Integració de sistemes operatius en xarxa lliures i propietaris

Oriol Pérez Lozano

Índex

Introducció

En els darrers anys, el continu canvi tecnològic en què s'ha vist immersa la informàtica ha modificat radicalment la manera com els usuaris intercanvien informació. Des de finals de la dècada dels seixanta fins a ben entrats els anys noranta, les xarxes informàtiques s'utilitzaven gairebé exclusivament en entorns empresarials i acadèmics. A dia d'avui l'escenari és completament diferent i poques són les empreses on les xarxes no hi són presents.

L'evolució dels sistemes operatius reflecteix aquesta tendència, i la majoria d'ells disposen de programari per a la comunicació entre els ordinadors d'una xarxa. En un entorn empresarial, l'accés als recursos s'acostuma a controlar mitjançant un sistema operatiu en xarxa (SOX) instal·lat als servidors. Aquests sistemes operatius, a diferència de la resta, permeten l'administració centralitzada dels recursos de la xarxa (generalment dades, programes i dispositius) i controlen la seguretat de la xarxa, oferint als usuaris la possibilitat de connectar-se o no als diferents recursos. Si no es disposa d'un sistema operatiu en xarxa, els equips no poden compartir els recursos i els usuaris no els poden fer servir.

Actualment, existeix un ventall molt ampli de sistemes operatius en xarxa per a servidors i resultaria pràcticament impossible llistar-los tots aquí. Tot i això, podem fer una distinció entre sistemes operatius en xarxa lliures i propietaris. Entre els SOX lliures més utilitzats podem destacar els sistemes de tipus Unix, com ara les distribucions GNU/Linux (Debian, Ubuntu, Fedora, OpenSuSE, etc.), els sistemes de la família BSD (FreeBSD, OpenBSD) i el sistema Open Solaris (Unix System V/Solaris). D'altra banda, els SOX propietaris amb més força al mercat són Microsoft Windows Server 2000/2003/2008 (Windows), Mac OS X Server (BSD/Unix) i Solaris (Unix System V).

Amb totes les opcions que existeixen, i els avantatges i inconvenients que tenen cadascun d'aquests sistemes, sembla lògic que cada vegada amb més freqüència les empreses no treballin exclusivament amb un tipus de sistema, sinó que apostin per solucions que ofereixen els diferents sistemes operatius. Aquesta unitat centra el seu contingut en explicar com integrar sistemes de diferents famílies, el que anomenem sistemes heterogenis.

Com que en l'àmbit de les estacions de treball Windows és el sistema operatiu més utilitzat i les variants d'Unix (com ara Linux) tenen una elevada quota en el món dels servidors, gran part del contingut de la unitat se centra en la interoperabilitat dels dos sistemes, i en aquest sentit, veureu com el programari **Samba** hi juga un paper important.

En el primer apartat veureu quines són les solucions destinades a la compartició de recursos en diferents famílies de sistemes operatius: Windows, Mac OS X i Unix (Linux). Alhora, es dóna una visió de les funcions que pot realitzar Samba dins d'una xarxa heterogènia com a substitut d'un servidor Windows.

En el segon apartat veureu com integrar dins d'una mateixa xarxa sistemes operatius Windows i servidors Linux amb el servei Samba. En aquest context us podeu trobar situacions molt diferents, i Samba disposa d'un nivell de configuració molt elevat que permet obtenir una bona adaptació a moltes d'aquestes situacions. Tractarem les dues situacions més comunes que us podeu trobar: Samba com a servidor independent en un grup de treball i Samba com a servidor de domini.

Resultats d'aprenentatge

En acabar aquesta unitat, l'alumne:

1. Integra sistemes operatius lliures i propietaris, justificant i garantint la seva interoperabilitat.
    - Estableix nivells de seguretat per controlar l'accés del client als recursos compartits en xarxa.
    - Comprova la connectivitat de la xarxa en un escenari heterogeni.
    - Descriu la funcionalitat dels serveis que permeten compartir recursos en xarxa.
    - Instal·la i configura serveis per compartir recursos en xarxa.
    - Comprova el funcionament dels serveis instal·lats.
    - Treballa en grup per accedir a sistemes de fitxers i impressores en xarxa des d'equips amb diferents sistemes operatius.
    - Documenta la configuració dels serveis instal·lats.

1. Xarxes heterogènies

Una xarxa és un conjunt d'equips interconnectats entre si que permet l'enviament i la recepció de dades. De manera anàloga a quan un conjunt de persones es vol comunicar entre si, en una xarxa els equips poden utilitzar diferents "idiomes" (protocols) per comunicar-se. D'aquesta manera, l'intercanvi de dades és possible només si els dos extrems de la comunicació entenen el protocol utilitzat. En aquest sentit, al llarg dels anys s'han desenvolupat enormes quantitats de protocols, més o menys especialitzats, destinats a aquest intercanvi de dades.

En els darrers anys, i gràcies al procés d'estandardització d'alguns protocols utilitzats a Internet (HTTP, FTP, SMTP, etc.), s'ha aconseguit que dispositius de diferents famílies es poguessin comunicar a través d'Internet sense problemes. Així, doncs, actualment seria impensable imaginar un escenari on per visitar una pàgina web allotjada en un servidor Linux no poguessis fer servir un equip Windows o a l'inrevés.

Com veureu a continuació, en les xarxes locals alguns dels protocols més utilitzats han anat sempre lligats al fabricant dels sistemes, fet que ha dificultat la integració entre diferents sistemes.

1.1 Descripció d'escenaris heterogenis

El model de xarxa determina quin és el rol dels equips que la integren. Aquest depèn en major o menor mesura de les necessitats de l'organització. En aquest aspecte es pot distingir entre:

1. Xarxes igualitàries
2. Xarxes centralitzades

Cada model té els seus avantatges i inconvenients, i per a cada família de sistemes operatius podem trobar diverses implementacions. Històricament, els grans fabricants han ofert solucions adaptades a la seva pròpia família de sistemes operatius i s'han preocupat poc de la compatibilitat amb la resta.

Actualment, però, són poques les xarxes homogènies que es troben en les organitzacions i cada vegada creix més la necessitat d'integrar diferents famílies de sistemes operatius en un mateix entorn.

Per això convé conèixer quines són les solucions que podem trobar en els diferents sistemes operatius.

1.1.1 Xarxes igualitàries

Originalment, les xarxes igualitàries es van dissenyar per permetre compartir recursos des de màquines d'escriptori amb altres usuaris de la xarxa.

En una xarxa igualitària, cada ordinador (*host*) pren el rol de client i servidor, de manera que cadascuna de les màquines determina els recursos que ofereix a la resta i és responsable de la seva pròpia seguretat.

La paraula *host* en aquest context fa referència a qualsevol ordinador connectat a la xarxa.

Els protocols utilitzats en aquestes xarxes també permeten visualitzar i navegar per la llista de recursos compartits sense que hi hagi un servidor central. Els usuaris poden encendre o apagar les seves màquines sense por d'interrompre altres usuaris o serveis de la xarxa (excepte quan estan accedint a recursos propis).

Aquest escenari és el més comú quan la xarxa té un nombre reduït d'ordinadors. En aquests casos també és el més simple de configurar i administrar. Alguns dels avantatges que presenten les xarxes igualitàries respecte a les xarxes centralitzades són:

1. Fiabilitat: la disponibilitat dels recursos no depenen només d'una màquina.
2. Escalabilitat: afegir ordinadors a la xarxa és una tasca simple.
3. Distribució de càrrega: la càrrega de treball es distribueix entre diferents màquines i no recau només en el servidor.
4. Disponibilitat: la caiguda d'una màquina només afecta els recursos compartits per ella.

Xarxes igualitàries en entorns Windows

Històricament, les xarxes igualitàries entre sistemes Windows es coneixen amb el nom de **grup de treball** o *workgroup* i utilitzen els protocols **NetBIOS** i **SMB/CIFS**. El grup de treball s'identifica amb un nom i determina una agrupació d'equips que comparteixen recursos, però en cap cas marca els límits d'una zona de seguretat (és a dir, un membre d'un grup de treball pot accedir a una màquina en un altre grup de treball).

Els equips que comparteixen el mateix nom de grup de treball i pertanyen a la mateixa xarxa apareixen agrupats quan s'explora l'entorn de xarxa. Un *host* Windows, independentment de la versió, ha de ser membre o bé d'un grup de treball o bé d'un domini.

Atès que cada màquina d'un grup de treball és responsable de la seva pròpia seguretat, quan un usuari vol accedir a un recurs compartit cal que tingui un compte d'usuari local a la màquina servidor.

Un recurs dins d'una xarxa s'identifica amb una ruta UNC (*universal naming convention*), que típicament pren la forma `\\NomMaquina\Recurs`. Per exemple, si suposem que dins del nostre grup de treball hi ha una màquina anomenada

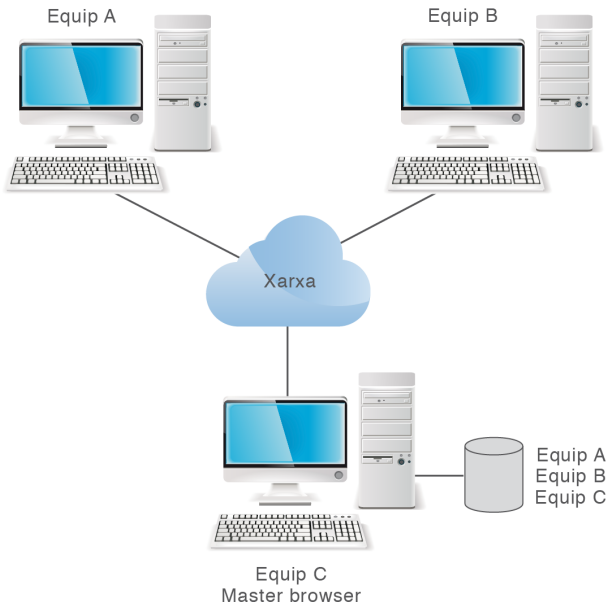
IOC que comparteix una carpeta anomenada *Public*, podrem accedir al recurs amb la UNC `\\IOC\Public`. També podem fer servir l'adreça IP del servidor (`\\192.168.0.6\Public`).

Les adreces UNC no distingeixen majúscules i minúscules.

Una de les característiques més útils dels grups de treball a Windows és la possibilitat d'explorar els recursos compartits d'una xarxa. D'aquesta manera, no és necessari que l'usuari sàpiga l'adreça UNC exacta del recurs al que vol accedir, sinó que pot "navegar" per tots els equips de la xarxa de manera similar a com ho faria en el sistema d'arxius local. Simplement cal que faci clic sobre el botó *Entorn de xarxa* i la llista d'ordinadors apareixerà a la finestra.

Per tal que tots els equips puguin explorar la xarxa d'una manera òptima i sense saturar-la, una de les màquines del grup de treball conté una base de dades amb tots els ordinadors connectats a la xarxa, com podeu observar a la figura 1.1. Aquesta màquina es coneix amb el nom de *master browser*. El *master browser* és responsable d'obtenir tota la informació necessària per crear i mantenir la llista d'ordinadors del grup de treball. La resta d'equips anuncien la seva presencia just en el moment en el qual es connecten al grup de treball i el *master browser* els afegeix a la base de dades. Qualsevol màquina d'un grup de treball és susceptible de ser *master browser* i el procés d'elecció es realitza de forma totalment transparent per als usuaris.

FIGURA 1.1. Master browser en un grup de treball



Per evitar que el *master browser* sigui un punt de fallida en cas que es perdi la connexió, també existeix el rol de *backup browser*. El *backup browser* és una altra màquina amb una còpia de la llista d'ordinadors. Cada cert temps, *master* i *backup browser* sincronitzen les seves bases de dades.

Problemes de sincronització en grups de treball

Si heu fet servir els grups de treball per compartir arxius entre sistemes Windows, probablement alguna vegada haureu vist com dos equips d'una mateixa xarxa mostren

llistes d'equips diferents sense raó aparent. Alguns equips apareixen en una llista però no en l'altra. El motiu principal acostuma a ser que el *master* i *backup browser* encara no s'han sincronitzat.

Els grups de treball funcionen relativament bé mentre hi hagi poques connexions i desconnexions a la xarxa. No passa el mateix quan ens trobem en un escenari amb canvis continus d'ordinadors, amb moltes connexions i desconnexions en intervals curts de temps. El resultat es tradueix en unes bases de dades no actualitzades i no sincronitzades, que comporten una experiència no gaire agradable per l'usuari. Actualment, amb l'auge dels dispositius portàtils, on són freqüents les connexions i desconnexions, aquest mecanisme resulta molt poc pràctic.

A partir de Windows 7 apareix un nou sistema destinat a la compartició de recursos en xarxes igualitàries domèstiques anomenat ***homegroup***. Es tracta d'una funció que simplifica la tasca de compartir recursos.

Microsoft ha publicat l'especificació de *homegroup* com a part del programa Open Specification. Aquest fet permet a qualsevol crear la seva pròpia implementació de *homegroup*, i per tant obre la porta a la implementació lliure en altres sistemes operatius. *Homegroup* fa servir una tecnologia similar a les que fan servir les xarxes P2P, com ara BitTorrent, gràcies a dos protocols:

1. ***Peer-to-peer graphing protocol*(PPGRH):** permet que tots els nodes d'una xarxa tinguin exactament la mateixa base de dades d'ordinadors (desapareix el rol de *Master Browser*).
2. ***Peer name resolution protocol*(PNRP):** permet la resolució de noms.

Aquests protocols, a diferència de NetBIOS i SMB/CIFS, s'han dissenyat de manera que la xarxa es pot expandir per Internet i sense necessitat que cap màquina actuï com a *master browser*. Per tant, s'eliminen els problemes de sincronització. La part negativa és que, de moment, el *homegroup* només està implementat en sistemes operatius Windows 7 i posteriors.

Xarxes igualitàries en entorns Unix/Linux

Tradicionalment, la compartició d'arxius entre màquines Unix s'aconsegueix amb el protocol *network file system* (NFS). L'última versió, NFSv4, incorpora moltes millores respecte a les versions prèvies i és la que es fa servir actualment en totes les distribucions de GNU/Linux.

A Debian podem instal·lar un servidor NFS afegint els paquets `nfs-kernel-server`, `nfs-common` i `portmap`:

```
1 # apt-get install nfs-kernel-server nfs-common portmap
```

La configuració d'NFS al servidor es realitza dins de l'arxiu `/etc/exports`. En aquest s'indica, per a cada línia:

1. Directori que es vol compartir
2. Nom o IP de la màquina que hi tindrà accés

3. Opcions (entre parèntesis i separades per comes)

```
# cat /etc/exports
/directori/compartit 192.168.0.0(ro,root_squash)
/directori/compartit2 192.168.0.0(ro,root_squash)
```

Els clients GNU/Linux poden accedir al servidor muntant el directori compartit tal i com es faria amb qualsevol altre dispositiu, indicant el tipus *nfs* a l'ordre `mount` i l'adreça o el nom del servidor tal i com es mostra a continuació:

```
$ mount –t nfs4 192.168.0.6:/directori/compartit /punt_muntatge
```

NFS controla qui pot muntar els sistemes de fitxers basant-se en la màquina que ho demana i no en l'usuari que farà servir el sistema de fitxers.

Tot i que el protocol NFS s'ha fet servir durant anys, en un món dominat pel sistema operatiu Windows moltes distribucions de GNU/Linux d'escriptori incorporen també Samba com a client-servidor SMB/CIFS per integrar-se a les xarxes Windows.

Xarxes igualitàries en entorns Mac

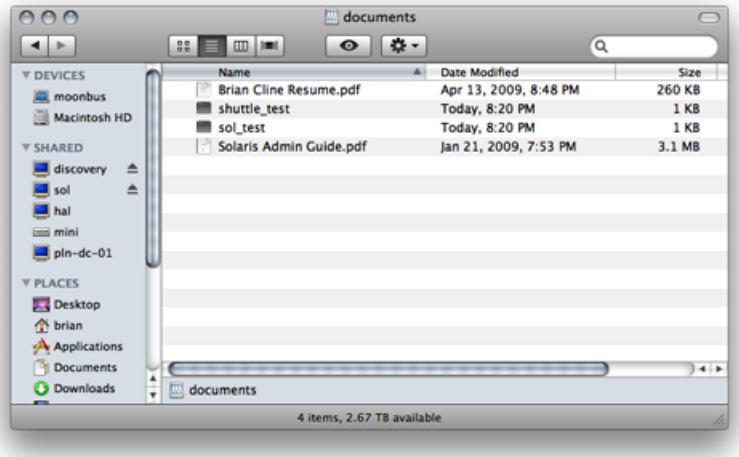
Els equips amb sistemes operatius Mac OS X treballen de forma nativa amb diversos protocols per a la compartició de recursos. En general, un sistema Mac OS X implementa:

1. El protocol *Apple filing protocol* (AFP)
2. Els protocols SMB/CIFS i NetBIOS
3. El protocol NFS

Aquesta característica permet la **compatibilitat amb sistemes operatius Unix/Linux i Windows** sense necessitat d'instal·lar cap software de tercers. Típicament, el protocol AFP s'utilitza quan es comparteixen fitxers entre equips Mac gràcies a que proveeix una interfície totalment adaptada al sistema de fitxers d'Apple (HFS+). L'adreça d'un recurs compartit per un servidor AFP comença per `afp://`. Però també podem connectar-nos a un recurs SMB i NFS fent servir les adreces `smb://` i `nfs://` respectivament.

Un dels avantatges de fer servir Mac OS és que la connexió a diferents tipus de servidors es realitza d'una manera uniforme a través del programa Finder (figura 1.2).

FIGURA 1.2. Finder permet l'accés als recursos compartits amb diferents protocols



L'accés a un recurs compartit per Windows s'especifica amb la forma `smb://servidor/recurs`, on *servidor* és la IP o el nom del servidor i *recurs* és el nom del recurs compartit.

1.1.2 Xarxes centralitzades

El model de xarxa d'igual a igual, o d'entorn de treball, funciona relativament bé quan s'implanta en un entorn amb un grup d'usuaris reduït i amb pocs equips. A mesura que el nombre d'ordinadors connectats a la xarxa va augmentant, l'administració dels recursos, dels usuaris i dels permisos comença a ser una tasca tediosa.

En les xarxes grans, els usuaris i les màquines s'acostumen a agrupar en **dominis**, de manera que l'administració dels recursos, així com els seus permisos, es pot realitzar de manera centralitzada.

> Des del punt de vista de l'administració de sistemes, un domini és un conjunt d'equips interconnectats que comparteixen informació administrativa (usuaris, grups, contrasenyes, etc.).

En aquest escenari, un servidor és el que s'encarrega del control d'accés als recursos, i no pas cada màquina, com és el cas de les xarxes igualitàries, típicament mitjançant un esquema client-servidor. Per exemple, quan un usuari vol iniciar una connexió en qualsevol dels ordinadors (clients) del domini, aquest ordinador haurà de validar les credencials de l'usuari al servidor, i obtenir d'aquest totes les dades necessàries per poder crear el context inicial de treball per a l'usuari.

D'altra banda, un dels desavantatges d'aquest model és que l'accés a la xarxa queda supeditat a la disponibilitat del servidor. És a dir, que si un client no pot contactar amb el servidor tampoc no podrà accedir als recursos. Aquest problema

es pot solucionar disposant un o diversos servidors de reserva (*backup*), que actuen en cas de caiguda del servidor principal.

Dominis en entorns Unix

Històricament, en el món Unix els dominis solien implementar-se mitjançant el conegut *network information service* (**NIS**), del qual n'existeixen actualment múltiples variants per diferents sistemes i entre les quals podem trobar versions per a GNU/Linux. El disseny original de NIS va ser desenvolupat per Sun Microsystems, i es tracta d'un protocol client-servidor que permet l'accés a un servei de directori. La finalitat d'aquest protocol és centralitzar l'administració de sistemes Unix. La implementació inicial de Sun constava d'un servidor, una llibreria per a la part dels clients i diverses eines d'administració del directori.

En general, en un domini NIS es diferencien tres tipus d'ordinadors: servidors mestres, servidors esclaus i clients. Un domini NIS ha de tenir, com a mínim, un servidor mestre. En aquest servidor s'hi emmagatzema la informació referida als usuaris i grups del domini, així com els recursos. Els servidors esclaus permeten alliberar la càrrega del servidor mestre i de cara als clients es comporten de la mateixa manera. Les actualitzacions només es poden realitzar directament al servidor mestre. Una limitació important de NIS és que tots els clients han de d'estar en la mateixa subxarxa IP que el servidor mestre.

El sistema NIS original ha demostrat tenir greus limitacions inherents al seu disseny, especialment en referència a l'escalabilitat i la seguretat. Aquest fet va provocar que el reemplacessin altres tecnologies. Com a contrapartida, i amb la intenció de millorar i corregir els problemes inicials de NIS, Sun Microsystems va introduir **NIS+**. Va afegir-hi fortes millores en seguretat, flexibilitat i escalabilitat. Aquestes millores també van anar lligades a un augment de la complexitat en l'administració d'aquests sistemes, cosa que va provocar, gairebé de forma definitiva, l'abandonament de NIS a favor d'altres tecnologies molt més potents i escalables com ara **LDAP**.

Un domini LDAP s'estructura de manera similar a un domini NIS: hi ha servidors mestres, esclaus i clients. Els clients poden obtenir informació dels mestres o esclaus, però tots els canvis han d'aplicar-se als servidors mestres. Hi ha moltes implementacions d'un servei de directori LDAP, però una de les més utilitzades és **OpenLDAP**.

OpenLDAP és un programari de codi lliure que permet adaptar-se a diverses necessitats. Es tracta d'un servei de directori robust, ràpid i escalable que no té res a envejar a altres serveis de directori. La complexitat d'OpenLDAP serà valorada per aquells administradors que vulgui construir un servei de directori personalitzat.

Dominis en entorns Windows

El servei de controlador de domini en xarxes Windows es va implementar per primera vegada a la versió 3.5 de Windows NT i va millorar posteriorment a Windows NT 4. Aquest servei es va conèixer inicialment com a *NT directory services* (NTDS). Per primera vegada s'oferia la possibilitat d'unificar i centralitzar l'administració dels equips Windows d'una xarxa. Fins aleshores, aquesta tasca s'havia de realitzar equip a equip. Entre molts altres avantatges, es permetia que els usuaris d'una xarxa poguessin accedir als recursos del domini independentment de la màquina que fessin servir.

L'estructura d'un domini Windows NT en una xarxa és molt simple. Dins de cada domini ha d'haver-hi, com a mínim, un controlador primari de domini (CPD) i, de manera opcional, un o més controladors de domini de reserva (BDC). És en aquestes màquines on es troba la informació administrativa i de seguretat del domini. Si el controlador primari deixa d'estar operatiu, els usuaris poden accedir al domini a través d'un dels controladors de reserva (en cas d'existir). Tot i així, les tasques administratives només es poden realitzar directament al controlador primari de domini.

Amb l'aparició del primer sistema operatiu de la família Windows Server (Windows 2000 Server) **es van introduir canvis importants en el servei de controlador de domini**. Aquest, que anteriorment es coneixia com a NTDS, va passar a anomenar-se *Active Directory domain services*. D'aquesta manera, podem distingir dos tipus de dominis Windows:

1. Dominis NT
2. Dominis Active Directory

La diferència més significativa entre dominis NT i active directory radica en que els segons permeten controlar una varietat molt gran de tipus d'objectes dins d'un domini: usuaris, grups, màquines, serveis, i fins i tot definir nous tipus d'objectes (NTDS només permetia definir usuaris i grups). A més, tots els objectes queden **organitzats de forma jeràrquica i accessible mitjançant el protocol LDAP**. Aquesta darrera característica va obrir la porta a la **interoperabilitat** amb aplicacions d'altres plataformes com Unix.

> Windows Server utilitza el protocol LDAP per accedir a la base de dades d'Active Directory, fet que permet la **interoperabilitat** amb aplicacions d'altres plataformes, com per exemple GNU/Linux.

Dominis en entorns Mac

El servei de directori natiu a Mac OS X s'anomena ***open directory***i qualsevol sistema actual d'Apple, sigui versió servidor o d'escriptori, inclou una base de

dades *open directory* local. En aquest directori s'emmagatzema la informació dels comptes d'usuaris locals.

Un ordinador Mac OS X Server pot prendre el rol de controlador de domini *open directory* quan es configura com a *open directory master*. *Open directory* fa servir el protocol LDAP i emmagatzema informació d'administració, usuaris, grups i comptes de màquina de forma jeràrquica. El servei de directori es pot vincular a un servidor de contrasenyes (*open directory password server*) i, opcionalment, a un regne Kerberos, que proveeix un mecanisme d'autenticació segur.

És important destacar que fins a la versió v10.6 els servidors Mac podien simular el rol d'un controlador de domini Windows NT. A partir de llavors aquesta funcionalitat, molt útil en entorns heterogenis, s'ha deixat d'implementar. De tota manera, a Mac OS X es pot fer servir Samba.

Dominis en entorns heterogenis

És cada vegada més habitual que les organitzacions tinguin simultàniament sistemes operatius de diferents famílies. En aquest tipus d'escenaris, la opció més senzilla, i moltes vegades utilitzada, és gestionar els diferents sistemes de forma independent, fent servir les eines administratives que cada fabricant proporciona.

En un entorn com el descrit, una de les solucions que es pot adoptar és crear diferents dominis per a cada tipus de sistema: un domini Unix, un domini Windows, etcètera. Aquesta és una manera simple amb la qual podem administrar, de forma centralitzada, els recursos de xarxa agrupats en famílies. És evident que aquesta solució suposa la repetició de tasques administratives per a cada domini: creació d'usuaris i grups, configuració de permisos, polítiques de seguretat, administració de recursos compartits entre sistemes...

Una opció més elegant, però més complicada, és integrar tots els equips en un mateix domini de manera que s'agrupin tots els sistemes de l'organització en una única administració centralitzada. Lamentablement, aquesta opció no és senzilla, ja que els diferents fabricants de sistemes no acostumen a fer el disseny perquè siguin compatibles entre sí (especialment quan el fabricant és una empresa que defensa un producte comercial). Fins i tot quan els sistemes es basen en tecnologies estàndard (com LDAP en el cas de Windows Server i Linux), aquesta integració no resulta fàcil. Això es degut principalment a les diferències de disseny entre sistemes i al fet que cap dels sistemes acostuma a implementar els estàndards de forma complerta fins a l'últim detall.

Tot i això, administrar un domini en el qual els sistemes no pertanyen a la mateixa família és una tasca que s'ha anat simplificant cada cop més. Si bé al principi era molt difícil integrar sistemes operatius diferents en un mateix domini, en els darrers anys han sorgit moltes solucions que faciliten aquesta integració, tant si es fan servir servidors Windows amb clients GNU/Linux com a l'inrevés.

Entre aquestes solucions podem destacar-ne dues:

1. ***Windows services for UNIX*** (**SFU**), per integrar sistemes Unix amb servidors Microsoft Windows Server.

2. **El paquet de software Samba**, per integrar sistemes Windows amb servidors Unix.

El *Windows services for UNIX* (SFU) o *Subsystem for UNIX-based applications* (SUA) és un paquet de programari produït per Microsoft que proporciona o emula parts d'un sistema Unix dins d'un sistema operatiu Windows NT o successor. La versió SFU 3.5 va passar a anomenar-se SUA (per això es coneix pels dos noms) i està inclosa a Windows Server 2003 R2 i Windows Server 2008. Dins dels sistemes Windows Server 2008 i d'algunes versions de Windows Vista i 7 (Enterprise i Ultimate) s'hi inclou un paquet mínim SUA. Aquest software es pot descarregar de manera gratuïta del lloc web de Microsoft.

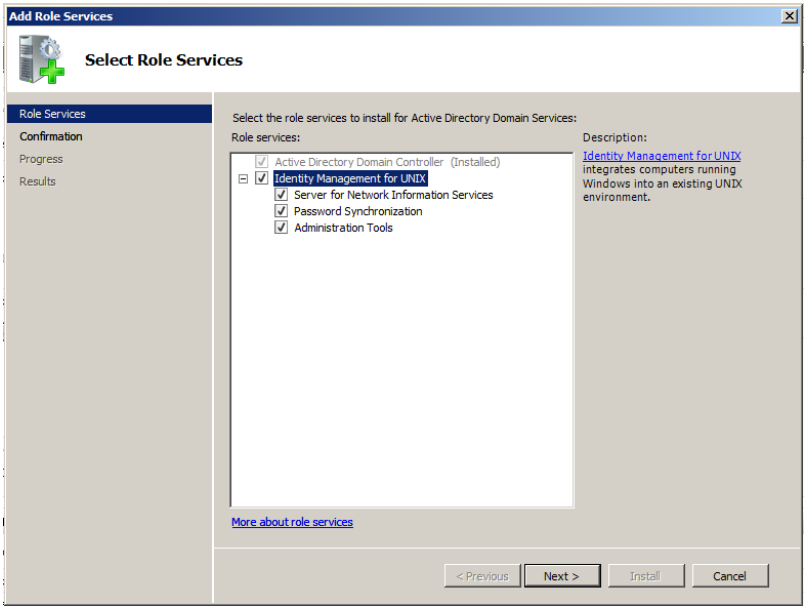
El paquet SUA de Microsoft ofereix moltes funcionalitats, però n'hi ha algunes que són molt útils a l'hora d'integrar sistemes Windows i Unix, com ara:

1. Administració d'identitats per a Unix
2. Client NFS
3. Servidor NFS
4. Servidor NIS

NFS

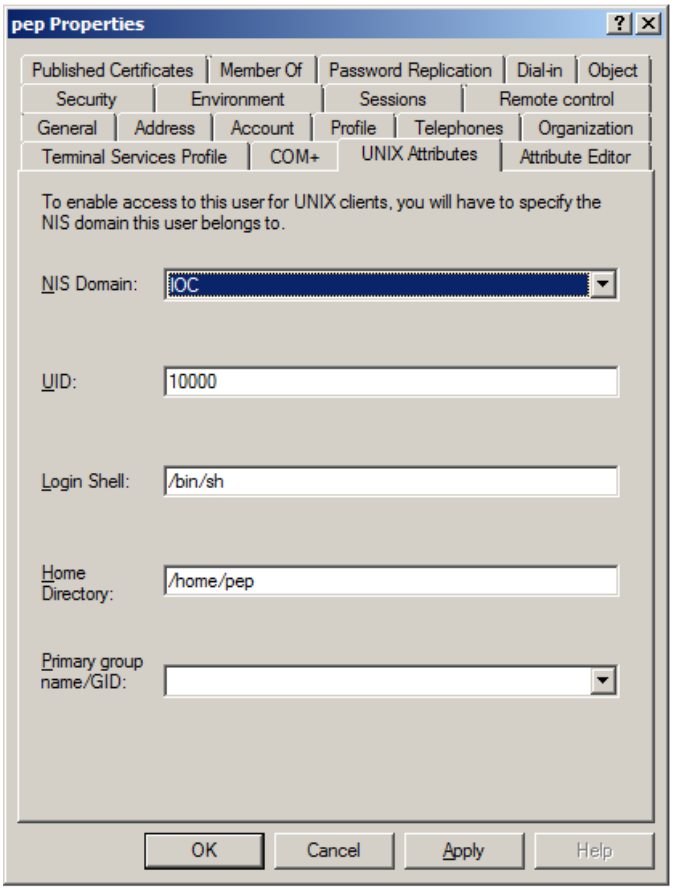
Network file system és un protocol dissenyat per accedir a sistemes d'arxius remots. NFS s'inclou per defecte en tots els sistemes operatius de la família Unix i permet compartir arxius a través de la xarxa.

FIGURA 1.3. Instal·lació del servidor NIS a Windows 2008



L'administració d'identitats per a Unix és un rol d'Active Directory que només es pot instal·lar en els controladors de domini i que **permet assignar atributs Unix als usuaris i grups del directori**. Podem afegir aquesta funcionalitat mitjançant l'eina *Administrador del servidor*, dins dels serveis de rol d'Active Directory (figura 1.3). Un cop instal·lada, podrem indicar per a cada usuari l'UID, el *shell*, el directori *home* i el GID del grup principal, tal com mostra la figura 1.4 (informació que en un sistema Unix es troba dins de l'arxiu `/etc/passwd`).

FIGURA 1.4. Atributs UNIX a Active Directory



Amb l'eina d'administració d'identitats per a Unix, una màquina Windows Server amb Active Directory treballa també com un servidor NIS i permet a les màquines Unix treballar en el mateix domini.

Windows Server pot actuar com un servidor NIS gràcies al paquet de software SUA, fent que els usuaris i grups d'Active Directory tinguin atributs específics de Unix.

Si els paquets SFU i SUA ens permeten afegir sistemes Unix a un domini administrat amb Windows, el paquet de software **Samba** ens permet tot el contrari: afegir sistemes Windows dins d'un domini administrat per màquines GNU/Linux. Samba va començar com un projecte que buscava oferir interoperabilitat als clients de Windows NT 3.x amb un servidor UNIX. Inicialment permetia compartir impressores i arxius entre Windows i Linux, però actualment **Samba pot actuar com un controlador de domini compatible amb Windows NT**. És a dir que podem unir un sistema Windows a un domini gestionat pel servei Samba, tal com ho faríem si el servidor fos Windows. Tot i això Samba té algunes limitacions que veureu més endavant i, per exemple, encara no ofereix la possibilitat de funcionar com un controlador de domini de tipus Active Directory.

1.2 El servei Samba en un escenari heterogeni

Samba és un dels grans èxits del moviment de codi obert. Prova d'això és el reconeixement i l'acceptació que ha tingut darrerament en el món de les TIC, on s'ha convertit en una espècie de servei estàndard en xarxes on conviuen sistemes operatius GNU/Linux i Windows. De fet, gran part de la seva popularitat es deu precisament a la seva capacitat per integrar-se en xarxes Windows. Samba pren el nom del protocol *server message block* (SMB), inicialment desenvolupat per Microsoft, IBM, Intel i d'altres per permetre que els sistemes operatius DOS, Xenix, OS/2 i Windows, al final dels anys 80, poguessin compartir unitats, arxius i impressores. El protocol SMB va canviar de nom l'any 1998 i va passar a anomenar-se *common Internet file system* (CIFS). A dia d'avui, aquest protocol és el que encara es fa servir als sistemes Windows per compartir arxius. L'alternativa en sistemes GNU/Linux és Samba: un paquet de software que pot estar present en situacions molt diverses, des d'un entorn domèstic per compartir arxius i impressores fins a un entorn corporatiu realitzant les tasques d'un controlador de domini.

SMB i CIFS

CIFS es pot considerar una evolució de les moltes que s'han fet del protocol SMB. El canvi de nom va ser part d'una estratègia de Microsoft, però popularment s'ha seguit anomenant SMB. Per això, en molts textos encara podem trobar les sigles SMB o CIFS, indistintament, per referir-se al mateix protocol.

Inicialment es va dissenyar per permetre la compartició de directoris i impressores entre màquines amb diferents sistemes operatius, en concret entre Windows i Unix, però a mesura que passava el temps s'hi han anat afegint més funcionalitats. Samba pot treballar en la majoria de sistemes de tipus Unix, com GNU/Linux, Solaris, AIX, BSD i Mac OS X. Actualment, Samba implementa diversos serveis i protocols que permeten, entre d'altres funcionalitats:

1. La compartició de directoris
2. L'administració i compartició d'impressores, amb controladors associats per accedir des dels clients Windows
3. L'autenticació de clients en un domini Windows
4. L'assistència a la navegació de l'entorn de xarxa (*network browsing*)

Aquestes funcions faciliten que màquines Windows i GNU/Linux **puguin conviure dins d'una mateixa xarxa**. Tant és així, que en algunes situacions és possible substituir un sistema Windows per un sistema GNU/Linux amb Samba sense que els clients se n'adonin. En realitat, un client Windows no sap si la màquina amb la que s'està comunicant és un altre sistema Windows, l'únic que cal és que la màquina de l'altre extrem es comporti com a tal, i en alguns aspectes Samba pot actuar com un servidor Windows.

Molts són els avantatges de l'ús de Samba respecte a un sistema Windows, però en destaquen sobretot:

1. El cost: fer servir els sistemes Windows requereix adquirir-ne prèviament les llicències; en canvi, podem fer servir GNU/Linux i Samba de forma gratuïta.

2. La interoperabilitat entre sistemes: podem fer servir GNU/Linux i Samba per compartir impressores o arxius accessibles des de Windows o Unix.

3. L'adaptabilitat: en tractar-se d'un projecte de codi obert, s'hi poden introduir les modificacions que convinguin.

Tot i això, no podem veure en Samba la solució gratuïta que ens permet substituir definitivament un servidor Windows. Hi ha funcionalitats que encara no estan implementades però que estan en procés, i n'hi ha d'altres que probablement no s'implementaran.

1.2.1 Rols del servei Samba en un escenari heterogeni

Heu de tenir molt clares les funcions que implementa Samba, ja que en alguns escenaris l'ús de Samba no és una bona opció i no queda més remei que fer servir un servidor Windows. El rol de Samba en una xarxa està determinat per la seva configuració, que generalment es farà a través del fitxer `/etc/samba/smb.conf`. La taula 1.1 detalla quins són els rols que compleix (fins a la versió 3.5.6).

TAULA 1.1. Rols que pot prendre Samba

Servidor de fitxers i d'impressores	Sí
Servidor independent (*stand-alone*)	Sí
Controlador de domini de tipus Windows NT	Sí
Membre de domini de Windows NT	Sí
Controlador de domini de tipus Active Directory	No
Membre de domini de tipus Active Directory	Sí
Interacció amb altres controladors de domini Windows	No
Interacció amb altres controladors de domini Samba	Sí
Master browser local	Sí
Master browser de domini	Sí

Protocols propietaris

Alguns dels protocols que fan servir els sistemes Windows són propietaris de Microsoft i no s'han publicat o estan protegits. Aquest és un dels motius que dificulta la tasca dels desenvolupadors de Samba a l'hora d'implementar les mateixes funcionalitats.

A continuació es descriu el significat de cadascun d'aquests rols:

- **Servidor de fitxers i d'impressores**: l'ús més comú de Samba és per compartir fitxers i impressores en escenaris heterogenis.

- **Servidor independent** (***stand-alone***): la forma més simple de funcionament de Samba és aquella en la qual actua com a servidor independent (*stand-alone*). Això significa que no forma part de cap domini i l'accés als recursos compartits és controlat exclusivament per Samba. Aquest rol és el que s'utilitza en escenaris amb xarxes d'igual a igual o grup de treball.

- **Samba com a membre d'un domini**: quan Samba forma part d'un domini, l'accés als recursos que ofereix és controlat pel controlador de domini i no

pas per la pròpia màquina. Samba pot unir-se a un domini NT (Samba o Windows NT) o Active Directory (Windows Server 200x).

- **Samba com a controlador de domini primari**: Samba pot actuar com un controlador primari de domini (PDC) de tipus Windows NT, però no de tipus Active Directory. En aquesta situació, Samba és responsable de l'autenticació dels clients.
- **Samba com a controlador de reserva**: els controladors de reserva (BDC) contenen una còpia de la base de dades d'usuaris i grups del controlador primari de domini, anomenada SAM (*security account manager)*. En cas de caure el PDC, el controlador de reserva s'encarregarà de substituir-lo fins que torni a estar operatiu.
- **Samba com a *local master browser***: en una xarxa d'igual a igual (sense controladors de domini) cada ordinador ha d'anunciar la seva presència a la resta d'equips de l'entorn de treball. Si el nombre d'equips és elevat es pot generar una situació on hi hagi un tràfic continu de paquets per la xarxa. Per evitar el problema, se selecciona una de les màquines del grup perquè contingui la llista de tots els equips connectats. D'aquesta manera, qualsevol una màquina pot anunciar-se i obtenir la llista de tots els equips fent una sola petició. L'equip amb la llista de màquines s'anomena *local master browser* i Samba es pot configurar per actuar com a tal.
- **Samba com a *domain master browser***: de manera similar al *local master browser*, quan ens trobem en un entorn de domini, una de les màquines es fa responsable de la llista d'equips registrats al domini. Aquesta es coneix com a *domain master browser*.

Samba4

Samba4 és el nom d'una versió de Samba en desenvolupament que implementarà un controlador de domini de tipus Active Directory.

Abans de d'aprofundir més en la configuració de Samba **és molt recomanable repassar els conceptes bàsics del seu funcionament**. En els apartats següents tractarem d'explicar alguns dels aspectes que cal conèixer prèviament a l'administració de Samba en un o altre escenari.

1.2.2 Instal·lació del servei Samba

Per instal·lar el servidor Samba en un equip amb el sistema operatiu Debian cal descarregar-se i instal·lar el paquet principal, anomenat **samba**.

```
1 # apt-get install samba
```

Aquest paquet té dues dependències que també s'instal·laran de forma automàtica: `samba-common` i `samba-common-bin`. Tot i que hi ha més paquets relacionats amb samba, com ara `smbclient`, `smbfs`, `swat`, etc., **només el paquet samba i les seves dues dependències són necessàries per establir un servidor**.

Podeu observar quins són els arxius que s'han instal·lat amb el paquet:

```
# dpkg -L samba
```

En general, el servei Samba inclou diverses aplicacions i els següents tres dimonis:

1. **smbd**: procés que rep i atén les peticions que permeten accedir als recursos compartits i autentica els clients.
2. **nmbd**: s'encarrega del registre de noms NetBIOS i participa en el procés d'eleccions a *master browser*.
3. **winbindd**: procés que es comunica amb els controladors de domini per intercanviar informació sobre els comptes d'usuari. Només és necessari quan volem que una màquina GNU/Linux formi part d'un domini Windows. Per defecte no s'inicia.

Un cop descarregat i instal·lat, el servei s'inicia de forma automàtica prenent com a configuració els paràmetres per defecte indicats a l'arxiu `/etc/samba/smb.conf`. Podeu comprovar si els dimonis estan funcionant correctament llistant tots els processos i filtrant pel nom del procés:

```
root@debian:/home/usuari# ps -A | grep nmbd
 2283 ?        00:00:00 nmbd
root@debian:/home/usuari# ps -A | grep smbd
 2287 ?        00:00:00 smbd
 2296 ?        00:00:00 smbd
```

Per aturar, iniciar o reiniciar els dimonis podem fer servir l'eina *service*, que serà necessària quan es canviïn certs aspectes de la configuració.

```
# service samba restart
Stopping Samba daemons: nmbd smbd.
Starting Samba daemons: nmbd smbd.
```

Iniciar o aturar serveis correctament

Fer servir la seqüència service `<nom_script> <paràmetre>` és la millor manera d'iniciar o aturar els serveis, ja que s'executa un script del directori `/etc/init.d/` que ho realitza de manera controlada. No és gens recomanable aturar els serveis directament fent servir l'ordre *kill*.

Opcionalment podem instal·lar un paquet amb documentació molt útil, tant en text pla com en PDF:

```
# apt-get install samba-doc samba-doc-pdf
```

Aquest paquet conté manuals i fitxers de configuració d'exemple que podem trobar dins del directori `/usr/share/doc/samba-doc`. Si disposem d'un navegador podem obrir un fitxer HTML que conté vincles a tota la documentació descarregada.

```
# firefox /usr/share/doc/samba-doc/htmldocs/index.html
```

Un cop comprovat que el servei funciona correctament, cal determinar quin rol ha d'assumir el servei Samba i configurar-lo adequadament segons l'escenari en el qual ens trobem.

Com que el procés de configuració és delicat, us recomanem que quan sigui necessari reviseu els registres (*logs*) dels dimonis **nmbd** i **smbd**. Els podeu consultar dins dels arxius `/var/log/samba/log.nmbd` i `/var/log/samba/log.smbd`

respectivament. És molt útil de cara a descobrir possibles problemes i us ajudarà en el procés d'administració.

Per defecte, Samba mostra només una quantitat molt reduïda de missatges als registres. Quan la informació que veieu al registre no us ajudi a detectar el problema podeu pujar el **nivell de *logging*** per veure missatges més detallats. El nivell dels missatges mostrats es pot canviar amb el paràmetre `log level`, i pot prendre un valor de 0 (menys detall) a 10 (més detall).

```
[global]
     ...
     log level = 3
     ...
```

En general, el nivell 3 és suficient en la majoria d'escenaris. Si feu servir l'ordre *tail* amb la opció *-f* veureu els missatges en temps real a mesura que apareixen:

```
# tail -f /var/log/samba/log.nmbd
```

O bé:

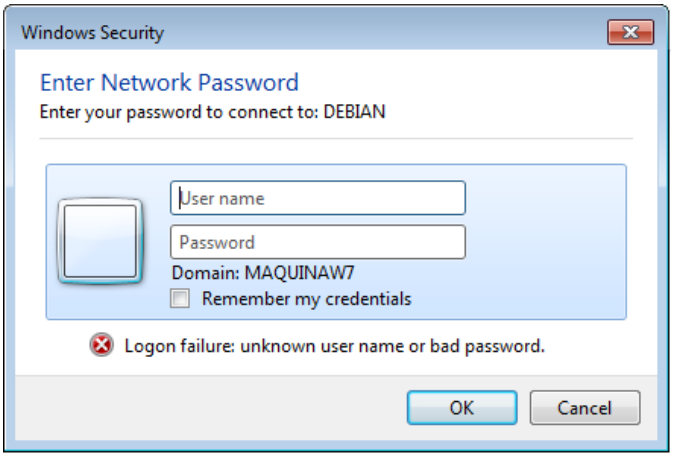
```
# tail -f /var/log/samba/log.smbd
```

1.2.3 Nivells de seguretat

Quan un client vol accedir a un recurs compartit per Samba o per Windows cal comprovar si l'usuari té els privilegis necessaris. Aquesta acció es pot dur a terme de diverses maneres, que estan determinades pel protocol SMB/CIFS. En general, SMB/CIFS defineix dos nivells de seguretat: *user* i *share*. Cadascun d'aquests implica un model d'autenticació per validar les peticions d'entrada. A continuació veiem quines són les diferències entre aquests dos nivells i com es poden configurar a Samba.

1. **Nivell de seguretat *share***. El nivell de seguretat *share* permet assignar una contrasenya a cadascun dels recursos compartits. D'aquesta manera, només aquells usuaris que coneguin la contrasenya hi podran accedir. Aquest sistema té molts inconvenients, el principal és que l'administrador no pot controlar quins usuaris saben la contrasenya. Això és especialment greu en xarxes amb un gran nombre d'usuaris. A més, si es canvia la contrasenya, cal donar-la a conèixer una altra vegada. Actualment, **el nivell *share* es considera obsolet**. Es manté per raons històriques, perquè era el sistema utilitzat en els sistemes Windows 95/98/Me i anteriors. Els desenvolupadors de Samba esperen eliminar aquesta característica en properes versions.
2. **Nivell de seguretat *user***. Quan es configura el nivell de seguretat *user*, l'autorització per accedir als recursos està determinada pels permisos de xarxa de cada usuari. **Quan un usuari (client) vol accedir a un recurs cal que s'autentiqui en el servidor**, típicament mitjançant nom d'usuari i contrasenya (vegeu figura 1.5).

FIGURA 1.5. El nivell de seguretat user requereix que el client s'autentiqui prèviament amb usuari i contrasenya



A Samba, el nivell de seguretat el determina la variable *security* dins de l'apartat `[global]`. Aquesta variable pot prendre cinc valors diferents, un corresponent al nivell de seguretat *share* i els quatre restants corresponents al nivell de seguretat *user*. Aquests valors són: *share*, *server*, *user*, *domain* i *ads*. Les opcions *server* i *share* estan obsoletes, pel que a continuació només es descriu el comportament de *user*, *domain* i *ads*.

Mode de seguretat user

```
1 [global]
2     ...
3     security = user
4     ...
```

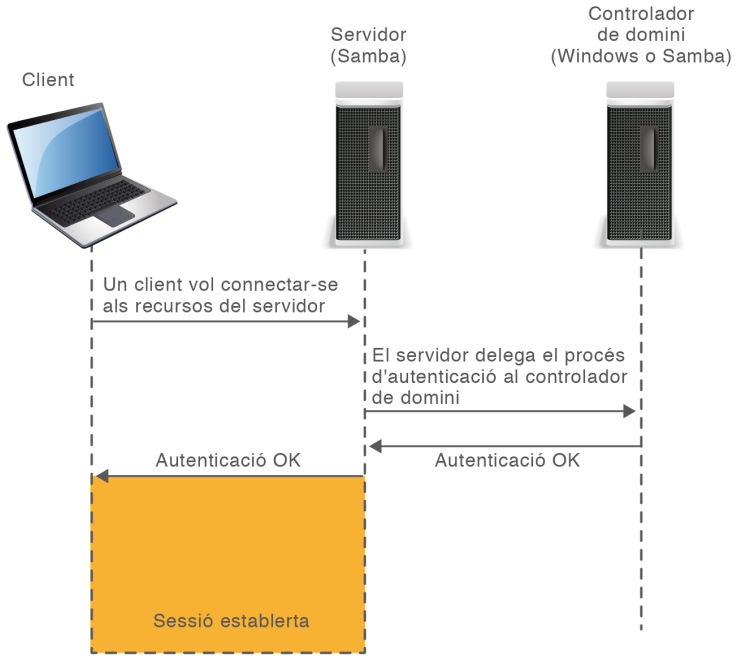
Aquest mode s'utilitza quan Samba actua com un servidor independent (*stand-alone*). Això significa que és el mateix servidor Samba el que s'encarrega de l'autenticació d'usuaris. Per tant, ***user* és el mode utilitzat en escenaris amb xarxes d'igual a igual o entorn de treball**. En aquest cas, Samba normalment disposa de la seva pròpia base de dades d'usuaris, que s'administra de forma local.

Modes de seguretat domain i ads

Quan el servidor Samba i el client es troben dins del mateix domini s'utilitzen els modes de seguretat *domain* i *ads*. D'aquesta manera, quan un usuari vol autenticar-se per accedir a un recurs del servidor Samba (directori o impressora), la petició es redirigeix a un controlador de domini i aquest determina si l'usuari és vàlid. Dit d'una altra manera, la tasca de decidir si l'usuari pot accedir es delega al controlador de domini.

El controlador de domini pot ser una màquina remota, tal i com es mostra a la figura 1.6. Però també pot ser la mateixa màquina amb el servidor Samba si aquest funciona com a CPD.

FIGURA 1.6. Modes de seguretat domain i ads



Amb el modes de seguretat //domain// i //ads//, Samba delega l'autenticació als controladors de domini.

Quina és la diferència entre els modes *domain* i *ads*? **Des del punt de vista del client no n'hi ha cap**: un servidor Samba configurat en el mode de seguretat *ads* es comporta de la mateixa manera que configurat en mode *domain*. La diferència entre aquests dos radica únicament en el procés de comunicació entre Samba i el controlador de domini, on es farà servir un protocol o un altre.

Els dos modes de seguretat, *domain* i *ads*, permeten l'ús del protocol de desafiament/resposta NTLM, que és l'utilitzat en el procés d'autenticació en dominis NT o Active Directory en mode mixt. Però el mode *ads* és l'únic que permet l'ús del protocol Kerberos, que és el que fan servir els controladors de domini Active Directory en mode natiu. En resum, el mode de seguretat *domain* es farà servir quan el controlador de domini sigui de tipus NT o Active Directory en mode mixt (opció activada per defecte a Windows Server). El mode *ads* es pot utilitzar en els mateixos casos que amb *domain* i, a més a més, quan el controlador de domini sigui Active Directory amb autenticació NTLM deshabilitada (mode natiu)**.**

Per configurar el servidor per fer servir el mode de seguretat *domain* cal especificar les opcions següents dins del fitxer de configuració:

```
[global]
     ...
     security = domain
     encrypt passwords = yes
     workgroup = NOM_DEL_DOMINI
     ...
```

Posteriorment cal unir el servidor Samba al domini. Per això farem servir l'ordre `net join`, tot indicant-li un compte d'usuari del domini.

```
# net join -U alumne
```

```
Enter alumne's password:
Joined domain NOM_DEL_DOMINI.
```

Configurar Samba en mode de seguretat *ads*és una mica més complex. En primer lloc, **és necessari que dins de la xarxa hi hagi un servidor DNS**, ja que les llibreries Kerberos el necessiten per resoldre les adreces dels centres de distribució de claus (*key distribution center*). Per tant, cal configurar la màquina amb Samba perquè faci servir aquests servidors (mitjançant el fitxer `/etc/resolv.conf`). A continuació se'n mostra un exemple suposant que el servidor DNS tingui l'adreça 10.0.0.1.

```
# cat /etc/resolv.conf
search NOM_DOMINI.com
nameserver 10.0.0.1
```

Active Directory i DNS

Les llibreries Kerberos necessiten el servei DNS per resoldre les adreces dels centres de distribució de claus (KDC). És per això que quan es promou una màquina Windows Server a controlador de domini (fent servir dcpromo) també s'acostuma a instal·lar el servei de DNS.

A més d'això, és indispensable que la màquina amb Samba tingui instal·lada una llibreria que implementi el protocol Kerberos versió 5. Hi ha diverses opcions, però les més conegudes són **Heimdal** (http://www.h5l.org/) i **krb5** (http://web.mit.edu/kerberos/). Als exemples fem servir krb5, però és vàlida qualsevol llibreria que implementi Kerberos v5. Tal com es mostra, krb5 es pot instal·lar fàcilment a Debian fent servir la seqüència següent:

```
# apt-get install krb5-config krb5-clients krb5-user
```

Aquestes llibreries es poden configurar a través del fitxer `/etc/krb5.conf`. En el cas que ens ocupa cal indicar, com a mínim:

1. **El regne Kerberos**: típicament coincideix amb el nom del domini, i s'especifica a la variable *default_realm*. És imprescindible que s'escrigui en majúscules.
2. **Adreces dels centres de distribució de claus Kerberos**: cal identificar quina o quines màquines dins del regne actuen com a centres de distribució de claus (KDC) Kerberos. Per esbrinar-ho de manera automàtica podem posar la variable *dns_lookup_kdc* a *true*.

```
[libdefaults]
default_realm = NOM_DOMINI.COM
dns_lookup_kdc = true
```

Per verificar que hem fet la configuració correctament, hem de poder connectar-nos fent servir l'eina `kinit` amb un nom d'usuari del domini.

```
# kinit alumne
Password for alumne@NOM_DOMINI.COM:
```

Si tot ha funcionat correctament, s'hauria d'haver obtingut un tiquet Kerberos. Aquest es pot consultar fent servir `klist`.

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: alumne@NOM_DOMINI.COM
```

```
4
5 Valid starting Expires Service principal
6 12/05/11 17:32:18 12/06/11 03:32:19 krbtgt/NOM_DOMINI.COM@NOM_DOMINI.COM
7 renew until 12/06/11 17:32:18
```

Finalment cal modificar el fitxer `smb.conf` de forma similar a com queda amb el mode *domain*, però indicant el regne Kerberos a la variable *realm*.

```
1 [global]
2      ...
3      security = ads
4      encrypt passwords = yes
5      workgroup = NOM_DOMINI
6      realm = NOM_DOMINI.com
7      ...
```

A continuació podeu unir la màquina al domini fent servir l'ordre `net`.

```
1 # net ads join -U alumne
2 Enter alume's password:
3 Using short domain name -- NOM_DOMINI
4 Joined 'DEBIAN' to realm 'NOM_DOMINI.com'
```

Tanmateix, no heu d'oblidar que encara que Samba estigui connectat a un domini, internament Linux assigna permisos basant-se en els usuaris locals de `/etc/passwd`. Per això, en aquesta situació cal també un mecanisme que tradueixi els noms del domini a noms locals.

Així, doncs, encara que el controlador de domini hagi autenticat correctament un usuari que vol accedir als recursos del vostre servidor, cal que Samba sàpiga quin usuari local representa. D'altra manera no tindrà permisos per accedir-hi. Per vincular usuaris del domini a usuaris locals podeu fer servir un dels mecanismes següents:

1. Crear tots els usuaris del domini localment i definir el paràmetre *username map* al fitxer de configuració.
2. De forma totalment transparent utilitzant el dimoni winbind.

winbind

winbind actua com a intermediari entre un controlador de domini Windows i el servei d'autenticació local de Linux. D'aquesta manera, es pot fer que els usuaris del domini siguin també usuaris de Linux.

Podeu trobar força informació al respecte a les pàgines oficials de documentació de Samba.

Quan Samba forma part d'un domini, cal fer servir un procés de traducció d'usuaris del domini a usuaris locals. Aquest procés es pot dur a terme mitjançant *id mapping* o el procés winbind.

Com teniu resumit a la taula 1.2, l'ús del mode de seguretat dependrà de la situació.

TAULA 1.2. Ús dels diferents modes de seguretat en diferents escenaris

	security = user	**security = domain**	**security = ads**
Samba com a servidor independent (xarxa d'igual a igual)	Sí	No	No
Samba com a membre d'un domini NT	No	Sí	No

TAULA 1.2 (continuació)

	security = user	**security = domain**	**security = ads**
Samba com a membre d'un domini d'Active Directory	No	Sí, sempre que Windows Server accepti autenticació via NTLM (mode mixt)	Sí

1.2.4 Backends

Tradicionalment, el sistema GNU/Linux emmagatzema la informació dels comptes d'usuari, de les contrasenyes i dels grups als fitxers `/etc/passwd`, `/etc/shadow` i `/etc/group`, respectivament. De manera anàloga, els sistemes Windows ho fan dins de la base de dades **SAM**, un fitxer que podem trobar dins del directori `\windows\system32\config`. Considerem que aquests fitxers contenen la base de dades d'usuaris del sistema. D'aquesta manera, quan un usuari local s'autentica en el sistema es consulten aquests arxius i es determina si les credencials són correctes o no.

Validació d'usuaris GNU/Linux

Per validar usuaris, GNU/Linux pot fer servir altres mecanismes a més de la consulta al conegut fitxer `/etc/passwd`. Els *pluggable authentication modules* (PAM) són mòduls de software que permeten fer servir altres mecanismes d'autenticació com ara sistemes biomètrics, directoris LDAP, dominis Windows, servidors Kerberos, RADIUS, etc.

De forma similar, el servei Samba implementa un mecanisme d'autenticació d'usuaris per accedir als recursos que ofereix. Així, quan un client vol connectar-se a un recurs compartit per Samba, com ara un directori o una impressora, s'envien les credencials i Samba verifica que l'usuari estigui donat d'alta. Si les credencials rebudes són correctes, es fa el pas següent: determinar si aquest usuari té permisos o no per realitzar l'acció sol·licitada. Es fa evident, doncs, que Samba ha de disposar d'una base de dades pròpia on emmagatzemar els comptes d'usuari. Sovint, a aquesta base de dades se la coneix amb el nom en anglès de ***backend***.

Alguns usuaris, sobretot els acostumats a treballar amb Microsoft Windows, potser es plantejaran la pregunta següent: per quin motiu Samba fa servir una base de dades diferent de la del sistema GNU/Linux? No resultaria més fàcil que els mateixos usuaris del sistema, donats d'alta a `/etc/passwd`, també hi tinguessin accés com a clients Samba? La resposta és que Samba necessita emmagatzemar atributs addicionals per a cada usuari que no es poden trobar a `/etc/passwd`. Exemples d'aquests atributs són: el SID de l'usuari, les contrasenyes xifrades en NT/LM o l'adreça UNC del directori *home* (per citar-ne alguns).

> Per a cada usuari, Samba necessita emmagatzemar atributs addicionals que no pot trobar dins de `/etc/passwd`. És per això que ha de disposar d'una base de dades independent de la del sistema.

Podem especificar el *backend* que Samba farà servir a l'atribut *passdb backend*, dins de la secció `[global]` del fitxer de configuració. De manera nativa, Samba permet utilitzar tres tipus de *backends* diferents:

1. Fitxer de text pla
2. Fitxer TDB

3. Directori LDAP

Tot i això, mitjançant mòduls addicionals podem utilitzar altres *backends* com bases de dades MySQL, PostgreSQL, fitxers XML, etcètera. A continuació es detallen les característiques dels tres *backends* utilitzats per Samba.

Fitxer de text pla

És el mètode més simple. Les dades dels usuaris queden registrades en un fitxer de text, normalment a `/etc/samba/smbpasswd`. Aquest fitxer el podem visualitzar amb un editor de text.

```
[global]
     ...
     security = user
     passdb backend = smbpasswd
     encrypt passwords = yes
     ...
```

La ubicació del fitxer es pot definir manualment:

```
passdb backend = smbpasswd:/ubicacio/fitxer/smbpasswd
```

El fitxer `smbpasswd` conté una línia per a cada usuari Samba, i a cadascuna d'aquestes, els seus atributs separats per dos punts ":".

```
usuari:uid:hash_1:hash_2:flags:darrera_modificació
```

On:

1. *usuari*: és el nom d'usuari que faran servir els clients per connectar-se als recursos.
2. *uid*: l'UID del compte d'usuari al sistema.
3. *hash_1*: *hash* de la contrasenya de tipus LanMan (LM).
4. *hash_2*: *hash* de la contrasenya de tipus NT/LM.
5. *flags*: diversos caràcters que representen el tipus i l'estat del compte.
6. *darrera_modificació*: mostra quan va ser l'última vegada que es va canviar la contrasenya (LCT o *last change time*), en format hexadecimal.

```
# cat /etc/samba/smbpasswd
usuari:1000:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:7CE21F17C0AEE7FB9CEBA532D0546AD6:[
    U ]:LCT-4EBA44DE:
lluis:1001:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:7CE21F17C0AEE7FB9CEBA532D0546AD6:[U
     ]:LCT-4EBA6D0C:
manel:1003:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:588FEB889288FB953B5F094D47D1565C:[U
     ]:LCT-4EBA6D15:
marta:1005:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:05B073DAA9C1B3B909FF5AE2E4604BB5:[U
     ]:LCT-4EBA6D1C:
silvia:1004:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:DF54DE3F3438343202C1DD523D0265BE:[
    U ]:LCT-4EBA6D22:
pep:1002:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:37D02806094AD4CE5AEDD139D9943BED:[U
    ]:LCT-4EBA6D39:
```

Hash

Les contrasenyes dels usuaris no s'emmagatzemen mai de manera llegible, sinó que s'hi aplica un mecanisme de xifrat per evitar que ningú, ni tan sols l'administrador, les pugui llegir. Al resultat d'aplicar un mecanisme de xifrat a una contrasenya se'l coneix com a hash.

Al llarg de la seva història, Windows, i de retruc Samba, ha fet servir dos mecanismes de xifrat per emmagatzemar les contrasenyes dels seus usuaris, LM i NT/LM. El primer, LM, ha quedat en desús per problemes de debilitat. NT/LM corregeix algunes d'aquestes debilitats i és el mètode utilitzat en les darreres versions. Windows XP utilitza els dos mecanismes alhora (per compatibilitat amb versions anteriors), però a partir de Windows Vista el mecanisme de xifrat per defecte és NT/LM.

Actualment, Samba tampoc fa servir el mecanisme LM. És per això que als backends hi podem observar una filera de X on hi hauria d'haver el hash LM.

L'ús del *backend* smbpasswd és ideal per a escenaris simples amb pocs usuaris, però no és recomanable quan el nombre d'usuaris és elevat. La raó és que no es pot accedir al fitxer de manera concurrent, és a dir que quan diversos clients volen autenticar-se a la vegada, Samba atendrà les peticions de manera seqüencial, una darrera de l'altra, de manera que pot provocar un coll d'ampolla a la xarxa. Un altre inconvenient és que no hi ha lloc per a atributs addicionals com ara la data d'expiració de la contrasenya o l'adreça UNC del directori home (necessària per aplicar perfils d'usuari).

Fitxer TDB

El *backend* TDB (*trivial database*) o `tdbsam` utilitza un fitxer binari per emmagatzemar les dades dels usuaris. Com a tal, no es pot manipular ni visualitzar amb un editor de text, sinó que hem d'utilitzar les eines que proporciona el paquet de Samba.

```
[global]
     ...
     security = user
     passdb backend = tdbsam
     encrypt passwords = yes
     ...
```

Per defecte, aquest fitxer està situat en un fitxer anomenat `passdb.tdb` al directori `/var/lib/samba/`, tot i que sempre dependrà de la distribució que estem utilitzant. La ubicació del fitxer es pot definir manualment:

```
passdb backend = tdbsam:/ubicacio/fitxer/passdb.tdb
```

Té alguns avantatges respecte al *backend* `smbpasswd`: disposa de **més atributs per usuari** i permet l'**accés concurrent** al fitxer, fet que millora el rendiment en cas de múltiples peticions d'autenticació. La part negativa és que **no es pot fer servir** en un escenari amb múltiples controladors de domini. El motiu és que quan hi ha diversos controladors de domini es necessita algun mètode de replicació del *backend*. Segons els desenvolupadors de Samba, aquesta configuració és la recomanada sempre i quan el nombre d'usuaris no sigui superior a 250. Aquest *backend* el trobem seleccionat per defecte en la majoria de distribucions de GNU/Linux, com ara Ubuntu, Debian o Fedora.

El *backend* `tdbsam` està configurat per defecte a la majoria de distribucions GNU/Linux actuals, com ara Ubuntu, Debian o Fedora.

Directori LDAP

El *backend* `ldapsam` ens permet utilitzar un servei de directori LDAP per emmagatzemar els comptes d'usuari Samba. LDAP ens permet mantenir una base de dades d'usuaris centralitzada i accessible per qualsevol controlador de domini. Per configurar-lo només cal indicar la URL del servei LDAP dins del fitxer de configuració, tal com mostra l'exemple.

```
[global]
     ...
     security = user
     passdb backend = ldapsam:ldap://servidor/
     ...
```

Per utilitzar un directori LDAP com a *backend* no n'hi ha prou d'instal·lar i iniciar el servei de directori, sinó que prèviament cal preparar-lo. A grans trets, preparar el directori vol dir:

1. Carregar els esquemes propis de Samba al directori LDAP: és necessari que els elements del directori, com ara usuaris o grups tinguin els atributs específics de Samba.
2. Configurar Samba per fer servir el directori: cal que Samba sàpiga on trobar els elements dins del directori. Recordeu que el directori pot emmagatzemar moltes més dades.

Hi ha situacions en les quals és convenient disposar de més d'una còpia del servidor LDAP. D'aquesta manera ens assegurem que en cas de fallida d'un d'ells hi pugui haver una alternativa. En aquest cas es poden indicar les adreces de tots els servidors en el fitxer de configuració:

```
passdb backend = ldapsam":ldap://servidor1/ ldap://servidor2/ ldap://servidor3
    "/
```

Un altre avantatge de tenir més d'un servidor LDAP configurat és que Samba realitza, de manera automàtica, **distribució de càrrega**. Així s'evita que totes les peticions d'autenticació es redirigeixin a un mateix servidor LDAP.

En resum, veiem que cada *backend* té els seus avantatges i inconvenients; la decisió sobre quin escollir depèn de la situació. La taula 1.3 mostra en quines situacions es poden utilitzar aquests *backends*.

Taula 1.3. Ús dels backends en diferents escenaris

	smbpasswd	**tdbsam**	**ldapsam**
Samba com a servidor independent	Sí	Sí	Sí

Taula 1.3 (continuació)

	smbpasswd	**tdbsam**	**ldapsam**
Samba com a controlador de domini (PDC)	No	Sí	Sí
Múltiples controladors de domini (PDC i BDC)	No	No	Sí

2. Configuració i utilització de xarxes heterogènies

En el món empresarial, Samba és un bon aliat dels administradors de sistemes quan es disposa d'una xarxa amb diversos sistemes operatius. Com veureu tot seguit, es pot integrar d'una manera senzilla en xarxes heterogènies, però hem de ser conscients de les seves limitacions.

En aquest context us podeu pot trobar situacions molt diferents i Samba disposa d'un nivell de configuració molt elevat que permet obtenir una bona adaptació a moltes d'aquestes situacions. Fer un recull de totes les possibilitats de configuració resultaria massa extens, però tractarem d'analitzar les dues situacions més comunes que us podeu trobar:

1. Samba com a servidor independent en un grup de treball
2. Samba com a servidor de domini

A continuació veureu com configurar i administrar Samba en cadascuna d'aquestes situacions.

2.1 El servidor Samba en un grup de treball

El servei Samba permet configurar un servidor basat en Linux per tal d'integrar-lo dins d'un grup de treball Windows, de manera que pugui compartir recursos com un equip més del conjunt lògic de la xarxa. Un dels requisits imprescindibles és que aquest servidor es comporti exactament igual que un sistema Windows. Per això, cal ajustar els paràmetres de configuració de Samba tal com es detallen a continuació:

1. **Nivell de seguretat**: el nivell de seguretat determinarà la manera com els usuaris s'identifiquen. El nivell adequat a una xarxa igualitària on intervenen ordinadors Windows és el nivell `user`. Les opcions restants no són adients o bé són caduques.
2. ***Backend***: el tipus de *backend* que fem servir determina de quina manera s'emmagatzemen els usuaris. En aquest cas, l'opció més recomanable és fer servir un arxiu local, de tipus `smbpasswd` o `tdbsam`.
3. **Grup de treball:** el nom del grup de treball (workgroup).
4. **Nom de l'equip:** també conegut com el *nom NetBIOS*. Determina quin nom tindrà aquest equip quan s'explori la xarxa.

5. ***Master browser*(opcional)**: el *master browser* és l'equip que conté la llista de tots els equips connectats a la xarxa.

Per establir aquesta configuració cal modificar l'arxiu `/etc/samba/smb.conf`. Com podreu observar, en aquest arxiu trobareu centenars de paràmetres que poden donar lloc a milers de configuracions diferents.

Tot i que l'arxiu de configuració `smb.conf` és molt extens, per començar heu de realitzar molts pocs canvis respecte a l'arxiu original que s'incorpora amb el paquet.

L'arxiu es divideix en seccions identificades per un nom entre claus, `[·]`. Hi ha tres seccions especials: `[global]`, `[homes]` i `[printers]`. La secció principal s'identifica amb `[global]` i ens permet configurar els paràmetres generals del servei. La secció `[homes]` ens permet compartir els directoris d'inici (*home*) de cada usuari per tal que cada usuari pugui accedir al seu directori a través de la xarxa. La secció `[printers]` permet compartir impressores.

Dins de l'apartat `[global]` s'ha d'especificar el nom del **grup de treball**, el nom de la màquina, el **nivell de seguretat** i el tipus de ***backend*** desitjat.

```
[global]
     workgroup = IOC
     netbios name = Debian-Samba
     security = user
     passdb backend = tdbsam
     encrypt passwords = yes
```

Com veieu, la configuració és simple: el nom amb el que s'anuncia aquesta màquina és Debian-Samba, i s'inclourà al grup de treball anomenat *IOC*. El paràmetre *security* determina el nivell de seguretat i el *backend* s'emmagatzemarà en una base de dades de tipus TDB.

Amb aquesta configuració ja en tindríem prou per incorporar el servidor al grup de treball. Per assegurar-nos que les modificacions del fitxer `smb.conf` es duen a terme, és convenient reiniciar el servei.

```
# service samba restart
Stopping Samba daemons: nmbd smbd.
Starting Samba daemons: nmbd smbd.
```

2.1.1 Usuaris

Samba inclou un conjunt d'eines per manipular els comptes d'usuari emmagatzemats al *backend*. Aquestes eines s'han dissenyat de manera que funcionin igual independentment del tipus de *backend* que feu servir: fitxer TDB, fitxer smbpasswd o directori LDAP. Les eines que es fan servir per manipular usuaris Samba són, principalment, les ordres `smbpasswd` i `pdbedit`.

Per afegir usuaris a Samba farem servir l'ordre `smbpasswd`, tal com mostra l'exemple següent:

```
# smbpasswd -a usuari
New SMB password:
Retype new SMB password:
```

La parella usuari/contrasenya que introduïm aquí és aquella amb la qual s'accedirà des dels clients Windows. Podeu fer servir `smbpasswd` tantes vegades com usuaris vulgueu crear.

L'ordre `smbpasswd` es comporta de dues maneres diferenciades:

1. Si l'executa l'usuari *root*, ens permet administrar els usuaris Samba: crear, esborrar, llistar, habilitar/deshabilitar i canviar la contrasenya.
2. Si l'executa qualsevol altre usuari, li permet canviar la contrasenya Samba en servidors remots.

Les opcions més comuns d'aquesta eina es mostren a la taula 2.1.

Taula 2.1. Rols que pot prendre Samba

Opció	Descripció
`-a nom_usuari`	Afegeix un usuari.
`-d nom_usuari`	Deshabilita el compte d'usuari.
`-e nom_usuari`	Habilita el compte d'usuari.
`-n nom_usuari`	Aplica una contrasenya buida a l'usuari.
`-x nom_usuari`	Esborra el compte d'usuari.
`-h`	Mostra l'ajuda.

Tot i que l'eina *pdbedit* també es pot fer servir per realitzar les mateixes accions, normalment s'utilitza per a tasques administratives de baix nivell, com ara canviar les propietats d'un usuari o importar i exportar usuaris del *backend*.

D'altra banda, Samba necessita que tots els usuaris que accedeixen als recursos es puguin **vincular a un usuari del sistema Linux** (UID). Per aquest motiu, cal que abans d'afegir un usuari Samba el donem d'alta com a usuari del sistema.

```
# useradd usuari
# passwd usuari
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
```

Aquest requisit també s'aplica als **usuaris convidats** i per tant, s'han de vincular a un compte específic de GNU/Linux. En general, quan Samba rep la petició d'un usuari que no s'ha pogut autenticar correctament, com en el cas de no trobar l'usuari al *backend*, la petició es rebutja per defecte i no s'atorga l'accés. De vegades, però, ens interessarà que un usuari sense registrar pugui accedir als recursos compartits, com, per exemple, en el cas d'una empresa amb molts

treballadors pot resultar útil que tothom tingui accés a un directori públic sense haver de donar d'alta tots els treballadors. En aquests casos és necessari **permetre l'accés a usuaris no registrats** i **habilitar l'accés de convidat**.

Si es desitja que els usuaris puguin entrar sense estar registrats, el primer que heu de fer és canviar el comportament que Samba té per defecte quan troba un usuari que no és al *backend*. Això es realitza indicant el paràmetre i valor `map to guest = bad user` dins de la secció `[global]`. D'aquesta manera li indiqueu que si no es troba l'usuari al *backend* es faci servir el compte de convidat.

Finalment, cal indicar quin usuari del sistema GNU/Linux es farà servir per vincular els usuaris invitats. Amb el paràmetre `guest account` determineu quin compte d'usuari GNU/Linux es fa servir com a convidat.

```
[global]
     workgroup = IOC
     netbios name = Debian_Samba
     security = user
     passdb backend = tdbsam
     encrypt passwords = yes
     map to guest = bad user
     guest account = invitat
```

Evidentment, el compte de convidat ha d'estar creat prèviament a Linux.

```
# useradd invitat
```

2.1.2 Recursos compartits

Els recursos compartits es defineixen afegint seccions al fitxer de configuració de Samba. Recordeu que el començament de cada secció s'indica amb un nom entre claus, `[·]`, i a continuació s'afegeix la informació relativa a un recurs compartit. Hi ha seccions especials amb noms reservats que no podem utilitzar perquè tenen un significat especial: `[global]`, `[printers]` i `[home]`.

Entre claus s'indica el nom del recurs compartit, que és aquell que veuran els clients quan hi vulguin accedir. Posteriorment, a la variable `path`, indiquem la ruta local al directori compartit.

```
[recurs_compartit]
     path = /directori
```

És indispensable que el directori existeixi prèviament dins del sistema de fitxers original.

```
# mkdir /directori
```

Aquesta configuració és la mínima necessària per compartir un recurs, però cal saber que **per defecte el recurs es compartirà amb permisos només de lectura**.

Tot i això, quan compartiu recursos amb Samba en una xarxa on s'integren sistemes operatius Windows i Linux, hi ha un seguit de **diferències que hem de tenir en consideració**. Principalment, es tracta de diferències directament relacionades amb els sistemes de fitxers.

Com sabeu, Windows i Linux disposen dels seus propis sistemes de fitxers. En el cas de Windows són FAT32 i NTFS, mentre que per a Linux els més comuns són ext2, ext3, ext4 i reiserFS. Cada sistema de fitxers té les seves característiques i limitacions. Entre aquestes limitacions trobem:

1. La distinció entre majúscules i minúscules
2. Els caràcters prohibits en els noms
3. Els accessos directes a Windows o *soft-links* i *hard-links* a Linux

Samba s'encarrega de solucionar les diferències entre sistemes de fitxers Windows i Linux.

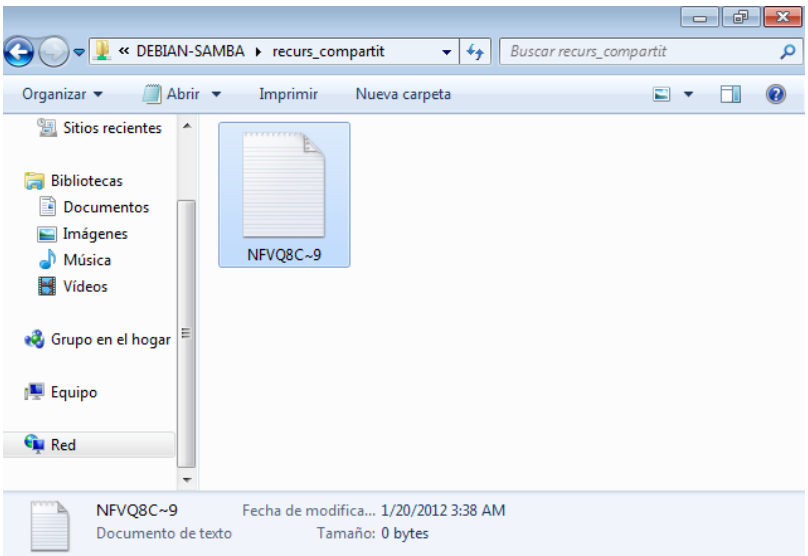
Per exemple, els noms dels fitxers en Windows no distingeixen entre majúscules i minúscules, de manera que els directoris anomenats *escriptori* i *ESCRIPTORI* són el mateix. Per això un directori no pot contenir un arxiu *document.txt* i a la vegada un *DOCUMENT.txt*. En canvi, si fem servir els sistemes de fitxers Linux sí que és possible. Com sabeu, a GNU/Linux se sol distingir majúscules i minúscules.

El sistema operatiu Windows no permet que els noms dels fitxers o directoris continguin els caràcters \/:*?"<>|, però en canvi, a Linux sí que podem crear fitxers amb els caràcters :*?"<>|. Llavors, què ocorre quan un servidor Samba comparteix algun fitxer amb un d'aquests caràcters prohibits per Windows? En aquests casos, el servidor realitza un procés de transformació anomenat *mangle* i mostra al client un nom modificat, no l'original. Aquest nom es representa en format 8.3.

Format 8.3

Els noms del fitxers amb format 8.3 tenen com a màxim 8 caràcters que indiquen el nom, seguits d'un punt i tres caràcters més que indiquen l'extensió de l'arxiu. Aquest format s'utilitzava a MS-DOS i a les primeres versions de Windows.

FIGURA 2.1. Arxiu compartit per Samba anomenat N*.txt vist des d'un client Windows



Tal com podeu observar en la figura 2.1, el procés de transformació permet que els clients Windows puguin accedir als fitxers amb caràcters prohibits, però amb un nom totalment diferent de l'inicial.

2.1.3 Permisos

L'autorització d'una acció sobre un recurs compartit està determinada pels permisos assignats al servidor. Així, si un usuari vol accedir a un recurs compartit i crear-hi fitxers haurà de tenir permisos d'escriptura dins d'aquell directori compartit.

Els recursos compartits per Samba estan afectats per dos tipus de permisos totalment independents:

1. Els permisos del sistema de fitxers
2. Els permisos Samba, també anomenats *permisos de xarxa*

Quan un client desitja realitzar una acció determinada (llegir o escriure), cal que tingui els permisos adequats tant al sistema de fitxers com al recurs compartit. No serveix de res que un usuari tingui tots els permisos a Samba si després no en té cap al sistema de fitxers. Per tant, sempre s'aplica el permís més restrictiu. Tenir això sempre present us estalviarà molts mal de caps.

> Els permisos sobre un recurs compartit depenen del sistema de fitxers i de Samba. En cas d'existir permisos oposats sempre s'aplicarà el més restrictiu dels dos.

Els **permisos del sistema de fitxers** o permisos locals es representen mitjançant 9 bits (`rwxrwxrwx`) amb els quals els sistemes Unix implementen el control d'accés als fitxers del sistema i que podem modificar amb l'ordre *chmod*.

El significat dels permisos varia depenent de si es tracta d'un fitxer o d'un directori, tal com mostra la taula 2.2.

TAULA 2.2. Permisos tradicionals Unix

Permís	Arxiu	Directori
`r`	Llegir arxius	Veure el contingut del directori
`w`	Gravar en un arxiu	Crear i esborrar arxius dins del directori
`x`	Executar com a programa	Entrar al directori
`-`	Sense permís	Sense permís

Convé recordar que en directoris, a més dels tres permisos mostrats, també podem assignar el permís de l'*sticky bit*. L'*sticky bit* permet que només els propietaris dels arxius puguin reanomenar o esborrar els seus arxius encara que la resta d'usuaris

tingui permisos d'escriptura en aquell directori. Les opcions *+t* i *-t* de l'ordre *chmod* permeten afegir o treure l'*sticky bit*.

```
# chmod +t directori
```

Els **permisos Samba** s'especifiquen en el fitxer de configuració, dins de cadascuna de les seccions on hi hagi un recurs compartit. Les variables que controlen els permisos s'indiquen a la taula 2.3. Per defecte, un recurs compartit té permisos només de lectura per a tots els usuaris del *backend*.

Taula 2.3. Variables que controlen els permisos dels recursos compartits

Variable	Definició
`admin users`	Llista d'usuaris amb control total sobre el recurs compartit.
`read list`	Llista d'usuaris que tenen accés de només lectura.
`write list`	Llista d'usuaris que tenen accés de lectura i escriptura.
`guest ok`	Permetre l'accés com a convidat al recurs.
`invalid users`	Llista d'usuaris als quals no se'ls permet accedir.
`valid users`	Llista d'usuaris que sí que hi poden entrar. Si la variable no s'especifica, tots els usuaris amb compte al *backend* hi poden accedir.
`read only`	Indica que el recurs només és de lectura.

Per exemple, la variable *read only = no* permet que els usuaris puguin llegir i escriure (sempre que també ho facin els permisos del sistema de fitxers).

```
[recurs_compartit]
     path=/directori
     read only = no
```

També podem indicar la llista d'usuaris als quals restringim l'accés amb la variable *invalid users*.

```
[recurs_compartit]
     path=/directori
     read only = no
     invalid users = alumne1, alumne2, @professors
```

Llistes d'usuaris i grups

Als permisos de Samba hi podeu indicar una llista d'usuaris amb els noms separats per comes. Els grups es mostren amb el símbol @ al davant.

Quan desitgem que els usuaris **convidats** tinguin accés a un recurs en concret, cal assignar la variable *guest ok* a *yes*. En cas contrari sempre es demanarà l'autenticació de l'usuari.

```
[public]
     path = /directori_public
     guest ok = yes
```

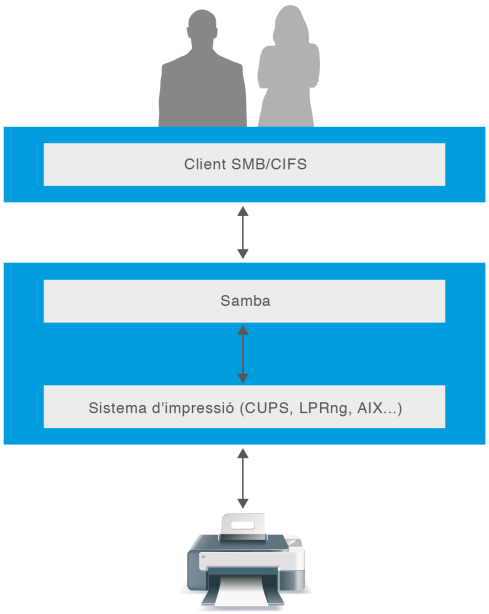
2.1.4 Impressores

Quan pensem en Samba normalment ens ve al cap la funció de compartir directoris, i de fet, aquest és l'ús principal que se li dóna. Però Samba també es pot fer servir com a servidor central d'impressores en una xarxa amb clients Windows. En aquest apartat veurem com configurar el servei per compartir impressores.

Cal dir, però, que **Samba no és un sistema d'impressió per se**, sinó que **actua com a intermediari entre les peticions dels clients iel sistema d'impressió del sistema operatiu** (figura 2.2). Això significa que Samba no es comunica directament amb les impressores, simplement executa les ordres del sistema necessàries per imprimir treballs, posar-los en pausa, cancel·lar-los, veure els treballs en cua, etcètera. En definitiva, Samba es comporta de la mateixa manera que ho faria un usuari de l'equip que vol imprimir.

> Samba no és un sistema d'impressió, sinó que actua com a intermediari entre els clients i el sistema d'impressió del sistema operatiu.

FIGURA 2.2. Esquema d'impressió del servei Samba



CUPS

CUPS (common Unix printing system) és el sistema d'impressió que per defecte es fa servir en moltes distribucions GNU/Linux actuals, entre elles Debian i Ubuntu.

Samba permet la comunicació amb diversos tipus de sistemes d'impressió Unix, entre els quals destaquem HPUX, BSD, PLP, LPRng, i el més utilitzat, **CUPS**.

Vist això, podeu suposar que **el pas previ a compartir una impressora amb Samba és tenir-la correctament configurada en el sistema d'impressió**. En el vostre cas suposarem que feu servir CUPS, i aquest es pot administrar de diverses maneres:

1. Des de les eines gràfiques que proporciona l'escriptori de Debian, fent clic a *Sistema* > *Administració* > *Impressió.*

2. Des del lloc web d'administració de CUPS: http://localhost:631/.

3. Directament des de l'arxiu de configuració a `/etc/cups/cups.conf`.

És convenient assegurar-nos que el servei CUPS està funcionant correctament.

```
# ps –A | grep cupsd
1097 ? 00:00:01 cupsd
```

Per afegir una impressora de manera senzilla podeu visitar el web http://localhost:631/, clicar a la pestanya d'*Administració* i a continuació al botó d'*Afegir impressora*. CUPS necessita que introduïu el nom i la contrasenya de l'administrador (*root*) de la màquina.

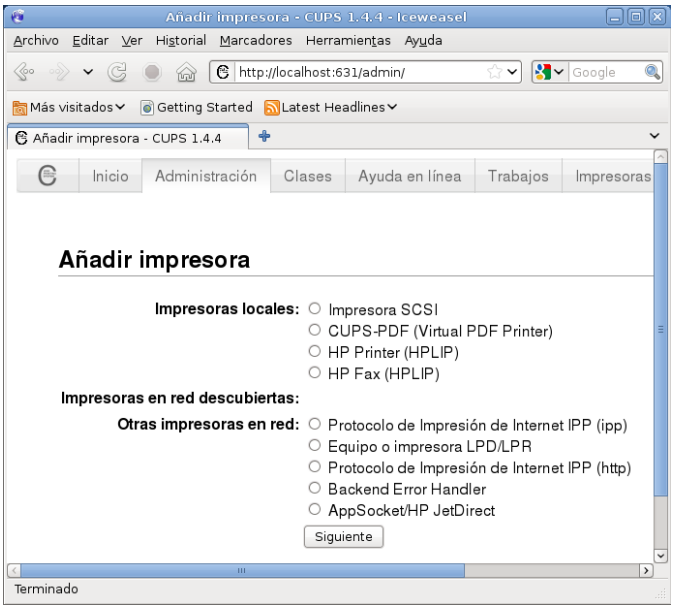
Posteriorment, i com mostra la figura 2.3, cal indicar-li on està connectada la impressora i quin protocol fa servir, el que es coneix com a *backend*. La majoria d'impressores per a entorns empresarials actuals permeten fer servir els protocols IPP, LPD/LPR o JetDirect (AppSocket).

En clicar a *Següent* us demanarà la marca i el model, el nom i la resta d'opcions. Si no és a la llista també podeu afegir un controlador específic amb extensió PPD.

Controladors (drivers) CUPS

Els controladors d'impressores per CUPS són arxius amb extensió `.ppd`. Actualment, la majoria de fabricants disposa de controladors per a Linux.

FIGURA 2.3. Aplicatiu web d'administració de CUPS



És recomanable que l'alumne revisi el funcionament dels serveis d'impressió a GNU/Linux.

Un cop heu afegit la impressora al sistema, heu d'indicar-li a Samba quin servei d'impressió fareu servir, en el nostre cas CUPS.

```
[global]
     workgroup = IOC
     netbios name = Servidor–debian
     security = user
     printing = cups
     printcap name = cups
```

Finalment, cal que afegiu la definició de la impressora compartida de manera similar a com ho faríeu amb un directori, amb les diferències següents:

1. El nom del recurs compartit ha de coincidir amb el nom de la impressora en el servei d'impressió de Linux. Així, si heu posat el nom *HP_1102W* a la impressora a CUPS, caldrà que el recurs a Samba s'anomeni igual.

2. Cal afegir la variable *print ok = yes* al recurs compartit per indicar que aquest recurs és una impressora.

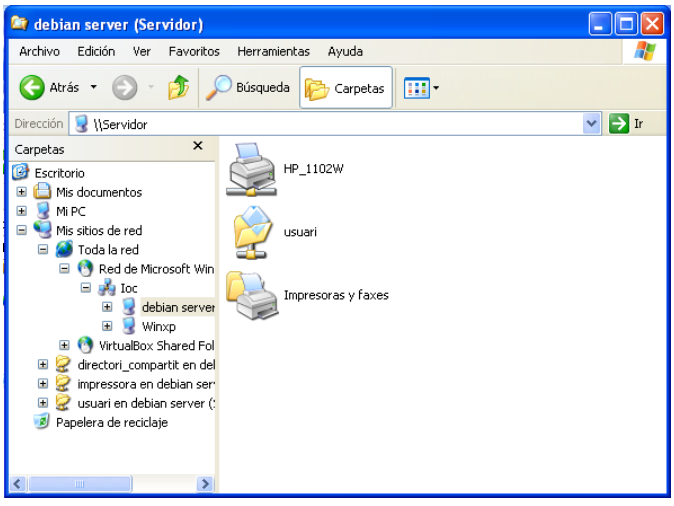
3. La variable *path* ha d'indicar el directori on s'emmagatzemen els treballs que seran impresos. És obligat que el directori indicat tingui permisos d'escriptura per a tothom que pugui imprimir, altrament els clients tindran un error en imprimir. Podem fer servir el directori `/var/spool/samba`, que ja està preparat amb el paquet Samba.

4. Típicament, els controladors d'impressió de Windows envien les dades a la impressora de manera que no és necessari cap filtre de processat, al contrari dels sistemes Linux que envien les dades en PostScript. Si no és necessari cap processat afegiu el paràmetre *cups options = "raw"*.

```
[HP_1102W]
     print ok = yes
     path = /var/spool/samba
     cups options = ""raw
```

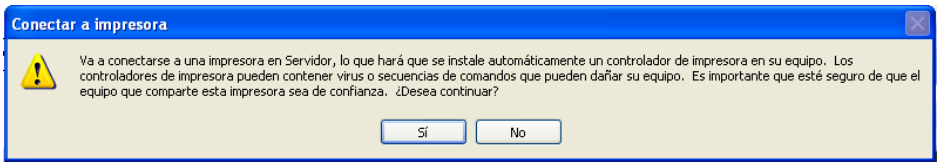
Aquesta és la configuració mínima imprescindible per tenir accessible la impressora des dels clients amb Windows, tal com podeu observar a la figura 2.4.

FIGURA 2.4. Impressora accessible des de clients Windows



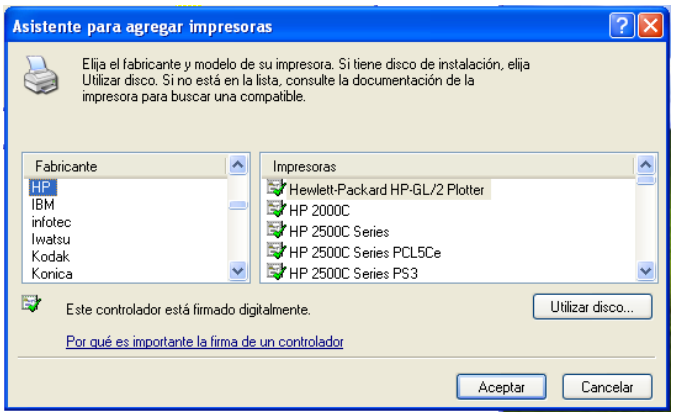
En fer doble clic en la impressora us avisarà que s'intentaran instal·lar els controladors de manera automàtica (figura 2.5).

FIGURA 2.5. Avís d'instal·lació de controladors



Com que no hem proporcionat cap controlador caldrà afegir-lo manualment (figura 2.6).

FIGURA 2.6. Addició manual del controlador



Com veieu, compartir una impressora és una tasca molt senzilla, però es pot millorar per facilitar les tasques l'administració. En primer lloc, podem fer que **Samba detecti automàticament les impressores connectades al sistema d'impressió** i les comparteixi. D'aquesta manera no cal afegir-les una a una. Per fer-ho només cal incloure el recurs compartit especial `[printers]` amb els mateixos paràmetres que una impressora.

```
[printers]
     path = /var/spool/samba
     print ok = yes
```

Aquesta petita modificació pot alliberar la càrrega de l'administrador quan hi hagi moltes impressores connectades a la màquina, com en el cas d'un servidor d'impressió d'una oficina. En segon lloc, podem facilitar la tasca d'instal·lació de les impressores als clients si permetem la **descàrrega i instal·lació automàtica de controladors**, és el que es coneix com a *Apuntar i imprimir*.

> *Apuntar i imprimir* (*Point and print*) és una característica dels dominis Windows que permet a un usuari utilitzar les impressores de xarxa fent clic sobre les seves icones.

Per habilitar aquesta característica, cal que al directori `/var/lib/samba/printers` hi hagi els controladors d'impressió que es poden descarregar els usuaris, separats segons l'arquitectura de la màquina client.

```
# ls -l /var/lib/samba/printers/
total 32
```

```
drwxr-xr-x 2 root root 4096 ene 8 16:56 COLOR
drwxr-xr-x 2 root root 4096 ene 8 16:56 IA64
drwxr-xr-x 2 root root 4096 ene 8 16:56 W32ALPHA
drwxr-xr-x 2 root root 4096 ene 8 16:56 W32MIPS
drwxr-xr-x 2 root root 4096 ene 8 16:56 W32PPC
drwxr-xr-x 2 root root 4096 ene 8 16:56 W32X86
drwxr-xr-x 2 root root 4096 ene 8 16:56 WIN40
drwxr-xr-x 2 root root 4096 ene 8 16:56 x64
```

Així, per exemple, caldrà afegir els controladors per a les màquines amb Windows XP, Vista o 7 de 32 bits dins del directori `W32X86`, els controladors per a les versions del sistema Windows de 64 bits s'hauran d'emmagatzemar dins de `x64`, i així successivament.

Aquest directori cal compartir-lo amb el nom de `[print$]`, que és el recurs on les màquines en un grup de treball Windows cerquen els controladors de les impressores. Llevat dels administradors, és important que tothom tingui accés de només lectura a aquest recurs.

```
[print$]
     path = /var/lib/samba/printers
     browseable = yes
     read only = yes
     guest ok = no
     write list = root
```

Hi ha d'haver al menys un usuari que pugui carregar els controladors en aquests directoris. Com veieu, en l'exemple assignem permisos d'escriptura a l'usuari *root*, però també podríem assignar-los a un altre usuari o grup si fos necessari, sempre i quan hi assignem els permisos d'escriptura al directori `/var/lib/samba/printers`.

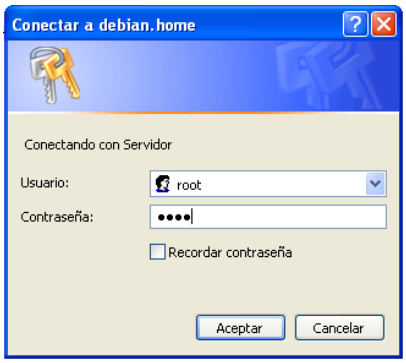
Finalment, cal donar el dret `SePrintOperatorPrivilege` a l'usuari que pugui afegir controladors.

```
# net -U root%contrasenya rpc rights grant root \ SePrintOperatorPrivilege
```

Consulteu l'apartat "Drets" per a més informació sobre com administrar els drets dels usuaris de Samba.

L'usuari *root* ja pot afegir al servidor tots els controladors que desitgi. Per fer-ho cal connectar-se al servidor des d'una màquina amb Windows (figura 2.7).

FIGURA 2.7. Connexió des d'una màquina Windows



Posteriorment cal entrar a *Impressores i faxos* (figura 2.8), fer clic amb el botó dret sobre una zona buida i entrar a *Propietats del servidor*. A Windows 7 haureu de fer clic a *Veure impressores remotes*.

Des d'aquesta finestra es poden administrar certs aspectes de les impressores en el servidor Samba de forma remota.

FIGURA 2.8. Impressores i faxos a Windows

Dins de la pestanya*Controladors* podeu veure els controladors que hi ha instal·lats al servidor Samba. Clicant a *Afegir...* podeu afegir, un per un, els controladors que necessitaran els vostres clients. Només cal indicar a quina ubicació es troben, a quina arquitectura pertanyen (figura 2.9 i figura 2.10) i finalment es carregaran automàticament al servidor, com mostra la figura 2.11.

FIGURA 2.9. Selecció del controlador

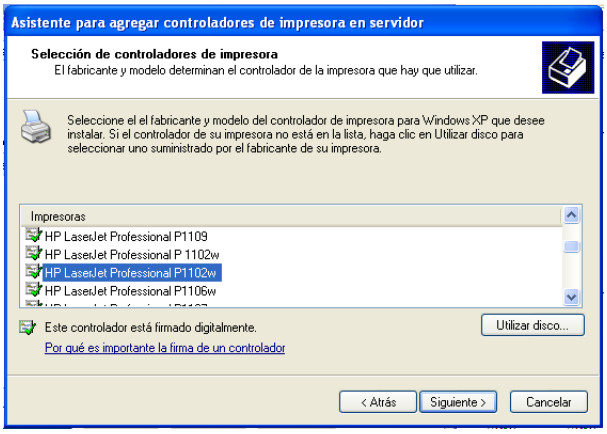


FIGURA 2.10. Selecció del SO de destinació

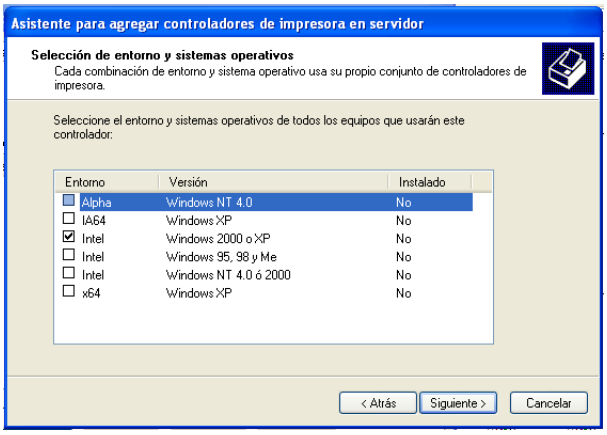
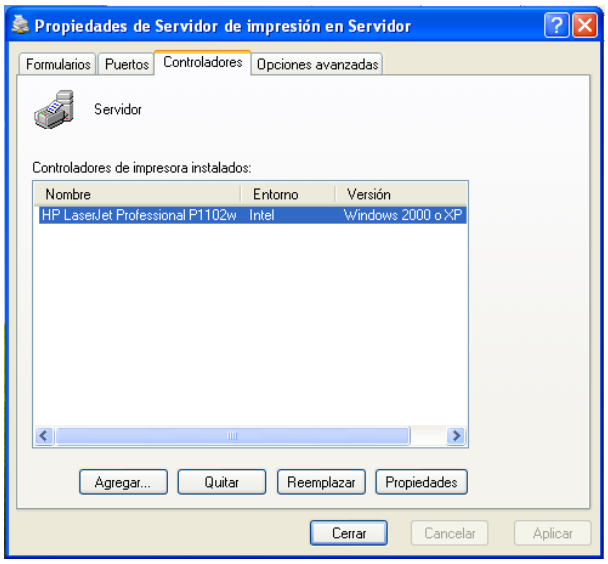


FIGURA 2.11. Controlador instal·lat

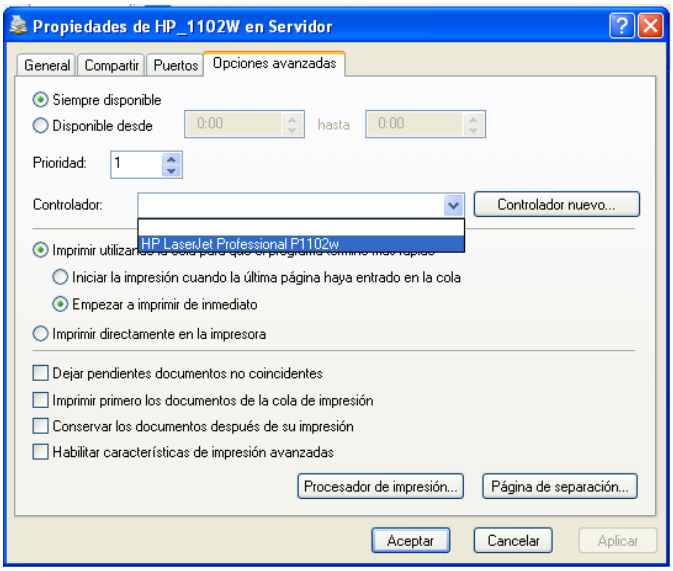


Si en aquest punt observeu el directori compartit de Samba amb els controladors, veureu que han quedat instal·lats a la carpeta corresponent.

```
# ls /var/lib/samba/printers/W32X86/3
AGACCST1.PPD hp1100sd.chm hp1100su.dll hp1600sd.sdd
     PSCRIPT.HLP
HP1100GC.DLL hp1100sd.dll hp1100su.ent PS5UI.DLL
     PSCRIPT.NTF
HP1100PP.DLL hp1100sd.sdd hp1100su.ver PSCRIPT5.DLL
```

Finalment, heu de vincular el controlador que acabeu d'instal·lar a la impressora determinada. Torneu a entra a *Impressores i faxos* (figura 2.8), feu clic amb el botó dret sobre la impressora i aneu a *Propietats*. A continuació, us avisarà que no teniu un controlador assignat i us demanarà si en voleu instal·lar un. Li haureu de dir que **no**, perquè en cas contrari instal·larà un controlador només en l'equip local, i el que voleu és vincular-li un controlador del servidor.

FIGURA 2.12. Selecció del controlador instal·lat



A la finestra que s'obre entreu a *Opcions avançades* i seleccioneu el controlador adient de la llista tal com es mostra a la figura 2.12. Si tot ha anat bé, els clients de la vostra xarxa podran fer servir les impressores simplement fent doble clic sobre elles, sense necessitat que cap tècnic instal·li els controladors ja que es descarreguen de manera automàtica.

Situacions en les quals cal l'ajuda d'un client Windows

Com veieu, en l'administració d'impressores i en altres aspectes de la configuració de Samba cal l'ajuda d'un equip amb el sistema operatiu Windows.

Realment, tota la tasca d'instal·lar els controladors es pot fer manualment des de la màquina amb Samba, però és un procés molt meticulós en el qual qualsevol errada pot provocar errors inesperats que són molt difícils de detectar. En aquest sentit, és recomanable fer servir eines que facilitin la tasca, i per això convé aprofitar les eines que ens ofereix Windows.

2.1.5 Master browser

En un entorn empresarial, els servidors acostumen a ser els equips més potents de la xarxa i els que estan disponibles la major part del temps. En aquest escenari és probable que Samba sigui un dels serveis instal·lats. Llavors, per què no aprofitar la potència d'aquestes màquines i fer que Samba actuï com a *master browser*?

Si Samba s'instal·la en una màquina amb alta disponibilitat i es configura com a *master browser* aprofitarem la potència de la màquina on està instal·lat i podrem evitar part dels problemes de sincronització deguts a la desconnexió sobtada de les màquines de l'entorn de treball.

Vegeu l'apartat "Xarxes igualitàries en entorns Windows" per a una descripció complementària sobre el rol del *master browser*.

En cas contrari podeu córrer el risc que una màquina menys potent, com la d'un treballador, assumeixi aquest rol. Si aquesta màquina no és suficientment potent o està saturada de treball, la resta del grup de treball tindrà problemes de lentitud quan vulgui accedir a la xarxa.

Qualsevol de les màquines d'un grup de treball és susceptible de prendre el rol de *master browser*. Si volem que Samba tingui aquest rol l'hem de **forçar perquè guanyi les eleccions**.

L'algorisme d'elecció està implementat en tots els sistemes Windows, de manera que quan es duu a terme, tots ells estaran d'acord en qui serà el *master* i el *backup browser*. També cal saber que en qualsevol moment es pot forçar el procés d'elecció.

El procés d'elecció es basa en alguns aspectes dels ordinadors, com ara el temps que porten encesos, el sistema operatiu o la versió del protocol que fan servir. L'algorisme de Microsoft determina la jerarquia següent:

1. Controladors de domini Windows NT/2000/2003/2008 (valor 32)

2. Windows NT/2000/2003/2008/Vista/XP/7 (valor 16)

3. Windows 95/98/Me (valor 1)
4. Windows per a grups de treball (valor 1)

El sistema operatiu que tingui un valor més alt en l'escala d'aquesta jerarquia guanya l'elecció. Així, doncs, un controlador de domini de Windows 2003, amb 32 punts, guanyarà l'elecció davant d'una màquina amb Windows 7, amb 16 punts. En cas d'empat entren en joc la resta de variables.

Problemes de seguretat en el procés d'elecció del master browser

El mecanisme utilitzat en el procés d'elecció permet que qualsevol màquina de la xarxa pugui prendre el rol de *master browser*. Això ocasiona un problema de seguretat, ja que d'aquesta manera, una màquina d'un possible atacant podria forçar l'elecció, guanyar-la i fer modificacions en la llista d'equips i suplantar així la identitat d'una de les màquines. A partir d'aquí, l'atacant podria obtenir els noms d'usuari i contrasenyes que envien els clients.

Per defecte, un servidor Samba està configurat per poder actuar com a *master browser* i s'assigna a si mateix un valor 20. Per tant, **en una xarxa igualitària** (sense controladors de dominis) **un ordinador Samba sempre guanyarà l'elecció davant d'equips Windows**. Si, en canvi, hi ha un controlador de domini, la perdrà, ja que aquests tenen assignat el valor 32.

En qualsevol cas, sempre podeu establir el valor des de l'arxiu de configuració amb la variable *os level*, que com a màxim pot prendre el valor 255.

```
1 [global]
2      ...
3      os level = 100
4      ...
```

Si a més es desitja forçar el procés d'elecció cada vegada que s'inicii el servidor Samba, cal posar la variable *preferred master* = *yes*.

```
1 [global]
2      ...
3      os level = 100
4      preferred master = Yes
5      ...
```

La taula 2.4 mostra un resum de les variables implicades en l'elecció del *master browser*.

TAULA 2.4. Variables implicades en el procés d'elecció del master browser.

Variable	Valor	Descripció
`local master`	yes/no	Determina si Samba pot actuar com a *master browser*. Per defecte, ho pot fer.
`os level`	Numèric 0-255	Valor que es tindrà en compte en el procés d'elecció. Com més elevat, més probabilitats té de guanyar-lo.
`preferred master`	yes/no	Si s'estableix a *yes*, es forcen les eleccions quan Samba s'incorpora a la xarxa.

2.1.6 Accés als recursos mitjançant clients GNU/Linux

A Linux un client disposa de diverses maneres d'accedir als recursos compartits en un grup de treball. En qualsevol distribució podeu descarregar-vos el paquet `smbclient` i accedir-hi via ordres.

```
# apt-get install smbclient
```

El paquet `smbclient` conté diverses eines:

```
# dpkg -L smbclient | grep bin
/usr/bin
/usr/bin/smbspool
/usr/bin/rpcclient
/usr/bin/smbtree
/usr/bin/smbcacls
/usr/bin/findsmb
/usr/bin/smbget
/usr/bin/smbcquotas
/usr/bin/smbclient
/usr/bin/smbtar
```

Només veureu algunes de les opcions més significatives, ja que explicar la funció de totes elles ocuparia molt temps, i en cas necessari totes disposen de pàgines al manual que podeu consultar escrivint *man <ordre>* en un terminal.

L'ordre `smbtree` mostra tots els equips del grup de treball en mode text, de manera similar a l'*Entorn de xarxa* de Windows. Dibuixa un arbre amb tots els dominis coneguts, els servidors que comparteixen recursos i els seus noms.

```
# smbtree -N
IOC
     \\WINXP
          \\WINXP\C$
          \\WINXP\ADMIN$               Admin remota
          \\WINXP\Compartit2
          \\WINXP\Compartit1
          \\WINXP\IPC$                 IPC remota
     \\SERVIDOR                   debian server
          \\SERVIDOR\HP_1102W          HP_1102W
          \\SERVIDOR\IPC$              IPC Service
          \\SERVIDOR\print$            Printer Drivers
```

Amb la opció *-N* podeu fer la consulta sense necessitat d'introduir cap contrasenya.

Per llistar els recursos compartits per una màquina es pot fer servir l'ordre `smbclient -L` seguida del nom de l'ordinador.

```
# smbclient -L WINXP -N
Domain=[WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

     Sharename      Type      Comment
     ---------      ----      -------
     IPC$           IPC       IPC remota
     Compartit1     Disk
     Compartit2     Disk
     ADMIN$         Disk      Admin remota
     C$             Disk      Recurso predeterminado
```

En l'exemple podeu observar que la màquina comparteix cinc recursos en total, tres dels quals són ocults. Fent servir la mateixa ordre podeu accedir al recurs indicant l'adreça UNC, i amb la opció *-U* especifiqueu quin usuari feu servir per realitzar la connexió.

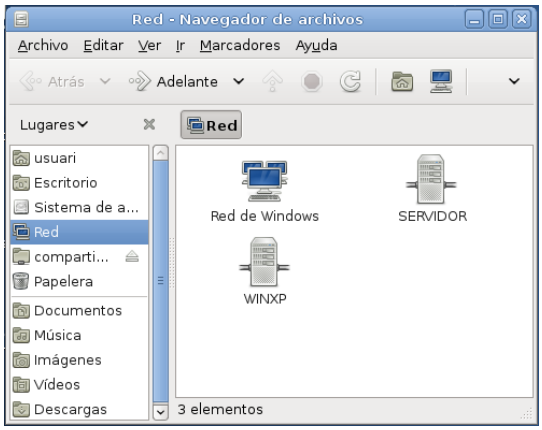
```
# smbclient //WINXP/Compartit1 –U usuari
Enter usuari's password:
Domain=[WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \>
```

Un entorn interactiu us permet realitzar les accions desitjades en el recurs compartit. Algunes de les ordres utilitzades són semblants a les d'Unix (*cd*,*ls*,*pwd*...), mentre que per pujar o descarregar-nos fitxers podeu fer servir *put* i *get*, respectivament. En cas de dubte, escrivint *help* obtindreu la llista d'opcions.

```
smb: \> help
```

Si feu servir Debian o Ubuntu podeu accedir amb l'interfície gràfica que proporciona l'escriptori. S'hi pot accedir des de *Llocs* > *Xarxa* i s'obrirà la finestra mostrada a la figura 2.13.

FIGURA 2.13. Accés a la xarxa des de l'interfície gràfica d'Ubuntu



De manera senzilla podeu navegar pels diferents servidors de xarxa de forma molt similar a Windows.

2.1.7 Accés als recursos mitjançant clients Microsoft Windows

L'accés als recursos compartits per Samba mitjançant un client Windows es pot realitzar fent servir les utilitats gràfiques que proporciona el mateix explorador del sistema operatiu de forma totalment intuïtiva.

Per accedir al servidor Samba primer heu d'assignar un nom NetBIOS i unir l'equip Windows al mateix grup de treball. Per fer-ho, a Windows Vista i Windows 7 seguiu els passos següents:

1. Fer clic a *Inici* >*Equip*.

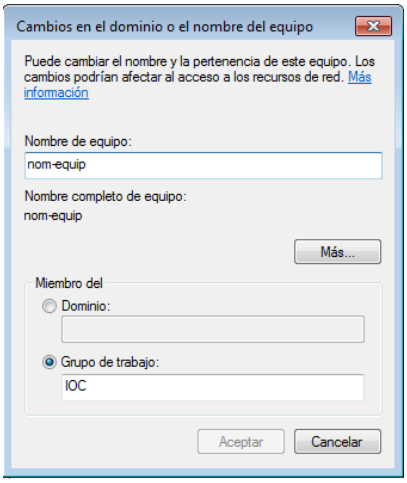
2. Fer clic al botó superior amb l'etiqueta *Propietats del sistema*.

3. Dins de la secció *Configuració del nom, domini i grup de treball del equip*, fer clic a *Canviar configuració*.

4. Fer clic al botó *Canviar*.

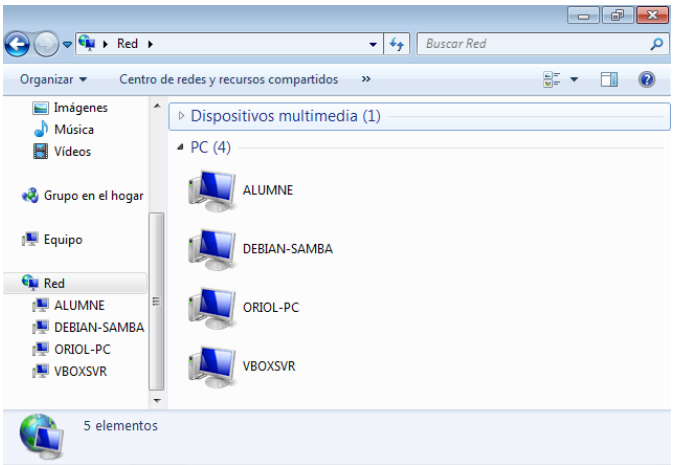
A la figura 2.14 s'observa la finestra de configuració d'un ordinador unit al grup de treball IOC amb el nom *nom-equip*. Un cop unit al grup de treball s'ha de reiniciar la màquina.

FIGURA 2.14. Finestra de configuració del grup de treball



S'accedeix als recursos compartits a través de l'explorador de la xarxa o bé escrivint l'adreça UNC del recurs compartit directament a la barra superior (per exemple, `\\Servidor\recurs`), fent servir el nom NetBIOS del servidor o bé l'adreça IP seguida del nom del recurs, tal i com mostra la figura 2.15.

FIGURA 2.15. L'accés als recursos compartits mitjançant Windows es realitza de manera intuïtiva



2.2 El servidor Samba com a controlador primari de domini

Quan el nombre d'equips d'una xarxa creix, l'administració dels recursos es fa cada vegada més complicada. Per això, en aquestes situacions és convenient fer servir un model de xarxa centralitzat amb un controlador de domini.

Per configurar Samba com a CPD cal realitzar els passos següents:

1. Especificar el nom del domini.
2. Admetre les peticions de *login*.
3. Establir el rol de *domain master browser*.
4. **Opcional:** compartir el recurs especial *netlogon*.
5. **Opcional:** habilitar els perfils mòbils.

Per establir el nom del domini es fa servir el paràmetre *workgroup*, el mateix que s'utilitza per especificar el grup de treball quan Samba és un servidor *stand-alone*. Així, si voleu crear un domini anomenat *IOC* cal que estabiu el paràmetre *workgroup = IOC*.

D'altra banda, Samba atén les peticions d'entrada al domini (*login*) quan estabiu el paràmetre *domain logons = yes*. En aquest cas també és necessari assignar-li el rol de *domain master* (`domain master = yes`) per tal que el servidor contingui la llista d'ordinadors del domini.

Domain master browser

El domain master browser conté la llista de tots els equips del domini, i no només els de la seva xarxa, com en el cas del local master browser.

```
[global]
     workgroup = IOC
     netbios name = Debian_Samba
     security = user
     encrypt passwords = yes
     domain logons = yes
     domain master = yes
```

Aquesta és la configuració mínima que requereix un servidor Samba per actuar com a controlador primari de domini. És convenient, però, que si realment voleu aprofitar les funcionalitats que ofereix un domini Windows NT afegiu també el recurs compartit *netlogon* i habiliteu els perfils mòbils.

Vegeu els apartats "El recurs *netlogon*" i "Perfils mòbils" per a més informació.

Cal reiniciar el servei per aplicar els canvis. Si us voleu assegurar que Samba s'ha configurat correctament com a controlador de domini, podeu consultar els missatges de *log* del dimoni `nmbd`.

```
# tail -f /var/log/samba/log.nmbd
```

En cas afirmatiu, obtindreu un missatge similar al següent:

```
[2012/01/25 09:03:59.523972, 0] nmbd/nmbd_logonnames.c:121(
    become_logon_server_success)
  become_logon_server_success: Samba is now a logon server for workgroup DOMINI
       on subnet 192.168.1.2
```

2.2.1 Comptes d'usuari i d'equip

Els usuaris que poden entrar al domini s'han de donar d'alta prèviament en el controlador de domini. Per tant, cal afegir-los primer com a usuaris GNU/Linux i després incorporar-los al *backend*.

El procediment per afegir usuaris és el que ja coneixeu, però abans cal considerar un aspecte relacionat amb la seguretat: la finalitat és que els usuaris puguin entrar al domini, però en cap cas que puguin fer servir el compte per iniciar sessió al servidor. Per això, podeu blocar l'entrada al servidor si no li assigneu cap *shell*. En aquest cas, *-s /bin/false*.

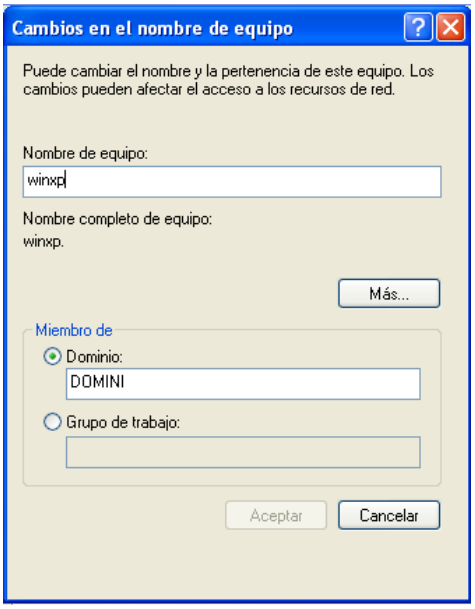
```
# useradd -d /home/usuari -s /bin/false -m usuari
# smbpasswd -a usuari
New SMB password:
Retype new SMB password:
Added user usuari.
```

Això no és suficient. A més d'afegir un compte d'usuari, per incorporar un equip al domini s'ha de crear un **compte d'equip**.

Els comptes d'equip, anomenats ***workstation trust accounts***, permeten que el controlador de domini mantingui una llista sobre quines són les màquines en les quals cal atendre els processos d'autenticació. D'aquesta manera, el controlador sap en tot moment si ha de fer cas o ha d'ignorar la petició de *login* que li arriba des d'un equip.

És indispensable crear un compte d'equip abans d'afegir-lo al domini.

FIGURA 2.16. Cada màquina dins del domini s'identifica per un nom



El compte d'un equip s'identifica per un nom i ha de coincidir amb el nom del sistema de Windows. Com qualsevol altre compte, s'ha d'emmagatzemar al *backend* de manera similar. Es podendiferenciar perquè **un compte d'equip conté el símbol del dòlar** (**$**) al final del nom. En el cas de tenir un equip Windows configurat tal com mostra la figura 2.16, hauríeu d'afegir un compte de màquina anomenat `winxp$`.

Recordeu que qualsevol compte que afegiu al *backend* ha d'estar també donat d'alta com a usuari Linux, i el cas dels comptes d'equip no és una excepció. És recomanable tenir els comptes de màquines agrupats, per això podeu crear un grup de Linux on afegirem tots els comptes de màquina.

```
# groupadd maquines
```

Posteriorment, cal afegir un nou usuari amb el mateix nom que la màquina acabat en $ que podeu assignar directament al grup de màquines.

```
# useradd -g maquines winxp$
```

A continuació ja podeu afegir el compte al *backend*, fent servir el paràmetre *-m* de l'ordre *smbpasswd* per indicar que és un compte d'equip.

```
# smbpasswd -a -m winxp
Added user winxp$.
```

Els comptes d'equip en servidors Windows

Per defecte, en dominis controlats per servidors Windows no cal crear comptes de màquina manualment com fem en Samba. La realitat és que Windows Server les afegeix de manera automàtica quan una màquina s'uneix al domini.

Amb Samba, podeu simular aquest comportament. La variable add machine script de l'arxiu de configuració permet que s'executi una ordre personalitzada cada vegada s'incorpora una màquina al domini.

Si voleu que els comptes d'equip es creïn automàticament haureu d'assignar l'ordre apropiada a la variable*add machine script*. Aquesta s'executarà cada vegada que detecti que una màquina es vol incorporar al domini. Si la màquina ja existeix no s'executa. En aquest cas es tracta d'executar l'script *useradd*.

```
[global]
     ...
     add machine script = /usr/sbin/useradd -g \ maquines -d /var/lib/samba -s/
         bin/false %u
     ...
```

2.2.2 Accés al domini mitjançant clients Microsoft Windows

Per unir una màquina Windows heu de seguir els passos següents:

1. Fer clic a *Inici* > *Equip*.

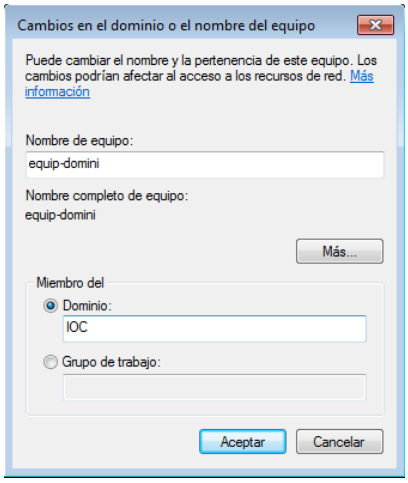
2. Fer clic al botó superior amb l'etiqueta *Propietats del sistema*.

3. Dins de la secció *Configuració del nom, domini i grup de treball del equip* fer clic a *Canviar configuració*.

4. Fer clic al botó *Canviar*.

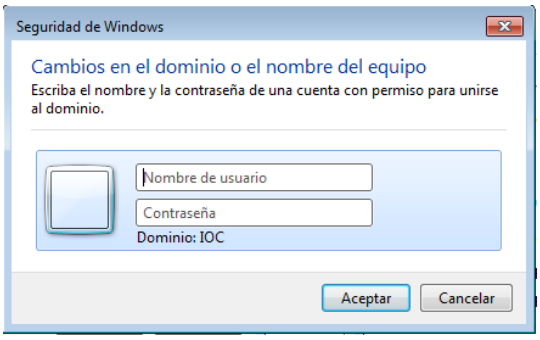
En aquesta finestra, mostrada en la figura 2.17, heu d'indicar el nom d'una màquina del domini i el nom del domini al qual voleu unir-vos. És imprescindible haver creat abans un compte de màquina en el controlador de domini.

FIGURA 2.17. Configuració del domini per accedir-hi



És important destacar que en un domini Samba, el nom del equip i el nom del domini no es poden canviar a la vegada.

FIGURA 2.18. Només un usuari amb permisos adequats pot afegir l'equip al domini



Posteriorment cal **indicar un compte d'usuari amb dret per unir màquines al domini** a la finestra mostrada en la figura 2.18. Quan el controlador de domini és Windows Server, normalment es fa servir el compte d'usuari *Administrador*, en canvi en dominis controlats per Samba es fa servir el compte *root*.

En general, l'usuari *root* té aquest dret per defecte, però si es vol delegar la feina a altres usuaris (recomanable) podeu assignar el dret *SeMachineAccountPrivilege* a qui cregueu convenient.

```
# net -U root%contrasenya rpc rights grant lluis \ SeMachineAccountPrivilege
Successfully granted rights.
```

En l'exemple s'ha donat el dret d'afegir i treure màquines del domini a l'usuari *lluis*. És evident que aquest dret no l'hauria de tenir tothom, només les persones encarregades d'administrar el sistema informàtic.

Consulteu l'apartat "Drets" per a més informació sobre com administrar els drets dels usuaris de Samba.

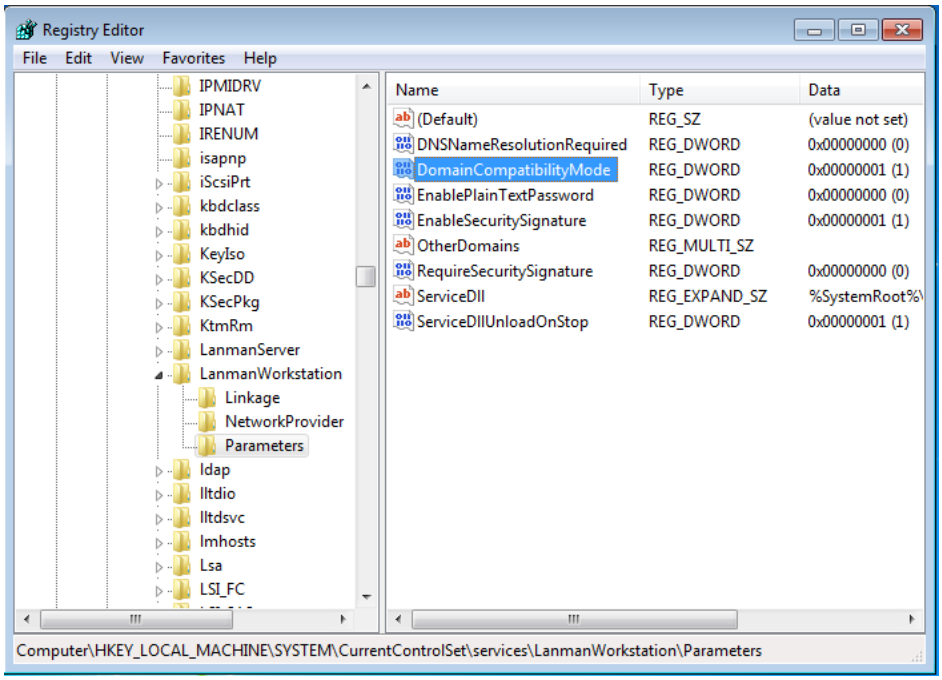
En general, no tindreu cap problema en el moment d'afegir un equip Windows excepte si ho intenteu amb un client Windows 7 o Windows 2008 R2. En aquests casos cal realitzar abans una sèrie de modificacions al registre del client (*regedit.exe*). La raó és que Microsoft ha deshabilitat per defecte la compatibilitat amb controladors de domini NT.

Cerqueu la clau següent:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\
    Parameters
```

En aquest punt cal afegir les dues noves variables següents amb els seus respectius valors tal com es mostra a la figura 2.19.

Figura 2.19. Addició de noves variables al registre de Windows

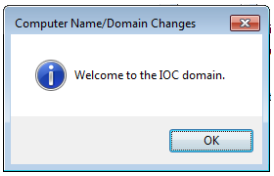



```
DWORD DomainCompatibilityMode = 1
DWORD DNSNameResolutionRequired = 0
```

Per afegir variables al registre feu clic amb el botó dret sobre la zona buida del editor i seleccioneu *Nuevo* > *Valor DWORD*, escriviu el nom i feu doble clic a sobre per assignar-li el valor.

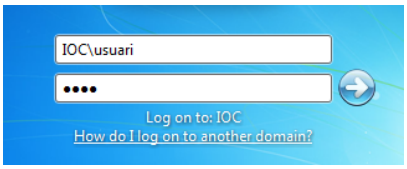
Salveu els canvis, reinicieu i podreu incorporar aquesta màquina al domini (figura 2.20).

FIGURA 2.20. Incorporació de la màquina al domini



Per entrar al domini amb un usuari heu d'indicar *NOMDOMINIusuari* a la pantalla de benvinguda del sistema operatiu, tal com mostra la figura 2.21.

FIGURA 2.21. Entrada amb un usuari



2.2.3 El recurs netlogon

En un controlador de domini, disposar del recurs compartit especial `[netlogon]` **és opcional**, però molt recomanable. Aquest recurs és un directori on s'emmagatzemen diversos arxius de gran utilitat en dominis, entre els quals trobem:

1. **El perfil per defecte dels usuaris**: quan un usuari entri al domini per primera vegada es carregarà el perfil per defecte. El perfil s'emmagatzema al subdirectori Default User.
2. **Els scripts de*login*:** Samba permet l'execució d'scripts de *login* Windows, arxius amb extensió *bat* o *cmd*que s'executen cada vegada que un client entra al domini. Aquests scripts s'emmagatzemen al recurs compartit i es transporten a la màquina client quan s'inicia sessió, i posteriorment s'executen. Cada script de *login* s'ha d'emmagatzemar al directori arrel del recurs `[netlogon]`.
3. **Les polítiques de grup**: fitxers `ntconfig.pol` o `config.pol`.

Aquest recurs es pot compartir com qualsevol altre, amb el requisit que ha de tenir permisos de **lectura per a tothom**i **opcionalment permisos totals per als administradors**. Altrament, qualsevol podria modificar els scripts de *login* i comprometre la seguretat del domini.

```
# mkdir /netlogon
# chgrp admins /netlogon
# chmod 775 /netlogon
```

El fitxer de configuració de Samba el compartirem amb el nom de `[netlogon]`.

```
# cat /etc/samba/smb.conf
```

```
[global]
     workgroup = IOC
     netbios name = Debian-Samba
     security = user
     encrypt passwords = yes
     domain logons = yes
     domain master = yes
[netlogon]
     path = /netlogon
     guest ok = yes
     read only = yes
     write list = @admins
     browseable = no
```

El paràmetre *browseable = no* amaga el recurs de l'explorador de xarxa.

Podem fer que cada vegada que un usuari entri en una màquina s'executi un script determinat. A la variable *logon script* cal indicar quin script volem que s'executi.

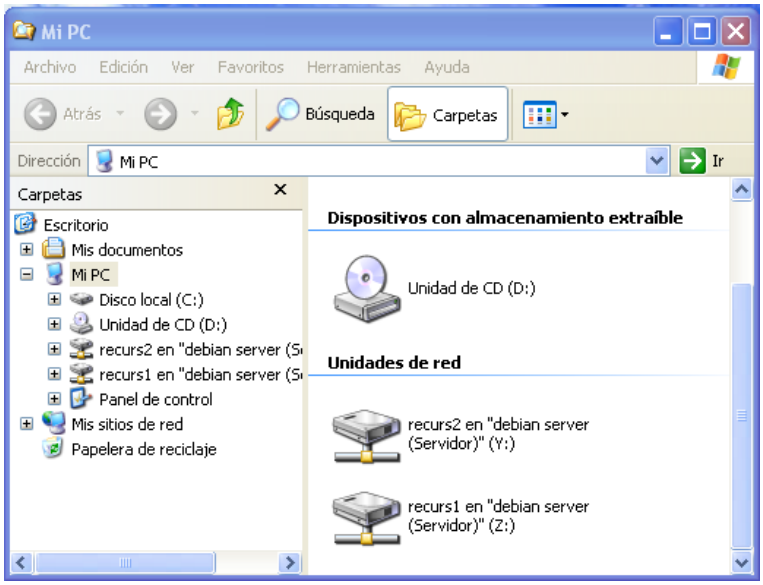
```
[global]
     ...
     logon script = logon.cmd
     ...
```

Cal que l'script estigui disponible al directori arrel del recurs *netlogon*. És a dir, si el recurs compartit és el directori `/netlogon`, llavors l'script haurà d'estar a `/netlogon/logon.cmd`.

Per exemple, si voleu muntar unitats de xarxa automàticament cada vegada que l'usuari inicia sessió (figura 2.22) podeu crear l'script següent:

```
# cat /netlogon/logon.cmd
net use z: \\Servidor\recurs1
net use y: \\Servidor\recurs2
```

FIGURA 2.22. Muntat automàtic d'unitats de xarxa



Recordeu que els scripts s'executen a la màquina del client (Windows), per tant, han d'estar en format DOS (final de línia CR/LF) i han de contenir ordres pròpies d'aquest sistema operatiu.

Els scripts del recurs *netlogon* han d'estar en format DOS, altrament no s'executaran correctament a la màquina del client.

Si genereu l'script amb un editor de Linux (**vi**, **nano**, **gedit**...), quan finalitzeu heu de canviar el format de l'arxiu d'Unix a DOS. Una de les maneres de fer-ho és amb la utilitat *todos*.

```
# apt-get install tofrodos
# todos /netlogon/logon.cmd
```

Formats DOS i Unix

Històricament, els arxius de text en DOS i Unix han fet servir codis diferents per representar el salt de línia, fet que provoca que els scripts editats en una família de sistemes operatius no es puguin executar directament en l'altre. S'han de convertir prèviament.

2.2.4 Perfils d'usuari

Els perfils d'usuari són una de les eines més importants de Windows per a la configuració de l'entorn de treball. Defineixen un entorn d'escriptori personalitzat, en el que s'inclou la configuració individual de la pantalla, així com les connexions de xarxa, les impressores, etcètera. Per defecte, cada usuari d'un sistema Windows té el perfil associat al nom d'usuari i s'emmagatzema al disc dur, normalment a `c:\documents and settings\` a Windows XP o `c:\Users` a Windows Vista i 7.

En un domini Windows distingim quatre tipus de perfils:

1. Perfils locals
2. Perfils per defecte d'un domini
3. Perfils obligatoris
4. Perfils mòbils

En un domini podeu definir un **perfil per defecte**, que és el que faran servir tots els usuaris quan es connectin per primera vegada. D'aquesta manera podem estalviar molta feina de configuració que s'hauria de realitzar màquina a màquina. Posteriorment, podeu habilitar els **perfils mòbils**, de manera que el perfil de l'usuari es desi al servidor cada vegada que tanca sessió i que es recuperi quan l'inicia. Si, en canvi, voleu que els usuaris puguin fer canvis durant la sessió però no desar els canvis, podeu establir un **perfil obligatori**.

Perfils per defecte

Quan un sistema Windows inicia sessió en un domini amb un usuari que no hi ha entrat mai, intenta descarregar-se el perfil per defecte del recurs compartit `[netlogon]` del controlador de domini. En cas de trobar-lo, fa una còpia local i inicia la sessió de l'usuari. Si no el troba s'inicia una sessió amb un perfil buit.

Hi ha dues versions de perfils diferents:

1. Perfils per a Windows XP, Windows 2000 i Windows 2003
2. Perfils versió 2, per a Windows Vista, Windows 7 i Windows 2008

Els diferents tipus de perfils són incompatibles entre si, el que significa que si al domini tenim sistemes de la família Windows XP i de Windows 7 haurem de crear dos perfils per defecte diferents.

> Els perfils de la família de sistemes operatius Windows XP, 2000 i 2003 són incompatibles amb els de Windows Vista, 7 i 2008.

Pels clients amb Windows XP, el perfil per defecte ha d'estar emmagatzemat dins de la UNC del servidor `\\<Servidor>\netlogon\Default User`. Així, si la configuració del servei *netlogon* de Samba és la següent:

```
[netlogon]
     path = /netlogon
     guest ok = yes
     read only = yes
     write list = @admins
```

Vegeu l'apartat "Identificadors de seguretat i grups" per a més informació sobre com crear un grup d'administradors a Samba.

Llavors el perfil s'haurà de situar dins de `/netlogon/Default User` i caldrà que tothom hi tingui permisos de lectura; altrament no podran descarregar-s'ho. Per fer-ho heu de seguir els passos següents:

1. **Generar un perfil local i adaptar-lo a les vostres necessitats**: inicieu sessió com un usuari local de la màquina i configureu l'entorn (configuració de programes, escriptori, documents, etcètera).
2. **Tancar la sessió d'usuari local**.
3. **Iniciar la sessió al domini amb un compte d'administrador** (figura 2.23). Si no heu generat el grup d'administradors, podeu fer servir l'usuari *root*.
4. **Copiar el perfil del pas 1 al servidor**: *Inicio* > *Mi PC* > *Propietats* > *Opcions avançades*. A la finestra mostrada a la figura 2.24 premeu el botó *Configuració* de l'apartat *Perfils d'usuari*.

   Seleccionar el perfil local que desitgem copiar al servidor i fer clic a *Copiar a...* (figura 2.25). A continuació indiqueu l'adreça al servei *netlogon* del servidor: `\\<Servidor>\netlogon\Default User\`.

   Si no podeu realitzar aquest pas segurament és perquè l'usuari amb el que us heu connectat no és administrador del domini o bé no té permisos per escriure en el recurs *netlogon*.
5. **Verificar que els arxius s'han copiat correctament al servidor**. Us podeu assegurar que el perfil s'ha copiat correctament entrant en el servidor i llistant el contingut del recurs *netlogon*. Haureu de poder veure el directori Default User.

```
# ls -l /netlogon
drwxr-xr-x 13 usuari usuari 4096 mar 2 17:53 Default User
```

FIGURA 2.23. Inici de sessió en Windows

FIGURA 2.24. opcions avançades de les Propietats del sistema

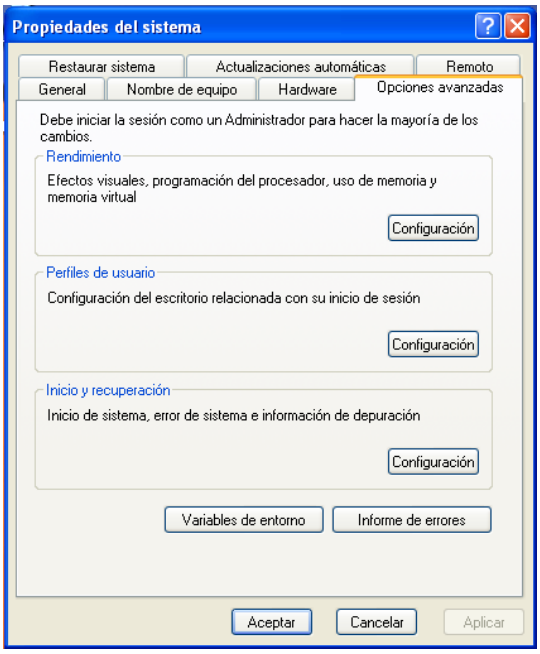


FIGURA 2.25. Perfils d'usuari

Els sistemes Windows Vista i 7 fan servir un altre tipus de perfils, coneguts com a *Perfils versió 2*. Per això, caldrà copiar-los al servidor dins del directori `Default User.v2` del recurs *netlogon* (`\\<Servidor>\netlogon\Default User.v2\`).

Els passos a seguir en sistemes Windows Vista, 7 o 2008 són molt similars als de Windows XP; l'única diferència és que només podem copiar al servidor el perfil per defecte de la màquina. En qualsevol cas, les accions que cal dur a terme són:

1. **Generar un perfil local i adaptar-lo a les vostres necessitats**: inicieu sessió com un usuari local i configureu l'entorn.

2. **Tancar la sessió d'usuari local i obrir una sessió local d'administrador**: inicieu sessió amb un compte d'usuari diferent de l'utilitzat en el pas anterior.

3. **Copiar el perfil generat en el primer pas al perfil per defecte**: obriu l'explorador, navegueu a `c:\Users` i seleccioneu el perfil de l'usuari local que heu generat en el primer pas. Canvieu el nom del perfil a *Default*. Com que aquest directori ja existeix, heu de canviar-li el nom prèviament: `Default > Copia` (figura 2.26).

4. **Iniciar sessió amb un compte d'administrador del domini**.

5. **Copiar el perfil per defecte al controlador de domini**: *Inici* > *Equip* > *Propietats* > *Opcions avançades*. Fer clic a la pestanya *Avançat*, i en la secció *Perfils d'usuari* prémer el botó *Configurar...*. Us apareixerà una finestra similar a la de la figura 2.27. Seleccioneu el perfil per defecte i copieu-lo al servidor.

6. **Verificar que els arxius s'han copiat correctament al servidor**.

```
# ls -l /netlogon
total 12
drwxr-xr-x 14 usuari usuari 4096 mar 4 10:10 Default User.v2
```

FIGURA 2.26. Còpia d'un perfil

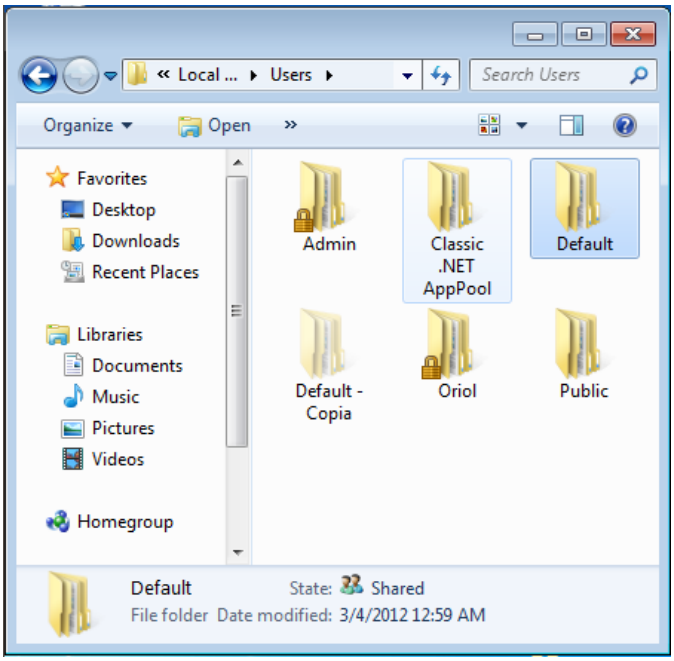
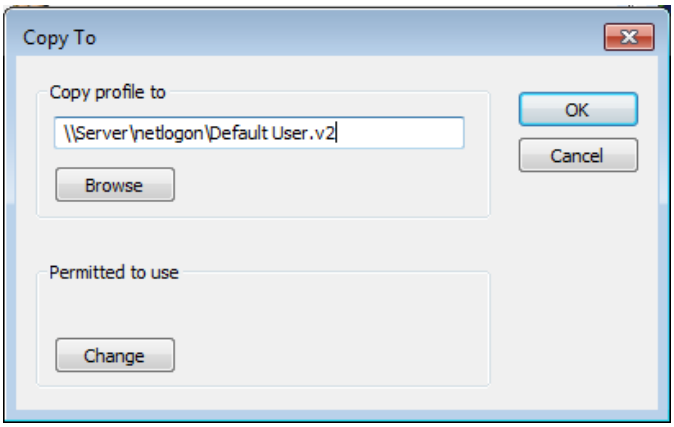


FIGURA 2.27. Còpia del perfil al servidor



Perfils mòbils

Gràcies als **perfils mòbils** els usuaris d'un domini poden iniciar sessió en qualsevol màquina de la mateixa xarxa i accedir als seus documents. Quan l'usuari es connecta, es recupera el seu perfil del servidor i se'n fa una còpia a la màquina local. Al finalitzar la sessió es desen els canvis del perfil al servidor. D'aquesta manera els usuaris tenen la sensació d'estar treballant sempre en el mateix equip.

Cal tenir en consideració la **càrrega extra que pateix la xarxa** quan es fan servir perfils mòbils, especialment en xarxes lentes o usuaris amb gran quantitat d'arxius al seu perfil. Per això, és recomanable que s'usi només en circumstàncies específiques.

Per habilitar l'ús dels perfils mòbils cal realitzar els passos següents:

1. Crear un recurs compartit on emmagatzemar els perfils.

2. Configurar els paràmetres adequats de Samba per habilitar els perfils mòbils.

És evident que si es vol disposar de perfils mòbils cal disposar d'un lloc en el servidor on emmagatzemar cadascun dels perfils dels usuaris. Per tant, el primer pas és crear un recurs compartit per emmagatzemar perfils. Típicament es fa servir el nom `[profiles]`, però en realitat pot anomenar-se com es desitgi.

Cal crear un directori on emmagatzemar els perfils, de manera que tothom tingui accés d'escriptura i només pugui modificar els seus arxius (*sticky bit*). En aquest cas es desitja emmagatzemar-los en un directori situat a l'arrel anomenat `perfils`.

```
# mkdir /perfils
# chmod 1777 /perfils
```

Aquest directori s'ha de compartir amb unes quantes consideracions de seguretat:

1. És recomanable que el recurs estigui ocult: *browseable = no*.
2. Els usuaris no han de poder entrar al perfil d'altres usuaris ni modificar-los: *create mask = 0600* i *directory mask = 0700*.
3. Els invitats no hi han de poder entrar: *guest ok = no*.
4. S'ha de permetre l'escriptura al recurs: *read only = no*.

Per tant:

```
[profiles]
     comment = Perfils d'usuari
     path = /perfils
     guest ok = no
     browseable = no
     create mask = 0600
     directory mask = 0700
     read only = no
```

Finalment, cal habilitar l'ús dels perfils mòbils amb el paràmetre *logon path* de la secció `[global]`. En aquest paràmetre hem d'indicar en quin lloc de la xarxa tenen els clients el seu perfil, especificant l'adreça UNC del recurs.

Els perfils són a l'adreça `\\<servidor>\profiles\`, i s'haurien d'emmagatzemar de manera separada per a cada usuari. És a dir, l'usuari *oriol* emmagatzemarà el seu perfil a `\\<servidor>\profiles\oriol` i l'usuari *lluis* a `\\<servidor>\profiles\lluis`.

Per tant, a la variable *logon path* posarem el següent:

```
[global]
     ...
     logon path = \\%N\profiles\%U
     ...
```

On *%N* substitueix el nom del servidor i *%U* substitueix el nom de l'usuari. Si s'hi connecta un usuari que no té perfil, el directori amb el seu nom es crearà automàticament.

Aquesta configuració té un problema: com heu vist, hi ha diferents tipus de perfil segons la versió de Windows, doncs un perfil de Windows XP no és compatible amb un de Windows 7. Llavors, **si en el domini hi ha diferents versions de Windows cal separar els perfils d'una família de la resta**. Amb la variable *%a* podem crear diferents directoris per als diferents tipus d'arquitectures.

```
[global]
     ...
     logon path = \\%N\profiles\%U\%a
     ...
```

L'exemple següent mostra el directori de perfils d'un usuari que ha fet servir diversos sistemes operatius per iniciar sessió al domini:

```
# ls -l /perfils/oriol/
total 8
drwx------ 2 oriol oriol 4096 mar 4 13:01 Vista.V2
drwx------ 13 oriol oriol 4096 mar 4 12:58 WinXP
```

Com veieu, quan s'habiliten els perfils mòbils cal tenir en consideració l'espai que poden arribar a ocupar al servidor i la sobrecàrrega de la xarxa.

Perfils obligatoris

Hi ha casos en què no és desitjable desar els canvis dels perfils dels usuaris. Els **perfils obligatoris**són la manera de forçar tots els usuaris a usar un perfil únic. El perfil es descarrega durant l'inici de sessió i tots els canvis realitzats són esborrats al acabar.

Per transformar un perfil normal en un perfil obligatori només cal modificar el nom de l'arxiu `NTUSER.DAT` per `NTUSER.MAN`. Aquest arxiu és a l'arrel del perfil.

```
# mv ntuser.dat ntuser.man
```

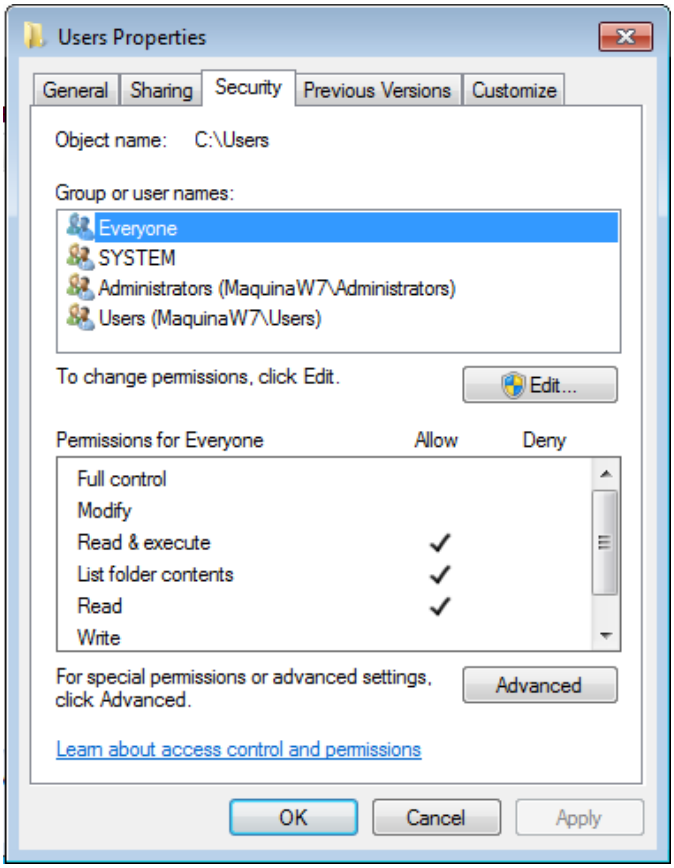
Així, doncs, si apliquem un perfil obligatori només és necessari tenir un sol perfil per usuari al servidor. Per tant, podem copiar-lo dins del recurs `profiles` i eliminar la variable del nom d'usuari del paràmetre *logon path*.

```
[global]
     ...
     logon path = \\%N\profiles\%a
     ...
```

2.2.5 Identificadors de seguretat i grups

El mecanisme de permisos de Windows està basat en les llistes de control d'accés (ACL). Com podeu veure en la figura 2.28, cada recurs (fitxer, directori, impressora, etc.) té associada una ACL en la qual es detallen el conjunt d'accions que estan autoritzades a certs usuaris o grups (llegir, escriure, esborrar...). El sistema és l'encarregat de decidir si un determinat usuari està autoritzat a fer l'acció que ha sol·licitat basant-se en l'ACL.

FIGURA 2.28. En Windows, els permisos es basen en les ACL i els identificadors de seguretat



A l'hora d'autoritzar o denegar una l'acció, Windows no ho determina fent servir el nom d'usuari o el nom del grup, sinó que, tal com ocorre a Unix, es fa servir un identificador. Aquest identificador rep el nom d'**identificador de seguretat** o **SID** i, depenent de l'àmbit, podem parlar de SID del domini o de SID local.

> A l'hora d'autoritzar o denegar una acció sobre un recurs, Windows no es basa en el nom d'usuari sinó en el seu identificador de seguretat (SID).

L'identificador de seguretat de Windows és un codi alfanumèric que **identifica usuaris o grups en un entorn local, o un objecte qualsevol dins d'un domini**: usuaris, grups, màquines, impressores, etcètera. Aquest codi és únic per cada a objecte i s'assigna en el moment de la seva creació. És similar a l'identificador d'usuari (UID) i de grup (GID) en un sistema GNU/Linux.

El mecanisme de seguretat basat en el SID també està implementat a Samba: tot usuari, grup i objecte dins del *backend* té associat un identificador de seguretat. Aquesta característica pren especial rellevància quan aquest actua com a controlador de domini.

En general, tant a Windows com a Samba, es pot distingir entre:

1. SID local
2. SID de domini

En el moment d'instal·lar un sistema operatiu Windows o iniciar per primera vegada el servei Samba en un sistema GNU/Linux, s'assigna aleatòriament un SID local que queda emmagatzemat al registre. A Windows, aquest SID només s'utilitza en un context local de cara als usuaris creats dins de la màquina, sobretot a l'hora de determinar els permisos d'accés a les particions de disc NTFS.

En el cas d'un equip que es promogui a controlador de domini, el SID local es copiarà per crear el SID de domini. En aquest cas,**el SID local serà idèntic al SID del domini** i és el que s'utilitzarà per determinar els permisos dins de l'àmbit domini.

Així, quan un usuari accedeix a un domini, en el procés de *login* el controlador li atorga una espècie de carnet d'identitat anomenat *token*. Aquest conté el SID corresponent al seu usuari i els de tots els grups als quals pertany. Quan aquesta persona vol accedir a un recurs, com ara un directori compartit, es verifica el seu *token* juntament amb l'ACL del recurs i s'autoritza o es denega l'acció que vol realitzar.

El SID local o de domini s'acostuma a representar com una cadena de caràcters separats per guions, com mostra l'exemple:

```
1 S-1-5-21-2919073133-884734282-1099352923-1104
```

Sense entrar en detall en el significat de cadascun dels caràcters, podem dividir un SID en dues parts mostrades en la figura 34. La primera, que comprèn des del primer caràcter fins a l'últim guió, conté l'identificador del domini (en l'exemple és `S-1-5-21-2919073133-884734282-1099352923`). **Aquest valor és el mateix per a tots els objectes dins d'un domini**. És a dir, els SID de dos usuari, grups o màquines pertanyents al mateix domini contenen aquests mateixos caràcters. La part restant del SID és l'identificador relatiu, o RID, i identifica l'objecte dins del domini. En l'exemple de la figura 2.29, el RID és `1104`. Aquest nombre **mai es repeteix dins d'un mateix domini**.

FIGURA 2.29. SID del domini i RID de l'objecte

Samba implementa un mecanisme per emmagatzemar identificadors de seguretat SID de manera similar a Windows. Podem obtenir el SID local o de domini mitjançant l'ordre *net*, amb les opcions *getdomainsid* o *getlocalsid*, respectivament.

```
# net getdomainsid
SID for local machine DEBIAN is: S-1-5-21-2862684848-1588976619-3858101340
SID for domain DOMINI is: S-1-5-21-2919073133-884734282-1099352923
```

Quan Samba és un controlador de domini es pot observar que el SID local i el SID de domini es corresponen.

Fent servir l'ordre *pdbedit* podem consultar el SID d'un usuari, així com el SID del seu grup principal.

```
# pdbedit -Lv lluis
Unix username: lluis
NT username:
Account Flags: [U ]
User SID: S-1-5-21-2862684848-1588976619-3858101340-1000
Primary Group SID: S-1-5-21-2862684848-1588976619-3858101340-513
Full Name:
Home Directory: \\debian\lluis
HomeDir Drive:
Logon Script:
Profile Path: \\debian\lluis\profile
Domain: DEBIAN
Account desc:
Workstations:
Munged dial:
Logon time: 0
Logoff time: never
Kickoff time: never
Password last set: sáb, 12 nov 2011 18:31:22 CET
Password can change: sáb, 12 nov 2011 18:31:22 CET
Password must change: never
Last bad password : 0
Bad password count : 0
Logon hours : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

En aquest exemple podem observar que el SID del domini és:

```
S-1-5-21-2862684848-1588976619-3858101340
```

i els RID de l'usuari i grup principal són 1000 i 513, respectivament. Com veureu a continuació, l'elecció d'aquests valors no és aleatòria.

En un domini Windows, existeixen una sèrie d'identificadors de seguretat associats a usuaris o grups que es creen per defecte cada vegada que es promou un controlador de domini. Aquests identificadors, resumits a la taula 2.5, tenen un RID inferior a 1000, al contrari dels grups o usuaris creats a posteriori, que tenen un RID igual o superior a 1000.

TAULA 2.5. RID del grups coneguts

RID	Descripció
500	Compte d'usuari per a l'administrador del sistema. Per defecte, és l'únic usuari que té control total.
501	Compte d'usuari convidat, sense contrasenya. Deshabilitat per defecte.

TAULA 2.5 (continuació)

RID	Descripció
512	Administradors del domini. Grup que permet als seus membres administrar el domini.
513	Usuaris del domini. Per defecte hi pertanyen tots els usuaris creats en el domini.
514	Convidats del domini.
515	Equips del domini.
544	Administradors.
548	Operadors de comptes.
550	Operadors d'impressió.
551	Operadors de còpies de seguretat.

Podeu consultar la llista d'identificadors més coneguts al web http://support.microsoft.com/kb/243330/es.

Samba permet associar SID dels grups de Windows a GID (identificador de grup) de Linux. El paràmetre *groupmap* de l'ordre *net* es pot fer servir per determinar aquestes associacions.

Per crear grups en un domini cal establir una associació entre el grup del domini Windows, identificat pel SID, i el grup de Linux.

Per defecte, Samba no crea cap mena d'associació ni grup. És a dir, tots aquells grups que per defecte es creen en un controlador de domini Windows no hi són i els heu d'afegir manualment (si els necessiteu). Per exemple, si voleu crear el grup d'administradors del domini, identificat pel RID 512, haureu de crear un grup Linux i vincular-los.

```
# groupadd admins
# net groupmap add rid=512 unixgroup=admins ntgroup="Administradors domini"
    comment="grup d'administradors del domini"
Successfully added group Administradors domini to the mapping db as a domain
    group
```

Crear l'associació del grup d'administradors és molt important, ja que un cop s'ha fet, **automàticament tots aquells usuaris que assignem al grup `admins` seràn administradors del domini amb tots els drets que això comporta**.

Així, doncs, si volem que l'usuari *oriol* sigui un administrador del domini només caldrà afegir-lo al grup *admins*:

```
# usermod –G admins oriol
```

A partir de l'assignació, l'usuari *oriol* podrà administrar màquines, impressores, usuaris, permisos, etcètera.

En general, però, podeu crear qualsevol grup i anomenar-lo com vulgueu; no esteu limitats a crear grups per defecte. Així, doncs, podríem crear grups per a professors i alumnes, tal com es mostra a continuació:

```
# groupadd professors
# groupadd alumnes
```

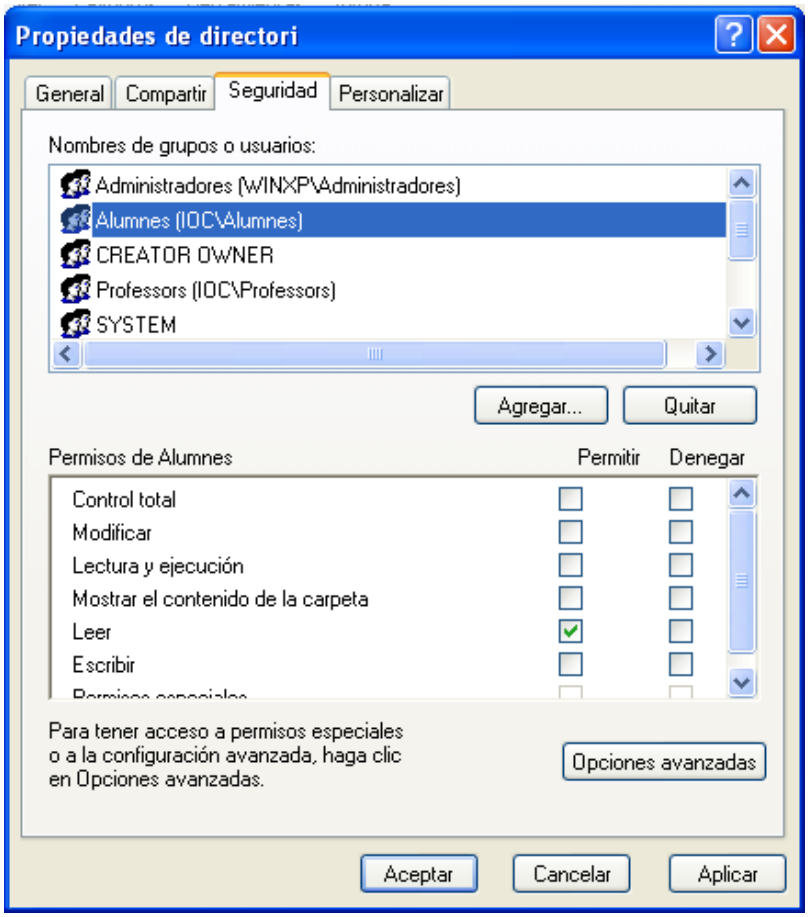
```
# net groupmap add rid=600 unixgroup=professors ntgroup="Professors"
Successfully added group Professors to the mapping db as a domain group
# net groupmap add rid=601 unixgroup=alumnes ntgroup="Alumnes"
Successfully added group Alumnes to the mapping db as a domain group
```

Llistant els grups veureu que la vinculació s'ha creat correctament:

```
# net groupmap list
Administradors domini (S-1-5-21-2768477417-3040658552-3227845813-512) -> admins
Alumnat (S-1-5-21-2768477417-3040658552-3227845813-601) -> alumnes
Professorat (S-1-5-21-2768477417-3040658552-3227845813-600) -> professors
```

Tots aquests grups, tal com podeu veure a la figura 2.30, apareixen creats correctament dins del domini.

FIGURA 2.30. Grups d'usuaris creats



Els vincles s'emmagatzemen en una base de dades, que per defecte és dins de l'arxiu `/var/lib/samba/group_mapping.ldb` i no al *backend*. Podeu afegir o treure usuaris dels grups fent servir l'ordre de Linux *usermod*.

```
# usermod -G alumnat -a usuari
```

Per a més informació sobre la manipulació de grups escriviu

```
# net groupmap
```

i obtindreu la llista d'opcions que es poden realitzar.

2.2.6 Drets

L'assignació de drets als usuaris permet alliberar la càrrega de l'usuari *root*. Fins fa poc, a Samba el superusuari era l'únic que podia realitzar algunes accions d'administració. En les darreres versions de Samba podem atorgar certes accions a usuaris o grups. Per defecte, Samba no assigna cap dret als usuaris. La taula 2.6 mostra el nom i la descripció de tots ells.

Taula 2.6. Drets d'usuari

Dret	Descripció
`SeMachineAccountPrivilege`	Afegir màquines al domini.
`SePrintOperatorPrivilege`	Administrar impressores.
`SeAddUsersPrivilege`	Afegir usuaris i grups al domini.
`SeRemoteShutdownPrivilege`	Forçar l'apagada des d'una màquina remota.
`SeDiskOperatorPrivilege`	Administrar un recurs compartit.
`SeTakeOwnershipPrivilege`	Prendre possessió d'un fitxer o directori del domini independentment del seu propietari.
`SeRestorePrivilege`	Assignar el propietari d'un fitxer o directori a un altre usuari.

Per defecte, només un administrador del domini pot assignar o treure els drets d'un usuari.

L'eina que es fa servir per administrar els drets és*net rpc rights*. Aquesta ordre permet assignar (*grant*), treure (*revoke*) o llistar (*list*) els drets en un servidor.

Per llistar tots els drets que permet assignar el servidor:

```
# net -S localhost -U root rpc rights list
Enter root's password:
     SeMachineAccountPrivilege
      SeTakeOwnershipPrivilege
             SeBackupPrivilege
            SeRestorePrivilege
     SeRemoteShutdownPrivilege
      SePrintOperatorPrivilege
           SeAddUsersPrivilege
       SeDiskOperatorPrivilege
```

Les opcions *-S* i *-U* indiquen el servidor i l'usuari que fem servir per realitzar l'acció. En aquest cas fem servir l'usuari arrel, però pot ser qualsevol administrador del domini. Si voleu assignar o treure un determinat dret a un usuari hem d'indicar el domini, el nom i el privilegi:

```
# net -S localhost -U root rpc rights grant 'IOC\usuari'
    SeDiskOperatorPrivilege
# net -S localhost -U root rpc rights revoke 'IOC\usuari'
    SeDiskOperatorPrivilege
```