podem trobar, per esmentar-ne algun, d'utilitzar Samba amb LDAP, en comptes d'un sistema Windows amb *Active Directory*, és que es perden algunes funcionalitats molt específiques d'*Active Directory* i Windows, com la replicació de les bases de dades SAM entre màquines Samba i màquines Windows o la possibilitat d'actuar com a controlador de domini *Active Directory*. Encara s'esten treballant a la versió 4 de Samba perquè totes aquestes opcions i més estiguin disponibles.

Una de les peculiaritats de combinar Samba amb LDAP és que permet substituir el *backends* per a la gestió d'usuaris smbpasswd i tdbsam per un específic d'LDAP, ldapsam. Els beneficis d'aquesta substitució són:

- Smbpasswd és un *backend* per a pocs usuaris, màxim d'un centenar i sense utilitzar comptes de domini de Windows, és a dir treballant com a Samba *stand-alone server*.
- El *backend* tdbsam només permet comptes de domini de Windows i és un sistema amb una capacitat limitada, màxim uns cinc-cents usuaris.
- Tdbsam no permet tenir rèpliques (BDC) del controlador principal de domini (PDC).
- LDAP dóna molta flexibilitat, ja que un servidor LDAP pot emmagatzemar al mateix temps usuaris de GNU/Linux i de Windows/Samba.
- És un sistema més escalable que utilitzar un fitxer (tdbsam) per emmagatzemar les comptes de domini.

2.10.1 Configuració d'un PDC Samba amb OpenLDAP

A continuació veurem el procés de configuració d'un servidor Samba que fa tasques de PDC d'un domini Windows NT amb OpenLDAP. Suposem que tenim instal·lats a la mateixa màquina els serveis Samba i OpenLDAP. El procés de configuració consta d'una sèrie de passos, tant al servidor OpenLDAP com al servidor Samba. Comencem pel primer:

1. Configuració del servidor OpenLDAP. Necessitem configurar el servidor OpenLDAP perquè actuï com una base de dades SAM. Per tant, per aconseguir això, hem de fer possible que:

- OpenLDAP incorpori i accepti l'esquema de Samba.
- El servidor OpenLDAP executi com a base el nostre directori.
- S'afegeixin a la base del directori les entrades mínimes per a començar a utilitzar-lo.

Per aconseguir els objectius anteriors, definirem l'estructura del directori segons aquest DIT (*directory information tree*).

```
dc=base del domini
ou = Users : comptes d'usuari tant per a GNU/Linux com per a Windows
ou = Computers : comptes de màquina per als sistemes Windows
ou = Groups : comptes de grups tant per a GNU/Linux com per a Windows
ou = DSA : comptes espcials del sistema
```

Aquesta estructura és conforme amb les recomanacions del RFC 2307bis. Per tant, la conjunció de Samba i OpenLDAP ens permetrà emmagatzemar la informació següent:

- Comptes d'usuari Microsoft Windows utilitzant la classe d'objecte **sambaSAMAccount** (samba.schema).
- Comptes de màquina Microsoft Windows utilitzant la classe d'objecte sambaSAMAccount.
- Comptes d'usuari GNU/Linux utilitzant les classes d'objecte **posixAccount** i **shadowAccount** (nis.schema).
- Grups d'usuaris utilitzant les classes d'objectes posixGroup i sambaGroupMapping.
- Comptes de seguretat utilitzades per programari de clients (Samba i GNU/Linux) que utilitzen la classe d'objecte **simpleSecurityObject** (core.schema).

2. Afegir l'esquema Samba a OpenLDAP. OpenLDAP no incorpora l'esquema per poder crear els objectes de Samba dins del directori. Així el primer pas serà incorporar l'esquema Samba al servidor OpenLDAP.

La primera cosa que hem de fer és obtenir l'esquema que defineix els objectes de Samba o samba.schema.

Podem trobar el samba.schema a la documentació de Samba concretament al directori **/usr/share/doc/samba-doc/examples/LDAP**. El fitxer amb l'esquema Samba és diu precisament samba.schema.gz i està comprimit. Per tant, per obtenir-lo el descomprimirem amb l'ordre següent.

```
1 sudo gunzip /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz\
2  /usr/share/doc/samba-doc/examples/LDAP/samba.schema
```

Una vegada descomprimit el copiarem al directori on el servidor slapd emmagatzema els esquemes:

```
1 sudo cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema  /etc/ldap/schema
```

El fitxer samba.schema concretament conté la informació necessària per crear un compte de domini de Windows NT. Dins de l'esquema es defineix entre altres classes d'objectes de Samba, la classe **sambaSAMaccount**, la qual implementa els atributs necessaris per treballar amb la SAM Windows Windows NT. En la taula 2.3 veiem els atributs que ens proporciona aquest objecte.

TAULA 2.3. Atributs dels objectes de Samba

	Descripció
sambaLMPassword	La paraula de pas LanMan (16-byte hash).
sambaNTPassword	La paraula de pas NT (16-byte hash).
sambaPWdLastSet	El temps en segons des de 1970 quan els valors anteriors van se establerts per última vegada.
sambaAcctFlags	Un string de 11 caràcters entre []amb flags: U (usuari), W (estació de treball), X (la paraula de pas no expira), I (*domain trust account*, H (*home dir* és obligatori), S (*server trust account*) i D (*disabled*).

Taula 2.3 (continuació)

	Descripció
sambaLogonTime	Valor enter que actualment no s'utilitza.
sambaKickoffTime	Especifica el moment (en format UNIX) en que l'usuari es bloquejarà i no podrà entrar al sistema.
sambaPwdCanChange	Especifica el moment (en format UNIX) en que l'usuari podrà canviar la seva paraula de pas.
sambaPwdMustChange	Especifica el moment (en format UNIX) en que l'usuari haurà de canviar la seva paraula de pas.
sambaHomeDrive	El drive Windows (p.ex. X:) on es muntaran una unitat de xarxa amb la HOME de l'usuari. Consulteu el paràmetre *logon drive* al manual del fitxer smb.conf.
sambaLogonSript	Especifica el camí (path) del fitxer que s'executarà quan l'usuari inicii una sessió (logon Script).El path és relatiu al recurs compartit *netlogon share*. Consulteu el paràmetre *logon script*al manual del fitxer smb.conf.
sambaProfilePath	Especifica el camí (path)del perfil de l'usuari. Cosulteu el paràmetre *logon path* al manual del fitxer smb.conf.
sambaHomePath	Especifica el camí (path)de la HOME de l'usuari. Consulteu el paràmetre *logon home* al manual del fitxer smb.conf.
sambaUserWorkstations	Una llista separada per comes de noms de màquina Net BIOS a les quals l'usuari pot fer logon. Si el paràmetre està buit l'usuari pot entrar a totes les màquines.
sambaSID	El security identifier (SID) de l'usuari. L'equivalent Windows als UID de UNIX
sambaPrimaryGroupSID	El security identifier (SID) del grup principal de l'usuari.
sambaDomainName	Dominial al qual l'usuari pertany.

En les versions anteriors a OpenLDAP 2.4 només cal incloure samba.schema al fitxer /etc/ldap/slapd.conf i reiniciar el servei.

En les versions posteriors a OpenLDAP 2.4 el procés d'afegir l'esquema al servei sladp és una mica tediós. Veiem:

Primerament hem de crear un fitxer de text on posarem els *includes* de tots els esquemes que volem afegir al servei. Suposem que hem anomenat al fitxer afegir_schema.conf. A continuació crearem també un directori temporal al qual anomenarem, per exemple, sortida. El procés per fer aquestos passos és el següent:

Editem el fitxer:

```
sudo nano afegir_schema.conf
```

Afegim el contingut següent al fixer i l'emmagatzemem:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
```

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

A continuació creem la carpeta sortida a tmp:

```
mkdir /tmp/sortida
```

Una vegada creats el fitxer i el directori, utilitzem l'ordre slaptest per convertir els esquemes en un fitxer amb format ldif i desar-lo al directori creat. Aquest fitxer serà utilitzat per exportar al servidor slapd les dades dels esquemes. L'ordre serà la següent:

```
slaptest -f afegir_schema.conf -F /tmp/sortida
```

Si mirem dins del directori */tmp/sortida* veurem que s'han generat un conjunt de fitxers i carpetes, similars als continguts a */etc/ldap/slapd.d*.

A continuació hem d'editar el fitxer **/tmp/sortida/cn=config/cn=schema/cn={12}samba.ldif** i canviar els atributs dn i cn i introduir els valors següents:

```
dn: cn=samba,cn=schema,cn=config**
...
cn: samba
...
```

També hem d'esborrar aquestes línies del final del fitxer:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

Per últim hem d'afegir l'esquema al servidor LDAP amb l'ordre ldapadd:

```
ldapadd -x -D -w contrsenya_admin cn=admin,cn=config -fi\
 /tmp/sortida/cn\=config/cn\=schema/cn\=\{12\}samba.ldif
```

3. Optimitzar el funcionament del servidor OpenLDAP. Per tal d'optimitzar el funcionament del servidor OpenLDAP és necessari crear una sèrie d'índexs. Per fer-ho creem un fitxer amb el contingut següent:

```
sudo nano samba_indexs.ldif

dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
```

```
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

A continuació utilitzem l'ordre **ldapmodify** per carregar els nous índexs:

```
ldapmodify -x -D -w contrasenya_admin cn=admin,cn=config -W -f samba_indexs.
    ldif
```

4. Crear l'arbre de Samba al directori OpenLDAP. Per poder treballar amb Samba al directori OpenLDAP, hem de crear l'arbre d'informació del directori (DIT) amb els objectes i entrades necessaris, especificant com a base el nostre directori. Podem fer-lo de dues maneres, creant a mà un fitxer amb les entrades o utilitzant l'eina smbldap-populate, la qual ens genera automàticament l'arbre bàsic per treballar amb Samba.

Per obtenir l'eina **smbldap-populate** hem d'instal·lar el paquet **smbldap-tools**, el qual incorpora una sèrie de *scripts* pensats per gestionar usuaris que estiguin emmagatzemats en un directori LDAP. Aquest paquet també incorpora eines que ens poden ajudar en la migració d'un Servidor Windows NT 4.0 a Samba.

Veiem el procés d'instal·lació i configuració d'smbldap-tools:

```
sudo apt-get install smbldap-tools
```

Amb la següent ordre veiem les eines que ens proporciona el paquet:

```
sudo dpkg -L smbldap-tools | grep bin

/usr/sbin
/usr/sbin/smbldap-groupadd
/usr/sbin/smbldap-groupdel
/usr/sbin/smbldap-groupmod
/usr/sbin/smbldap-groupshow
/usr/sbin/smbldap-passwd
/usr/sbin/smbldap-populate
/usr/sbin/smbldap-useradd
/usr/sbin/smbldap-userdel
/usr/sbin/smbldap-userinfo
/usr/sbin/smbldap-usermod
/usr/sbin/smbldap-usershow
```

Per tal de configurar correctament el funcionament de les eines de *smbldap-tools* hem de fer el següent: Copiar els exemples de configuració de la documentació a la carpeta **/etc/smbldap-tools** amb les ordres següents:

```
cd /usr/share/doc/smbldap-tools/examples
sudo gunzip smbldap.conf.gz
sudo cp /usr/share/doc/smbldap-tools/examples/smbldap.conf  /etc/smbldap-tools/
sudo cp /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf  /etc/smbldap-
    tools/
```

Establir els permisos d'aquests fitxers de la manera com segueix:

```
sudo chmod 0644 /etc/smbldap-tools/smbldap.conf
sudo chmod 0600 /etc/smbldap-tools/smbldap_bind.conf
```

Modificar els valors d'smbldap.conf per fer-los concordar amb el nostre entorn.

```
SID=" S-1-5-21-1329301582-845521840-2767172409"
sambaDomain="GRUPIOC"
slaveLDAP="127.0.0.1"
slavePort="389"
masterLDAP="127.0.0.1"
masterPort="389"
ldapTLS="0"
verify="none"
cafile="/etc/smbldap-tools/ca.pem"
clientcert="/etc/smbldap-tools/smbldap-tools.pem"
clientkey="/etc/smbldap-tools/smbldap-tools.key"
suffix="dc=grupioc,dc=ioc,dc=xtec,dc=cat"
usersdn="ou=People,${suffix}"
computersdn="ou=Computers,${suffix}"
groupsdn="ou=Groups,${suffix}"
idmapdn="ou=Idmap,${suffix}"
sambaUnixIdPooldn="sambaDomainName=GRUPIOC,${suffix}"
...
```

Per obtenir el SID, utilitzem l'ordre, al servidor Samba:

```
sudo net getlocalsid
```

Modificar el fitxer **/etc/smbldap-tools/smbldap_bind.conf:**

```
slaveDN="cn=admin,dc=grupioc,dc=ioc,dc=xtec,dc=cat"
slavePw="contrasenya_admin"
masterDN="cn=admin,dc=grupioc,dc=ioc,dc=xtec,dc=cat"
masterPw="contrasenya_admin"
```

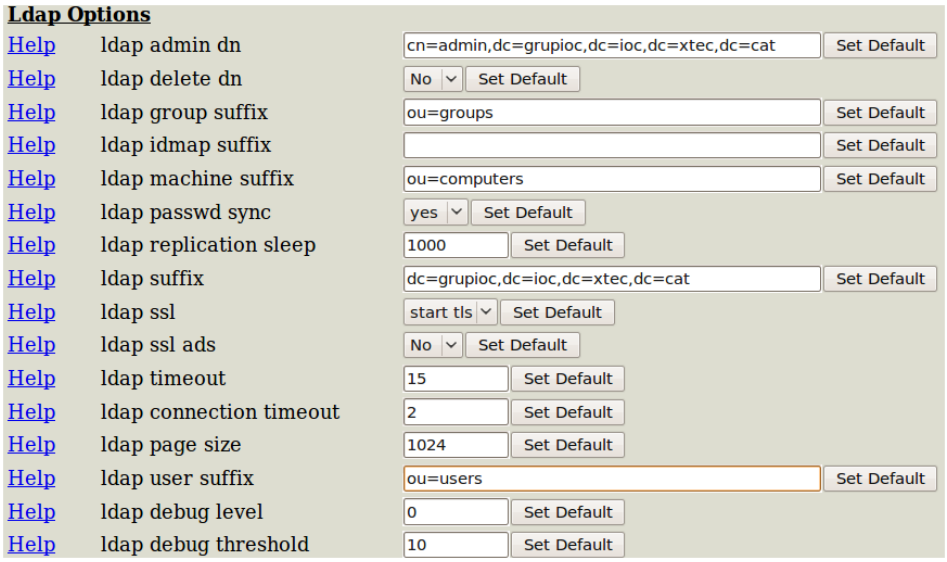
Un cop configurat podem fer que smbldap-tools ens generi l'arbre bàsic d'LDAP amb:

```
sudo smbldap-populate
```

Amb aquest pas finalitzem la configuració del servei OpenLDAP. El següent pas en la configuració de l'PDC Samba amb LDAP consisteix en la configuració del servidor Samba.

5. Configuració del servidor Samba. Si utilitzem Swat dins de la secció global trobem una secció d'opcions per establir els paràmetres d'LDAP. Un exemple de configuració amb el nostre domini és el que es mostra en la figura 2.20.

Figura 2.20. Configuració d'un domini



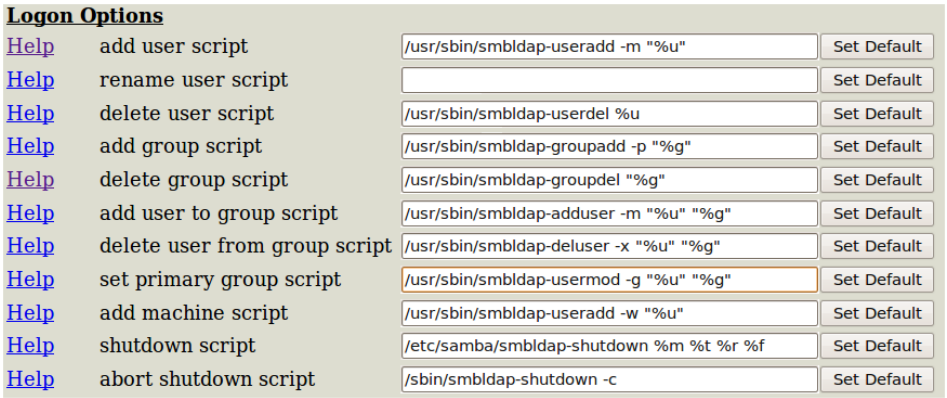
A més de les opcions que veiem en la imatge hem de configurar també l'opció passdb backend, el valor de la qual serà:

```
1 passdb backend=ldapsam:ldap://localhost
```

Utilitzarem localhost, si la màquina on tenim instal·lat el servei LDAP és la mateixa màquina on tenim instal·lat el servei Samba.

Per poder treballar amb les eines de gestió d'usuari remotament com a *root* des de Windows cal configurar els *scripts* de gestió d'usuari GNU/Linux, com es mostra en la figura 2.21.

Figura 2.21. Configuració d'scripts de gestió d'usuari



A més del següent parametre:

```
1 passwd program=/usr/sbin/smbldap-passwd %u
```

On el significat dels *scripts* és el mateix que el que s'ha vist anteriorment.

Una vegada fet tot el procés de configuració anterior, caldria comprovar que la implementació del servei Samba amb OpenLDAP funciona fent servir les ordres següents:

```
sudo pdbedit –Lv | more
smbclient -U nou_usuari –L GRUPIOC
Password: contrasenya_usuari
```

Amb aquest pas acaba el procés de configuració, només caldria la introducció de les dades dels usuaris i recursos del domini i començar a treballar.

Finalment, cal comentar que al servidor OpenLDAP hi ha dades confidencials, com els atributs SambaLMPassword i SambaNTPassword, que per qüestions de seguretat estan xifrades. Tot i això, es poden aplicar atacs de força bruta sobre aquests atributs o es poden utilitzar directament per fer-se passar per un altre usuari. Per tant, les comunicacions entre Samba i OpenLDAP sempre és millor que estiguin xifrades, és a dir, no s'ha d'utilitzar: **ldap ssl = off**. També cal evitar que els usuaris no administradors d'OpenLDAP puguin consultar els atributs crítics.