

Compartir recursos en xarxa i seguretat en sistemes lliures i de propietat

Jordi Cárdenas Guia i Juan José López Zamorano

Sistemes operatius en xarxa

Índex

Introducció	5
Resultats d'aprenentatge	7
1 Compartir recursos en xarxa i seguretat en sistemes de propietat	9
1.1 Activació d'unitats compartides	9
1.2 Utilització d'unitats compartides	10
1.2.1 Crear carpetes compartides	11
1.3 Administració de permisos de recursos compartits	12
1.4 Administració dels recursos	13
1.5 Connexió a unitats de xarxa	17
1.6 Administració d'impressores de xarxa	17
1.7 Seguretat en sistemes de propietat	19
1.7.1 Permisos d'arxiu i carpeta	20
1.7.2 Còpies de seguretat i restauració de dades	22
1.8 Auditoria de recursos en sistemes de propietat	32
2 Compartir recursos en xarxa i seguretat en sistemes lliures	37
2.1 Protocol NFS	37
2.1.1 Usos del protocol NFS	38
2.1.2 Funcionament de l'NFS	39
2.1.3 Instal·lació i configuració del client NFS	39
2.2 Què és el Samba?	42
2.2.1 Protocol NetBIOS	42
2.2.2 Protocol SMB	43
2.2.3 Característiques del Samba	43
2.3 Seguretat en el Samba	45
2.3.1 Share-level security	46
2.3.2 User-level security	47
2.3.3 Domain security mode (user-level security)	48
2.3.4 ADS security mode (user-level security)	48
2.3.5 Server security (user-level security)	49
2.3.6 Opcions de seguretat en l'apartat GLOBALS del fitxer de configuració	49
2.4 Instal·lació del servidor i del client Samba	49
2.5 Gestió d'usuaris, grups i permisos del Samba	52
2.5.1 Gestió d'usuaris Samba	52
2.5.2 Permisos i drets Samba	53
2.5.3 Gestió de grups i permisos	55
2.6 Configuració del servidor Samba	56
2.6.1 Configuració gràfica del servidor Samba amb el Swat	62
2.7 Utilització del client Samba	67
2.8 Muntar unitats de xarxa	69
2.9 Accés gràfic als recursos compartits	71

2.10	Servidor d'impressió CUPS	72
2.10.1	Funcionament del CUPS	72
2.10.2	Instal·lació i configuració del CUPS	73
2.10.3	Compartir impressores gràficament amb el CUPS	74
2.10.4	Samba i CUPS	78

Introducció

Un dels motius principals pels quals els equips, en les organitzacions, es connecten per mitjà d'una xarxa és la compartició de recursos del sistema informàtic. Quan parlem de recursos compartits ens podem referir a qualsevol entitat, sia programari o maquinari, susceptible de ser compartit. Els sistemes operatius tenen un paper fonamental en aquest mecanisme de compartició, ja que proporcionen les eines necessàries per controlar, gestionar i compartir els recursos que hi ha a la xarxa.

Tant en sistemes operatius lliures com en sistemes de propietat, hem de tenir clar el procés que cal seguir per tenir un sistema de xarxa que permeti autenticar els usuaris i proporcionar informació sobre els usuaris i els recursos que hi ha a la xarxa. Així, doncs, el pas següent serà conèixer i treballar amb els protocols i les aplicacions que ens permeten compartir els diversos recursos entre els usuaris de les xarxes Windows i GNU/Linux per separat.

En l'apartat "Compartir recursos en xarxa i seguretat en sistemes de propietat" es mostraran els mecanismes que es fan servir per compatir recursos en sistemes Windows. S'explicarà la manera de configurar i administrar els recursos que hi ha a la xarxa, tant impressores com unitats d'emmagatzematge. A més, es posarà èmfasi en la seguretat i l'auditoria dels recursos en els sistemes de propietat.

En l'apartat "Compartir recursos en xarxa i seguretat en sistemes lliures" s'exploraran les dues eines principals de compartició de recursos en els sistemes GNU/Linux: el protocol NFS i el paquet ofimàtic Samba. Es veurà el funcionament d'aquestes dues eines i també els nivells de seguretat que proporcionen. A més, es mostrarà amb exemples la configuració necessària per compartir directoris i impressores mitjançant les interfícies gràfiques que proporcionen l'Swat i el CUPS.

Per treballar els continguts d'aquesta unitat convé anar fent les activitats i els exercicis d'autoavaluació.

Resultats d'aprenentatge

En finalitzar aquesta unitat, l'alumne/a:

1. Reconeix la diferència entre permís i dret.
2. Identifica i assigna els recursos del sistema que es comparteixen en sistemes lliures i de propietat.
3. Comparteix impressores en xarxa en sistemes lliures i de propietat.
4. Utilitza l'entorn gràfic per compartir recursos en sistemes lliures i de propietat.
5. Estableix nivells de seguretat per controlar l'accés del client als recursos compartits en xarxa en sistemes lliures i de propietat.
6. Gestiona grups d'usuaris i l'accés als recursos compartits dels sistemes lliures i de propietat.
7. Comprova que les configuracions efectuades funcionen correctament.
8. Documenta les tasques de gestió de recursos que s'han fet, les incidències que hi ha hagut i les solucions que s'han aportat.
9. Cerca i interpreta documentació tècnica en les llengües oficials i en les que més s'utilitzen en el sector.

1. Compartir recursos en xarxa i seguretat en sistemes de propietat

La compartició de recursos és un dels pilars bàsics en el sistema operatiu Microsoft Windows Server 2008. És molt important establir models que permetin accedir als recursos compartits de manera segura i que facin possible auditar les dades i el sistema.

El sistema operatiu Microsoft Windows Server 2008 inclou dos models de compartició d'arxius:

- **El model estàndard:** permet que els usuaris remots accedeixin a recursos com arxius, carpetes i unitats. Aquest model fa que totes les carpetes i tots els arxius continguts en una carpeta compartida, o en una unitat compartida, siguin accessibles a un conjunt determinat d'usuaris.
- **El model públic:** consisteix a copiar o modificar els arxius d'una carpeta pública. Tots els usuaris que iniciïn sessió en local en aquell equip accediran sense problemes al contingut de la carpeta pública. Així, doncs, els usuaris que tinguin permís d'accés a l'equip de manera remota podran accedir, per mitjà de la xarxa, a aquesta carpeta pública, que és a `%SystemDrive%\Users\Public`.

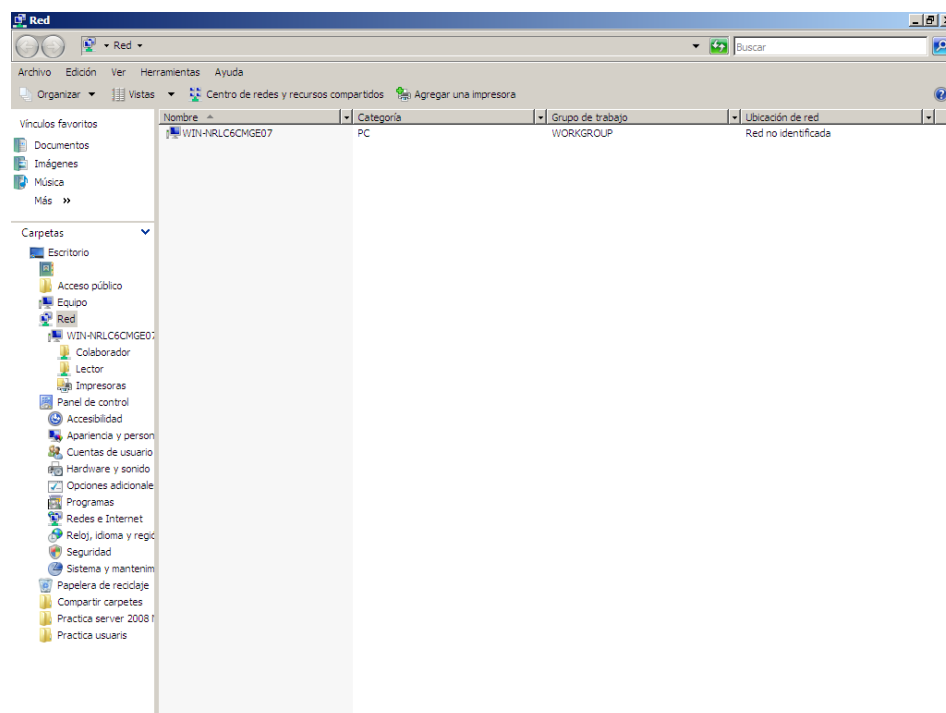
En l'apartat Annexos del material web d'aquesta unitat disposeu d'un enllaç a un document de Microsoft on es presenta la virtualització de màquines.

El model estàndard també es coneix com a *model in situ*.

1.1 Activació d'unitats compartides

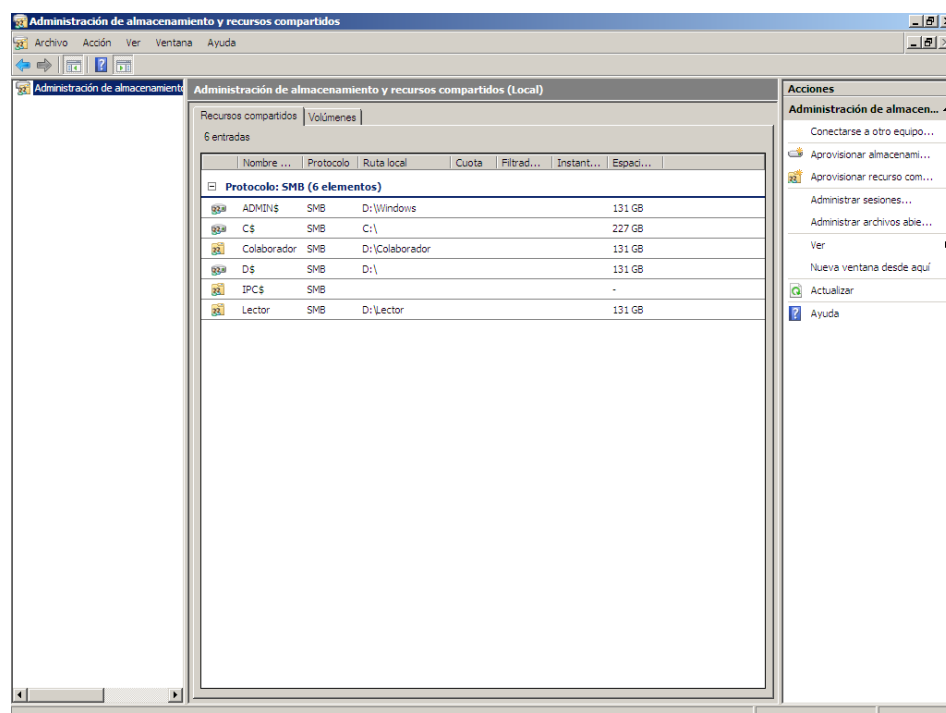
Per configurar les opcions bàsiques d'unitats i arxius compartits, cal que utilitzeu el centre de xarxes i recursos compartits. La figura 1.1 mostra l'aspecte bàsic d'aquesta utilitat i, com podeu observar, se segueix el concepte d'*administració gràfica* dels sistemes del Microsoft. Si seguiu els passos següents, podreu configurar el funcionament dels recursos compartits:

1. Cliqueu a *Inici > Xarxa* i accedireu al *Centre de xarxes i recursos compartits*.
2. L'opció *Ús compartit d'arxius* controla l'accés als recursos compartits per mitjà de la xarxa. Per poder compartir arxius d'aquest equip haureu de seleccionar *Activar l'ús compartit de fitxers*.
3. L'opció *Ús compartit de la carpeta Accés públic* controla l'accés a les carpetes públiques de l'equip.
4. L'opció *Ús compartit d'impressores* controla l'accés a les impressores connectades a l'equip.

FIGURA 1.1. Centre de xarxes i recursos compartits

1.2 Utilització d'unitats compartides

Per poder treballar amb els recursos compartits podeu utilitzar l'administració d'equipos, l'administració d'emmagatzematge i recursos compartits o l'ordre *net share* des de la interfície d'ordres. La figura 1.2 mostra l'aspecte que té l'administració d'equipos a Windows Server 2008.

FIGURA 1.2. Administració d'emmagatzematge i recursos compartits

Una manera d'examinar els recursos compartits en la màquina local mitjançant l'administració d'equips seria la següent:

Quan assigneu un nom a un recurs, cal que procureu que es relacioni el nom amb el recurs en qüestió.

1. Des d'*Administració d'equips* expandiu *Eines del sistema* i *Carpets compartides*.
2. Cliqueu a *Recursos compartits* i es mostraran, a la part principal de la finestra, els recursos que actualment estiguin compartits. S'ofereix aquesta informació:
 - **Nom del recurs:** és el nom del recurs compartit.
 - **Ruta de la carpeta:** és la ruta sencera en el sistema local.
 - **Tipus:** és el tipus d'ordinador que pot utilitzar el recurs.
 - **Nre. de connexions de client:** és la quantitat de clients que estan accedint al recurs en aquell precís moment.
 - **Descripció:** és la descripció del recurs.

Una manera d'examinar els recursos compartits en la màquina local mitjançant l'administració d'emmagatzematge i recursos compartits seria la següent:

Des d'*Administració d'emmagatzematge i recursos compartits* cliqueu a la fitxa *Recursos compartits*. N'obtindreu aquesta informació:

- **Nom del recurs compartit:** és el nom del recurs compartit.
- **Protocol:** és el nom del protocol utilitzat per compartir la carpeta.
- **Ruta local:** és la ruta completa de la carpeta en el sistema local.
- **Quota:** és el resum de l'estat de les quotes de l'administrador de recursos sobre la carpeta compartida.
- **Filtratge d'arxius:** és el resum de l'estat del filtratge d'arxius sobre la carpeta compartida.
- **Instantànies:** és el resum de l'estat de les instantànies sobre la carpeta compartida.
- **Espai lliure:** és la quantitat d'espai lliure en el disc si no hi ha quotes establertes.

1.2.1 Crear carpetes compartides

Hi ha tres camins per crear carpetes compartides en el servidor Microsoft Windows Server 2008: utilitzant l'explorador del Windows, utilitzant l'administració d'equips o utilitzant l'administració d'emmagatzematge i recursos compartits. Per compartir carpetes en un servidor Microsoft Windows Server 2008 s'ha de ser membre del grup d'administradors o operadors del servidor.

Compartir una carpeta

En compartir una carpeta per mitjà d'una xarxa, Windows, quan torna a iniciar la sessió, intenta connectar-se una altra vegada, de manera predeterminada, a totes les unitats assignades. Si no voleu que això passi, cal que desactiveu la casella de verificació *Connectar de nou en iniciar sessió*.

Mitjançant l'administració d'equips, els passos a seguir per compartir una carpeta són els següents:

1. Expandiu *Eines de sistema* i *Carpetes compartides*.
2. Seleccioneu *Recursos compartits*.
3. Cliqueu amb el botó dret a *Recursos compartits* i cliqueu a *Recurs compartit nou*. Aquest pas inicia un auxiliar que arrenca de manera automàtica.
4. Cliqueu a *Següent*.
5. Escriviu la ruta de la carpeta que voleu compartir en el quadre de text *Ruta de la carpeta*. Si la carpeta no existeix, l'auxiliar us preguntarà si la voleu crear respectant la ruta que heu introduït. Si no recordeu la ruta exacta, podeu navegar pels llocs mitjançant el botó *Examinar*.
6. Escriviu el nom que vulgueu posar al recurs compartit en el camp *Nom del recurs*.
7. Escriviu una descripció del recurs en el quadre *Descripció*.
8. Si voleu prohibir o habilitar l'accés al recurs per mitjà de la xarxa, cliqueu a *Canviar* i seleccioneu l'opció més adequada a *Configuració sense connexió*.
9. Cliqueu a *Següent* per establir els permisos.
10. Per acabar, cliqueu a *Finalitzar*.

Els tallafocs i les carpetes compartides

Heu de revisar la configuració dels tallafocs activats en el sistema quan treballeu amb compartició de recursos. És molt possible que no accediu a una carpeta compartida a causa de l'acció d'un tallafoc. No oblideu mai revisar la configuració dels tallafocs si teniu problemes d'accés a carpetes compartides.

Els permisos possibles d'accés a un recurs compartit són els següents:

- **Tots els usuaris tenen accés només de lectura:** els arxius es poden veure i llegir, però no es poden crear, modificar ni eliminar arxius i carpetes.
- **Els administradors tenen accés total; els altres usuaris tenen accés només de lectura:** els administradors poden veure, crear, modificar o eliminar continguts, però la resta d'usuaris només poden veure els arxius i llegir-ne el contingut.
- **Els administradors tenen accés total; cap altre usuari hi té accés:** els administradors poden veure, crear, modificar o eliminar continguts, però la resta d'usuaris no hi tenen accés.
- **Personalitzar membres:** permet configurar l'accés per a usuaris específics

i per a grups específics.

1.3 Administració de permisos de recursos compartits

La base de l'administració de permisos de recursos compartits en el Microsoft Windows Server 2008 és el format dels volums. Els volums NTFS permeten

utilitzar els permisos d'arxius i carpetes i també els perfils dels comptes dels propietaris d'arxius i carpetes per restringir les accions sobre el recurs. Si es fes servir un volum que utilitza la taula d'assignació de fitxers (en anglès, *file allocation table*, FAT), però, només es podria controlar l'accés.

Els permisos dels recursos que es comparteixen indiquen les accions permeses dins la carpeta. Quan es crea un recurs compartit, tothom que tingui accés a la xarxa tindrà permisos de **lectura**.

El sistema disposa de quatre permisos per als recursos compartits:

- **Sense accés:** no hi ha cap permís sobre el recurs.
- **Lectura:** aquest permís permet veure el nom dels arxius i de les subcarpetes, accedir a les subcarpetes, llegir la informació dels arxius i dels atributs que tinguin, i executar programes.
- **Modificar:** aquest permís inclou les possibilitats del permís de lectura i dóna capacitat per crear arxius i subcarpetes, modificar arxius, modificar atributs d'arxius i subcarpetes, i eliminar arxius i subcarpetes.
- **Control total:** aquest permís inclou les possibilitats dels permisos de lectura i de modificar. A més, però, permet canviar els permisos dels arxius i de les carpetes. També es pot fer seus els arxius i les carpetes.



Administració de permisos

Heu de comprendre molt bé el significat real dels permisos i administrar-los correctament. Si no ho feu, tindreu seriosos problemes de seguretat.

Per conèixer els permisos que té un recurs, es poden seguir els passos que es mostren a continuació:

1. Connecteu-vos al recurs dins de l'administració d'equips.
2. Expandiu *Eines de sistema*, *Carpetes compartides* i cliqueu a *Recursos compartits*.
3. Cliqueu amb el botó dret al recurs que vulgueu examinar i cliqueu a *Propietats*.
4. La fitxa *Permisos dels recursos compartits* us mostrarà l'usuari o grups d'usuaris que tenen accés al recurs i com és aquest accés. Aquesta fitxa permet modificar els permisos existents.

1.4 Administració dels recursos

L'administració de recursos del sistema és una tasca molt interessant i important dins l'administració del sistema. El sistema operatiu crea automàticament una sèrie de recursos compartits que facilitaran l'administració de recursos.

Els recursos compartits administratius o recursos compartits ocults són recursos compartits que ajuden en les tasques dels administradors del sistema.

No és possible assignar permisos sobre els recursos especials; l'encarregat d'aquesta tasca és el sistema operatiu mateix. Per crear manualment els vostres propis recursos compartits ocults, només haureu d'afegir el caràcter \$ al final del nom del recurs.

Tot i que els recursos compartits ocults es poden eliminar amb els permisos d'administrador, cada vegada que es reiniciï el sistema tornaran a crear-se de manera automàtica. Si voleu desactivar permanentment aquests recursos haureu de posar a zero dos registres:

1	HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer
2	
3	HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareWks

En la taula 1.1 es descriuen uns quants recursos compartits ocults:

TAULA 1.1. Recursos compartits ocults

Nom del recurs compartit ocult	Descripció	Utilització
ADMIN\$	Proporciona accés a la carpeta %SystemRoot%	S'utilitza en estacions de treball i servidors. Els administradors i els operadors de còpia hi tenen accés. En controladors de domini també hi poden accedir els operadors de servidor.
FAX\$	Proporciona suport per a faxos de xarxa.	L'utilitzen els clients de fax per enviar faxos.
IPC\$	Proporciona suport per a les comunicacions entre processos.	L'utilitzen els programes quan fan administració remota i quan examinen recursos compartits.
NETLOGON	Proporciona suport per al servei NetLogon.	L'utilitza el servei NetLogon quan processa peticions d'inici de sessió en el domini. Tots els usuaris tenen permís de lectura.
PRINT\$	Proporciona suport per a les impressores que estiguin compartides.	L'utilitzen les impressores compartides. Tots els usuaris tenen accés de lectura.
PUBLIC	Proporciona suport per als recursos compartits per mitjà de carpetes públiques.	S'utilitza per emmagatzemar dades públiques.
SYSVOL	Proporciona suport per al directori actiu.	S'utilitza per emmagatzemar dades i objectes del directori actiu.
LletraUnitat\$	Proporciona accés a l'arrel d'una unitat.	S'utilitza en estacions de treball i servidors. Els administradors i operadors de còpia hi tenen accés. En controladors de domini també hi poden accedir els operadors de servidor.

Realment recursos NETLOGON i SYSVOL no són recursos compartits ocults, sinó recursos compartits administratius especials. No es recomana eliminar-los.

Per accedir a un recurs compartit ocult heu de seguir els passos següents:

1. Cliqueu a *Inici* i, tot seguit, a *Equip*.
2. Cliqueu a *Connectar a unitat de xarxa*.
3. Seleccioneu la unitat que voleu de la llista *Unitat*.
4. Escriuiu la ruta del recurs al qual voleu accedir.
5. Cliqueu a sobre de *Finalitzar*.

Per crear un recurs compartit ocult nou, cal que feu el següent:

1. Al *Tauler de control*, feu doble clic a *Eines administratives* i, a continuació, feu doble clic a *Administració d'equips*.
2. Expandiu *Carpets compartides*, cliqueu amb el botó dret a *Recursos compartits* i, a continuació, feu clic a *Nou recurs compartit d'arxiu*.
3. En el quadre *Carpeta per compartir*, escriuiu la ruta d'accés de la carpeta que voleu compartir o cliqueu a *Examinar* per buscar-la.
4. Escriuiu el nom del recurs compartit que voleu utilitzar seguit del signe de dòlar i, a continuació, feu clic a *Següent*.
5. Activeu la casella de verificació *Els administradors tenen control total; la resta d'usuaris no tenen accés* per especificar que el recurs compartit només està disponible per als administradors. A continuació, feu clic a *Finalitzar*.

Per eliminar un recurs compartit ocult, cal que feu el següent:

1. Al *Tauler de control*, feu doble clic a *Eines administratives* i, a continuació, feu doble clic a *Administració d'equips*.
2. Expandiu *Carpets compartides* i cliqueu amb el botó dret a *Recursos compartits*.
3. En la *Carpeta compartida*, cliqueu amb el botó dret del ratolí al recurs compartit que voleu suprimir, feu clic a *Deixar de compartir* i, a continuació, feu clic a *Acceptar*.

Per comprovar les connexions a recursos compartits, podeu obrir el símbol de sistema i executar l'ordre *net session* o bé fer el següent:

1. Connecteu-vos a l'equip en què hi ha el recurs compartit des de l'administració d'equips.
2. Expandiu *Eines del sistema* i, tot seguit, *Carpets compartides*.
3. Seleccioneu *Sessions*.

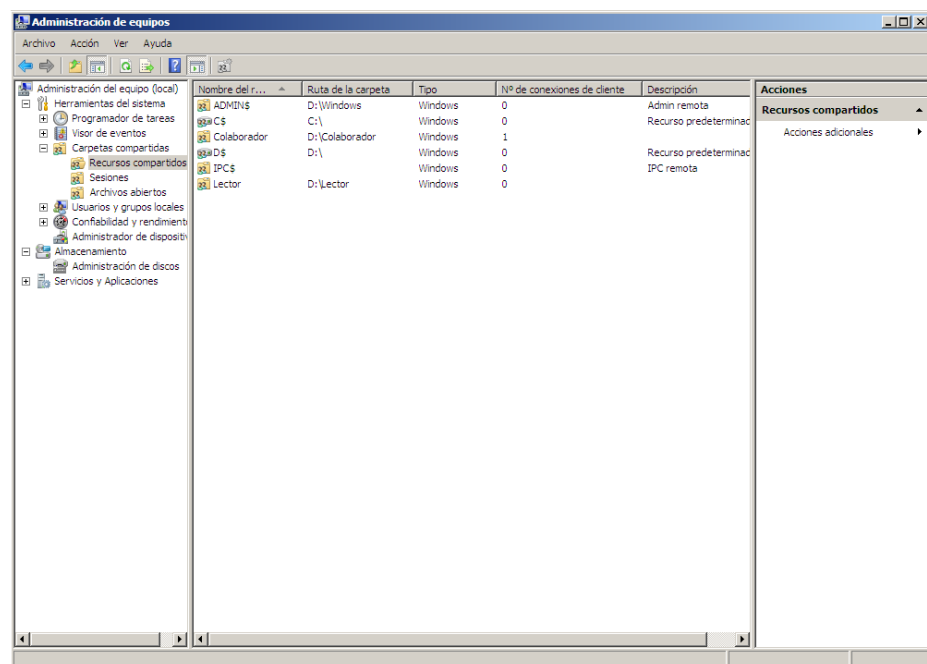
La informació que proporcionen les columnes del node *Sessions* és la següent:

Quan deshabiliteu un recurs compartit administratiu, cal que proveu que tot funciona correctament, ja que hi ha serveis del sistema i programes que els necessiten.

- **Usuari:** indica els noms dels usuaris o dels equips connectats al recurs. Detectareu els noms dels equips perquè van precedits pel caràcter dòlar.
- **Equip:** és el nom de l'equip que s'està utilitzant.
- **Tipus:** és el tipus de connexió de xarxa que s'està emprant.
- **Nombre d'arxius oberts:** és la quantitat de fitxers amb els quals està treballant l'usuari.
- **Connectat:** indica el temps que ha passat des que es va establir la connexió.
- **Inactiu:** indica el temps que ha passat des que es va utilitzar la connexió per última vegada.
- **Convidat:** indica si l'usuari que està connectat al recurs correspon a una sessió de convidat.

A la figura 1.3 es pot observar com es poden administrar els recursos compartits des de l'administrador d'equips.

FIGURA 1.3. Recursos compartits



Per tancar tots els fitxers oberts dels recursos compartits d'un equip, cal que seguïu els passos següents:

1. Connecteu-vos a l'equip en què hi ha el recurs compartit des de l'administració d'equips.
2. Expandiu *Eines del sistema* i, tot seguit, *Carpetes compartides*.
3. Seleccioneu *Arxius oberts*.
4. Cliqueu a *Desconnectar tots els arxius oberts* i cliqueu a *Sí* per confirmar.

1.5 Connexió a unitats de xarxa

Per connectar-se a una unitat de xarxa i accedir als recursos que conté, només cal executar l'ordre *net use*. Per exemple, si es vol accedir a un recurs amb l'etiqueta *Imatges* que s'emmagatzema en una màquina anomenada *Multimedia* i la lletra de la unitat és la *d*, cal escriure el següent: *net use d: [[]]*.

Per desconnectar-se d'una unitat de xarxa caldrà seguir aquests passos:

1. Executeu l'explorador del Windows mentre l'usuari estigui connectat a l'equip.
2. Dins del menú *Eines*, seleccioneu *Disconnectar de la unitat de xarxa*.
3. Seleccioneu la unitat que voleu desconnectar.
4. Cliqueu a *Acceptar*.

1.6 Administració d'impressores de xarxa

L'accés als dispositius d'impressió connectats a la xarxa requereixen que hi hagi un servidor d'impressió. Aquest servidor d'impressió s'encarregarà de compartir les impressores mitjançant la xarxa.

Per fer una administració correcta de les impressores de xarxa, cal tenir en compte els punts següents:

- Serveis d'impressió
- Configuració de servidors d'impressió
- Impressió compartida
- Propietats de les impressores
- Mostrar les impressores en el directori actiu

1. Serveis d'impressió. El sistema operatiu Microsoft Windows Server 2008 requereix una configuració específica per poder funcionar com a servidor d'impressió.

Un **servidor d'impressió** s'encarrega de compartir impressores dins una xarxa i de gestionar la cua d'impressió.

Els dispositius d'impressió que podeu trobar poden ser locals o de xarxa:

Si no podeu accedir a la carpeta d'impressores de manera remota, proveu de connectar-vos remotament al servidor Windows Server 2008 i, tot seguit, obriu la carpeta *Impressores*.

- **Dispositius d'impressió local:** aquest dispositiu està connectat físicament a un equip i només el poden utilitzar els usuaris que iniciïn una sessió en aquest equip.
- **Dispositius d'impressió de xarxa:** aquest dispositiu està configurat per poder-hi accedir remotament mitjançant una xarxa. Aquests dispositius poden connectar-se directament a la xarxa o bé poden utilitzar un servidor d'impressió per ser accessibles des d'altres equips.

2. Configuració de servidors d'impressió. És necessari afegir la funció *Serveis d'impressió* com una funció de servidor de l'*Administrador de servidor* per poder configurar un servidor com a servidor d'impressió. Hi ha tres serveis de funció:

- **Servidor d'impressió:** aquest servei configurarà el servidor d'impressió. Instal·la una consola d'administració d'impressió que permet gestionar diferents impressores i servidors d'impressió. A més, possibilita l'administració de treballs d'impressió.
- **Servei LPD:** aquest servei permet que equips que estiguin funcionant amb sistema operatiu UNIX o que utilitzin el servei LPR puguin accedir a les impressores compartides.
- **Impressió a Internet:** genera un espai web que permet als usuaris autoritzats gestionar els treballs que hagin enviat a les impressores compartides.

LPD o LPR

LPD o LPR és un protocol de xarxa que permet utilitzar impressores de manera remota. Les sigles volen dir *line printer daemon protocol* i *line printer remote protocol*, respectivament.

Per afegir la funció de serveis d'impressió, seguiu els passos següents:

- Obriu l'administrador del servidor.
- Seleccioneu el node *Funcions*.
- Cliqueu a *Afegir funcions*.
- S'inicia un auxiliar.
- Seleccioneu *Serveis d'impressió* i premeu *Següent* per validar.
- Escolliu tots els serveis que vulgueu a *Seleccionar serveis de funció*.
- Cliqueu a *Instal·lar*, després de seguir una sèrie de passos opcionals, per iniciar el procés d'instal·lació.

3. Impressió compartida. Mitjançant la impressió compartida és possible controlar l'accés a les impressores que estiguin connectades a un equip. Per defecte la compartició d'impressores està desactivada en el sistema Microsoft Windows Server 2008. Per activar aquesta característica haureu de fer el següent:

- Cliqueu a *Inici* i, tot seguit, a *Xarxa*.
- Obriu *Centre de xarxes i recursos compartits*.
- Cliqueu al botó *Ús compartit d'impressores*.

A partir d'aquí podreu activar o desactivar l'ús d'impressores compartides i seleccionar l'opció que més us convingui.

4. Propietats de les impressores. Les impressores tenen una sèrie de propietats. Si es gestionen bé, als usuaris de la xarxa els serà més fàcil utilitzar les impressores. Per exemple, és important incloure comentaris i informació sobre la ubicació física de la impressora. Per fer-ho, només cal que empleu els camps *Comentari* i *Ubicació* que hi ha dins la fitxa *General* de *Propietats*.

Per accedir al quadre *Propietats* de la impressora heu de fer el següent:

- Obriu l'administrador d'impressió.
- Expandiu el node *Servidores d'impressió*.
- Seleccioneu el node *Impressores*.
- Cliqueu amb el botó dret a sobre de la impressora que més us interessi i apareixerà *Propietats*.

5. Mostrar les impressores al directori actiu. Als usuaris els és molt útil la presència de les impressores al directori actiu. Per incloure una impressora al directori actiu haureu de fer el següent:

- Accediu a *Propietats* de la impressora que vulgueu incloure al directori actiu.
- Cliqueu a *Compartir*.
- Marqueu la casella *Compartir impressora*.
- Premeu *Acceptar* per validar.

Per publicar impressores heu de tenir drets d'administració de serveis de directori.

1.7 Seguretat en sistemes de propietat

Tots els objectes de la xarxa contenen informació sobre el control d'accés. Aquesta informació s'anomena *descriptor de seguretat*. El descriptor es genera automàticament i defineix el tipus d'accés permès a usuaris i grups. Per exemple, un arxiu és un objecte amb un descriptor de seguretat.

Cada assignació de permisos a un usuari o grup es representa en el sistema com una entrada de control d'accés (ACE). El conjunt complet d'entrades de permís d'un descriptor de seguretat s'anomena *conjunt de permisos* o *llista de control d'accés* (ACL).

Hi ha dos tipus de permisos:

- Els **permisos explícits**: s'estableixen de manera predeterminada en objectes pare quan es creen, o els que crea l'usuari a objectes que no són fills.

Jerarquia dels objectes

Els objectes es defineixen utilitzant l'estructura jeràrquica pare-fill. L'objecte pare és en el nivell més alt de jerarquia i el fill, en l'inferior.

- Els **permisos heretats**: es propaguen a un objecte des d'un objecte pare. Els permisos heretats faciliten la tasca d'administrar permisos i asseguren la coherència d'aquests permisos entre tots els objectes d'un contenidor determinat.

Per defecte, els objectes d'un contenidor hereten els permisos des d'aquest contenidor quan es creen els objectes.

El format NTFS del volum és el que possibilita l'establiment de permisos de seguretat en arxius i carpetes. Per veure els permisos d'un arxiu o d'una carpeta només heu de fer el següent:

1. Cliqueu amb el botó dret a sobre de l'arxiu i de la carpeta a estudiar.
2. Seleccioneu *Propietats*.
3. Cliqueu a la fitxa *Seguretat*.
4. Seleccioneu l'usuari, l'equip o el grup que vulgueu consultar dins la llista *Noms de grups o usuaris*.

1.7.1 Permisos d'arxiu i carpeta

Els arxius i les carpetes poden emprar els mateixos permisos, però s'ha de tenir en compte que el significat del permís canvia segons si s'aplica a un fitxer o a una carpeta. En la taula 1.2 es resumeixen els permisos d'arxius i carpetes en el Microsoft Windows Server 2008:

TAULA 1.2. Permisos de carpeta i fitxer

Permís	Significat en una carpeta	Significat en un fitxer
Lectura	Permet examinar i llistar arxius i subcarpetes.	Permet examinar o accedir al contingut.
Escriptura	Permet afegir arxius i subcarpetes.	Permet escriure dins l'arxiu.
Lectura i execució	Permet examinar i llistar els arxius i les subcarpetes, i també executar arxius.	Permet examinar l'arxiu, accedir al contingut i executar-lo.
Mostrar el contingut de la carpeta	Permet examinar i llistar arxius i subcarpetes, i també executar arxius.	Aquest permís no es pot aplicar sobre els arxius.
Modificar	Permet llegir i escriure arxius i subcarpetes, i també eliminar la carpeta.	Permet llegir, escriure i eliminar l'arxiu.
Control total	Permet llegir, escriure, modificar i eliminar arxius i carpetes.	Permet llegir, escriure, modificar i eliminar l'arxiu.

Tot i que els permisos *Mostrar el contingut de la carpeta* i *Lectura i execució* semblen tenir els mateixos permisos especials, s'hereten de manera diferent. El permís *Mostrar el contingut de la carpeta* l'hereten les carpetes (no l'hereten els

arxius) i només hauria d'aparèixer quan es veuen els permisos de carpeta. El permís *Lectura i execució* l'hereten els arxius i les carpetes, i sempre hi és quan es veuen els permisos d'arxiu o carpeta.

En el Microsoft Windows Server 2008, el grup *Tots* no inclou el grup *Inici de sessió anònima* per omissió, de manera que els permisos que s'apliquen al grup *Tots* no afecten el grup *Inici de sessió anònima*.

S'ha de tenir en compte que per executar *scripts* només cal que tingueu permís de lectura per poder accedir a un accés directe i a la destinació.

En la taula 1.3 es mostren les limitacions d'accés per a cada conjunt de permisos d'NTFS especials:

Control de carpetes

És molt important que no hi hagi gaires usuaris amb control total sobre les carpetes, ja que aquest control els permet eliminar els continguts de la carpeta independentment dels permisos que l'usuari tingui sobre aquests continguts.

TAULA 1.3. Permisos especials

Permisos especials	Control total	Modificar	Llegir i executar	Mostrar el contingut de la carpeta*	Lectura	Esriptura
Recórrer carpeta / executar arxiu	Sí	Sí	Sí	Sí		
Mostrar carpeta / llegir dades	Sí	Sí	Sí	Sí	Sí	
Llegir atributs	Sí	Sí	Sí	Sí	Sí	
Atributs estesos de lectura	Sí	Sí	Sí	Sí	Sí	
Crear arxius / escriure dades		Sí	Sí			Sí
Crear carpetes / annexar dades	Sí	Sí				Sí
Escriure atributs	Sí	Sí				Sí
Escriure atributs estesos	Sí	Sí				Sí
Eliminar subcarpetes i arxius	Sí					
Eliminar	Sí	Sí				
Permisos de lectura	Sí	Sí	Sí	Sí	Sí	Sí
Canviar permisos	Sí					
Prendre possessió	Sí					
Sincronitzar	Sí	Sí	Sí	Sí	Sí	Sí

* (només aplicable a carpetes)

1.7.2 Còpies de seguretat i restauració de dades

La protecció de les dades és necessària en qualsevol organització. El sistema operatiu ha de poder crear còpies de seguretat de les dades per evitar la pèrdua d'informació a causa d'esborraments accidentals o premeditats, errors del maquinari, corrupció de les bases de dades o qualsevol acció que pugui provocar un dany en els arxius emmagatzemats.

S'ha d'establir un pla de còpies per tal de dissenyar l'estratègia a seguir. Caldrà fer el següent:

- Establir quan i com s'ha de fer la còpia de seguretat i de quines dades.
- Comprovar el tipus d'informació que contenen les dades i decidir la importància que tenen.
- Detectar si les dades canvien lentament o no, cosa que determinarà la freqüència amb què se n'han de fer còpies.
- Decidir si és interessant fer instantànies per complementar les còpies de seguretat.
- Estudiar si cal que la restauració de les dades es faci pràcticament a l'instant o no.
- Comprovar, un cop determinades les característiques de les còpies que s'han de fer, que disposeu de tot el maquinari necessari.
- Assignar a una persona la responsabilitat de revisar el pla de còpies i de fer les còpies manuals i les restauracions.
- Establir el millor moment per fer les còpies.
- Decidir, tenint en compte el nivell de seguretat, si cal emmagatzemar les dades en una ubicació diferent a l'entorn de treball.

Problemes amb l'Exchange

La còpia de seguretat de servidor del Windows del Windows Server 2008, a diferència de versions anteriors, ja no és compatible amb les restauracions o les còpies de seguretat de l'Exchange. Ara hauríeu d'utilitzar alguna aplicació que hi fos compatible, com el Microsoft System Center Data Protection Manager.

La característica *Còpies de seguretat* del Microsoft Windows Server 2008 consta d'un complement Microsoft Management Console (MMC), eines de la línia d'ordres i *cmdlets* del Windows PowerShell. Tots aquests elements proporcionen una solució completa per a les necessitats diàries de còpia de seguretat i recuperació. A més, podeu usar còpies de seguretat del Windows Server per fer una còpia de seguretat d'un servidor complet, de volums seleccionats, de l'estat del sistema o d'arxius i carpetes específics. També les podeu utilitzar per crear una còpia de seguretat amb la finalitat de fer una reconstrucció completa.

Podeu fer servir *Còpies de seguretat* del Microsoft Windows Server 2008 per crear i administrar còpies de seguretat de l'equip local o d'un equip remot. També pot programar còpies de seguretat perquè s'executin de manera automàtica.

Tipus de còpies de seguretat

Hi ha cinc tipus bàsics de còpies de seguretat en el Microsoft Windows Server 2008, cosa que significa que heu d'estudiar quin format és el més adient per al vostre sistema. Tot seguit s'expliquen breument les diferents formes de que disposa Microsoft Windows Server 2008 de realitzar còpies de seguretat:

- **Normal/Completa:** es copien tots els fitxers seleccionats, independentment de si els arxius o els directoris estan preparats per ser copiats. En cas de copiar un fitxer no preparat, l'atribut A es desactiva.
- **Còpia:** es copien tots els fitxers seleccionats, independentment de si els arxius o els directoris estan preparats per ser copiats. En cas de copiar un fitxer no preparat, l'atribut A no canvia, cosa que permet fer altres tipus de còpia de seguretat més tard.
- **Diferencial:** es copien els arxius modificats després de l'última còpia.
- **Incremental:** es copien els arxius modificats després de l'última còpia normal o incremental. Quan es fa la còpia, l'atribut A es desactiva fins que no es modifica el fitxer.
- **Diària:** si un arxiu ha estat modificat el mateix dia en què es fa la còpia de seguretat, s'hi inclou. No afecta l'atribut A.

Cal no confondre els conceptes de *còpia diferencial* i *còpia incremental*. Les còpies diferencials inclouen tots els fitxers que s'hagin modificat des de l'última còpia, mentre que les còpies incrementals només inclouen els fitxers que s'hagin modificat des de la còpia completa o incremental més recent. La grandària d'una còpia incremental normalment és inferior a la d'una còpia completa.

Abans de crear una còpia de seguretat, d'un tipus o d'un altre, cal analitzar una sèrie de factors:

- **Quantitat de dades:** si la quantitat de dades a emmagatzemar és molt gran, caldrà tenir preparat tot el maquinari necessari.
- **Fiabilitat dels equips i del programari:** el preu dels equips i del programari pot determinar quins equipaments i quin suport cal utilitzar. És important considerar la fiabilitat de tot el conjunt.
- **Ampliació:** no us podeu arriscar que el vostre disseny quedi petit. Cal, doncs, que el vostre disseny de còpies s'adapti sense problemes a les necessitats del sistema.
- **Velocitat:** normalment l'alta velocitat va lligada a preus alts. D'aquesta manera, heu de valorar si la vostra organització necessita invertir pressupost per reduir el temps que es triga a fer les còpies i el que s'inverteix a fer les recuperacions de les dades.
- **Cost econòmic:** és un factor molt important, ja que pot marcar la qualitat del vostre disseny.

Atribut

Arxiu llest per arxivar-se és un atribut (anomenat A) dels fitxers i les carpetes. Aquest atribut indica si l'element s'ha d'incloure en la còpia de seguretat.

Utilització d'instantànies

Recuperar còpies de seguretat quan hi ha hagut una pèrdua de dades pot significar una inversió de temps i de recursos del sistema força gran. El Microsoft Windows Server 2008 permet simplificar aquesta feina mitjançant una eina que fa instantànies.

Una **instantània** és una còpia de seguretat, que es crea amb una freqüència determinada, dels arxius als quals els usuaris poden accedir directament mitjançant les carpetes compartides.

Per poder crear instantànies és imprescindible treballar amb volums NTFS, ja que les instantànies s'han de crear en tots els volums de què es disposi.

Per defecte, es creen dues còpies de seguretat diàriament de dilluns a divendres, l'una a les 07.00 i l'altra a les 00.00. L'espai lliure mínim necessari per crear instantànies és de 100 MB, però cal tenir molt en compte que aquesta quantitat depèn bàsicament de la quantitat de dades emmagatzemades en les carpetes compartides dels volums. Podeu configurar una mida màxima de les còpies de seguretat per tal de controlar encara més el comportament del sistema.

Per comprovar la configuració de les instantànies podeu fer el següent:

1. Cliqueu amb el botó dret del ratolí a sobre de la icona del disc que us interressi.
2. Seleccioneu *Propietats* i cliqueu a *Instantànies*.
3. Escolliu *Seleccioni un volum*.

La informació que hi trobareu és la següent:

- **Volum:** és l'etiqueta que identifica el volum NTFS.
- **Hora de la propera execució:** indica quan es generarà la pròxima còpia instantània. Es pot deshabilitar.
- **Recursos compartits:** indica la quantitat de carpetes compartides que hi ha en el volum.
- **Utilitzat:** indica la quantitat d'espai del disc que utilitzen les instantànies.

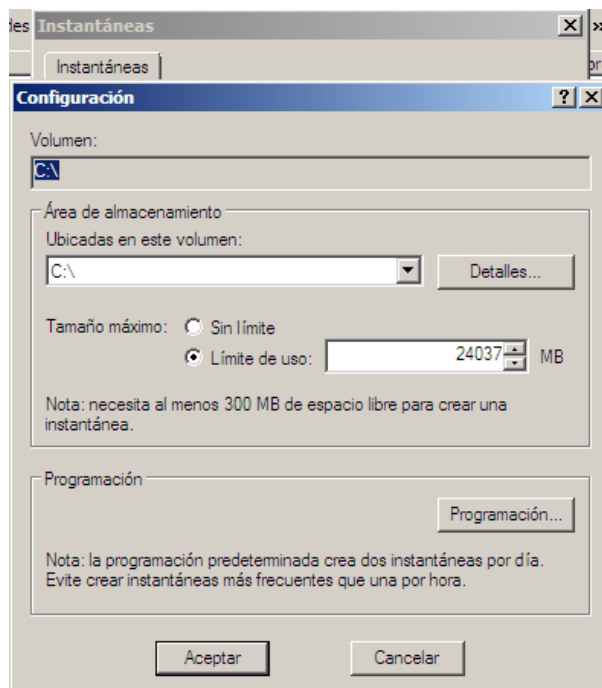
Per restaurar una instantània només cal fer tres passos:

1. Cliqueu amb el botó dret a sobre del recurs compartit que vulgueu revisar i seleccioneu *Propietats*.
2. Feu clic a la fitxa *Versions anteriors*.
3. Podeu seleccionar la versió de la carpeta dins de la fitxa *Versions prèvies*. Podeu comprovar que les versions contenen data i hora.

Les instantànies que es creen amb el Windows Server 2003 es perden quan s'inicia l'equip amb el Windows Vista o el Windows Server 2008.

La figura 1.4 mostra la finestra de configuració de les instantànies. Podeu comprovar que aquesta eina tan útil es configura d'una manera molt senzilla.

FIGURA 1.4. Configurant una instantània



Hi ha tres accions que podeu fer sobre les instantànies:

- **Obrir:** accedireu al contingut emmagatzemat a la carpeta.
- **Copiar:** es pot fer una còpia de l'arxiu de la instantània en una carpeta.
- **Restaurar:** permet tornar la carpeta a l'estat en què estava en el moment de fer la instantània.

També és possible tornar un volum sencer a l'estat en què estava en el moment de fer una determinada instantània, sempre que el volum en qüestió no sigui de sistema. Per fer aquesta acció cal seguir aquests passos:

1. Obriu l'administració de l'equip.
2. Expandiu el node *Emmagatzematge* i cliqueu amb el botó dret a *Administració de disc*.
3. Seleccioneu *Totes les tasques* i *Configurar instantànies*.
4. Cliqueu a la fitxa *Instantànies* i escolliu el volum de la llista *Seleccioni un volum*.
5. Escolliu la instantània que us interessi dins l'apartat *Instantànies del volum seleccionat* i premeu *Revertir*.
6. Feu clic a *Aceptar* per tancar el quadre de diàleg, un cop confirmades les opcions que hi apareixen.

Per eliminar una instantània cal fer el següent:

1. Obriu l'administració de l'equip.
2. Expandiu el node *Emmagatzematge* i cliqueu amb el botó dret a *Administració de discos*.
3. Seleccioneu *Totes les tasques* i *Configurar instantànies*.
4. Cliqueu a la fitxa *Instantànies* i escolliu el volum de la llista *Seleccioni un volum*.
5. Escolliu la instantània que us interessi dins l'apartat *Instantànies del volum seleccionat* i premeu *Eliminar ara*.

Les instantànies també es poden deshabilitar. Cal seguir aquests sis passos:

1. Obriu l'administració de l'equip.
2. Expandiu el node *Emmagatzematge* i cliqueu amb el botó dret a *Administració de discos*.
3. Seleccioneu *Totes les tasques* i *Configurar instantànies*.
4. Cliqueu a la fitxa *Instantànies* i escolliu el volum de la llista *Selecciona un volum*.
5. Feu clic a *Deshabilitar* i confirmeu les accions.
6. Premeu *Acceptar* per tancar el quadre de diàleg.

Còpies de seguretat amb el Microsoft Windows Server 2008

Per poder fer còpies de seguretat i restauració heu de disposar de diversos permisos i drets d'usuari. L'usuari administrador i el grup d'operadors de còpies de seguretat tenen autoritat total per copiar i restaurar qualsevol tipus de fitxer, independentment dels permisos que tinguin els fitxers i de qui en sigui el propietari. El propietari d'un arxiu i els usuaris que tinguin permisos per controlar aquests arxius podran fer còpies de seguretat, però només dels fitxers que siguin de propietat o que tinguin els permisos s'escriptura, lectura i execució, modificació o control total.

Les còpies de seguretat proporcionen extensions per gestionar uns quants tipus de dades especials:

- **Dades d'estat del sistema:** són els arxius imprescindibles del sistema per poder recuperar el sistema local.
- **Dades d'aplicació:** són els arxius imprescindibles de les aplicacions per poder recuperar-les si fos necessari.

Si inicieu les còpies de seguretat del Microsoft Windows Server 2008, us connectareu a l'equip local. De totes maneres, si necessiteu accedir a un equip remot, podeu fer el següent:

1. Inicieu les còpies de seguretat del Microsoft Windows Server 2008.
2. Seleccioneu l'opció *Connectar-se a un altre equip* del plafó d'accions.
3. Escolliu *Un altre equip*.
4. Introduïu el nom del servidor o l'adreça IP.
5. Premeu *Finalitzar* per acabar d'establir la connexió amb l'equip remot.

Instal·lar la característica Còpies de seguretat del Microsoft Windows Server 2008

Còpies de seguretat de Windows Server és una característica del Microsoft Windows Server 2008 i no està instal·lada per defecte. Abans de poder fer una còpia de seguretat amb *Còpies de seguretat de Windows Server*, s'ha d'instal·lar la característica mitjançant l'administrador de servidors o mitjançant la utilitat de línia d'ordres *SERVERMANAGERCMD*:

```
C:\> servermanagercmd -install Backup-Features
```

Còpies de seguretat del Windows Server consta de dues característiques:

- Còpies de seguretat del Windows Server
- Les eines de línia d'ordres.

S'ha de tenir en compte que les eines de línia d'ordres fan referència a un conjunt de *cmdlets* del Windows PowerShell™, no a l'eina de línia d'ordres *WBADMIN.EXE*. Per tant, si decidiu instal·lar totes dues característiques, també haureu d'instal·lar la característica del Windows PowerShell.

La característica *Còpies de seguretat* del Microsoft Windows Server 2008 consta de quatre components:

- La interfície d'usuari del MMC (*WBADMIN.MCS*).
- La interfície de línia d'ordres (*WBADMIN.EXE*).
- El servei de còpies de seguretat (*WBENGINE.EXE*).
- El conjunt de *cmdlets* del Windows PowerShell.

Ordres del Wbadmin

El Microsoft Windows Server 2008 inclou la possibilitat d'utilitzar la línia d'ordres per administrar tots els aspectes de configuració de còpies de seguretat.

El **Wbadmin** permet fer còpies de seguretat i restaurar el sistema operatiu, els volums, els arxius, les carpetes i les aplicacions des de la línia d'ordres.

Per configurar una programació de còpia de seguretat, heu de ser membres del grup d'administradors. Per dur a terme totes les altres funcions amb aquesta ordre, heu de ser membres dels operadors o el grup d'administradors, o heu d'haver delegat els permisos adequats.

Podeu executar l'ordre *wbadmin* des de la línia d'ordres.

Des de la línia d'ordres podeu executar *Wbadmin* amb una sèrie d'instruccions que li donen molta versatilitat. Aquestes ordres es descriuen en la taula 1.4:

TAULA 1.4. Ordres relacionades amb wbadmin

Ordre	Descripció
<i>Wbadmin enable backup</i>	Configura i permet una programació de còpia de seguretat diària. Aquesta ordre només s'aplica al Windows Server 2008.
<i>Wbadmin disable backup</i>	Desactiva les còpies de seguretat diàries. Aquesta ordre només s'aplica al Windows Server 2008.
<i>Wbadmin start backup</i>	S'inicia una còpia de seguretat. Si s'utilitza sense paràmetres, fa servir la configuració de la programació de còpia de seguretat diària.
<i>Wbadmin stop job</i>	Atura la còpia de seguretat que s'està executant o l'operació de recuperació.
<i>Wbadmin get versions</i>	Llista els detalls de còpies de seguretat de l'equip local o, si s'especifica una altra ubicació, des d'un altre equip.
<i>Wbadmin get items</i>	Enumera els elements inclosos en una còpia de seguretat específica.
<i>Wbadmin start recovery</i>	S'executa una recuperació dels volums, les aplicacions, els arxius o les carpetes que s'especifiquen. Aquesta ordre només s'aplica al Windows Server 2008.
<i>Wbadmin get status</i>	Mostra l'estat de la còpia de seguretat que s'està executant o l'operació de restauració.
<i>Wbadmin get disks</i>	Llista les unitats que estan en línia actualment. Aquesta ordre només s'aplica al Windows Server 2008.
<i>Wbadmin start systemstaterecovery</i>	Executa una recuperació de l'estat del sistema. Aquesta ordre només s'aplica al Windows Server 2008.
<i>Wbadmin start systemstatebackup</i>	S'executa una còpia de seguretat de l'estat del sistema. Aquesta ordre només s'aplica al Windows Server 2008.
<i>Wbadmin delete systemstatebackup</i>	Elimina una o més còpies de seguretat de l'estat del sistema. Aquesta ordre només s'aplica al Windows Server 2008.
<i>Wbadmin start sysrecovery</i>	Executa una recuperació del sistema complet (almenys tots els volums que contenen l'estat del sistema operatiu). Aquesta ordre només s'aplica al Windows Server 2008.

TAULA 1.4 (continuació)

Ordre	Descripció
<i>Wbadmin restore catalog</i>	Recupera un catàleg de còpia de seguretat des d'una ubicació d'emmagatzematge remot en cas que el catàleg de còpia de seguretat en l'equip local estigui malmès. Aquesta ordre només s'aplica al Windows Server 2008.
<i>Wbadmin delete catalog</i>	Elimina el catàleg de còpia de seguretat en l'equip local. Aquesta ordre només s'ha d'executar si el catàleg de còpia de seguretat en aquest equip està malmès i no té còpies de seguretat emmagatzemades en remot que es puguin utilitzar per restaurar el catàleg. Aquesta ordre només s'aplica al Windows Server 2008.

Per veure els identificadors del disc de tots els discos durs connectats, heu d'escriure *wbadmin get disks* en el símbol de sistema i, a continuació, prémer **ENTRAR**.

A continuació es farà una còpia de seguretat diària del directori actiu mitjançant la interfície gràfica:

1. Cliqueu a *Inici*.
2. Feu clic a *Eines administratives*.
3. Premeu *Còpies de seguretat del Windows Server*.
4. Confirmeu, si apareix el quadre de diàleg *Control de comptes d'usuari*, que l'acció que mostra és la correcta i, a continuació, feu clic a *Continuar*.
5. Cliqueu a *Acció*.
6. Feu clic a *Realitzar còpia de seguretat de programació*.
7. Comproveu la informació que apareix en el quadre *Introducció* i cliqueu a *Següent*.
8. Premeu *Sí* per confirmar que és la primera còpia de seguretat si és la primera vegada que feu una còpia de seguretat del controlador de domini.
9. Cliqueu a *Servidor complet (recomanat)* i premeu *Següent*.
10. Especifiqueu l'hora en què es farà la còpia de seguretat i, a continuació, premeu *Següent*.
11. Activeu la casella del disc de destinació i, a continuació, feu clic a *Següent*.
12. Premeu *Sí* per confirmar que el disc de destinació es tornarà a formatar.
13. Comproveu l'etiqueta del disc de destinació i, a continuació, premeu *Següent*.
14. Verifiqueu la informació de la pàgina *Resum* i, a continuació, cliqueu a *Finalitzar*.
15. Feu clic a *Tancar* a la pàgina *Confirmació*.

Per programar còpies de seguretat diàries del servei de domini mitjançant la línia d'ordres, haureu de seguir els passos següents:

IdentificadorDeDisc

L'*IdentificadorDeDisc* és la ubicació d'emmagatzematge extern per a la còpia de seguretat programada. *HH: MM* correspon a l'hora o hores en què es farà la còpia de seguretat diàriament, separada per comes i sense espais. *UnitatDOrigen_x* és el volum o volums imprescindibles de què es faran còpies de seguretat, separats per comes i sense espais.

1. Cliqueu a *Inici*, obriu el *Símbol del sistema* i, a continuació, premeu *Executar com a administrador*.
2. Confirmeu, si apareix el quadre de diàleg *Control de comptes d'usuari*, que l'acció que mostra és la correcta.
3. Feu clic a *Continuar*.
4. Obteniu el valor de *IdentificadorDeDisc* per usar-lo per a la destinació de la còpia de seguretat.
5. Escriviu en el símbol del sistema la línia *wbadmin enable backup -addtarget: IdentificadorDeDisc -schedule: HH:MM , HH:MM ,...HH:MM -include: UnitatDOrigen_1 ;, UnitatDeOrigen_2 ;,...UnitatDeOrigen_x:*.
6. Escriviu *S* si és la primera còpia de seguretat del controlador de domini que es crea.
7. Escriviu *S* per habilitar còpies de seguretat amb les opcions que vau configurar.
8. Escriviu *S* per donar format i fer servir els volums en la unitat especificada com a ubicació per emmagatzemar les còpies de seguretat programades.
9. Etiqueteu el disc de còpia de seguretat com s'especifica en la resposta de manera que pugui identificar-lo.

Per deshabilitar una còpia de seguretat programada, haureu de fer el següent:

1. Premeu *Realitzar còpia de seguretat de programació* a *Còpies de seguretat de Windows Server* i, a continuació, feu clic a *Aturar còpia de seguretat*.
2. Feu clic a *Següent* i, després, a *Finalitzar*.
3. Cliqueu a *Sí* per confirmar que voleu aturar la programació de la còpia de seguretat i, a continuació, premeu *Tancar*.

Xifratge i certificació

Moltes vegades és necessari xifrar les dades amb les quals es treballa per tal d'augmentar la seguretat. Tot i que *a priori* es podria pensar que això complica la tasca de fer còpies de seguretat i restaurar dades, la realitat és una altra.

Si utilitzeu programari aliè a Microsoft Windows Server per fer còpies de seguretat xifrant les dades o per recuperar dades xifrades, heu de tenir en compte que aquest programari ha de ser compatible amb el sistema *EFS*.

L'*EFS* (*encrypting file system*) és un sistema de xifratge d'arxius. El xifratge d'arxius s'aplica a carpetes o arxius. Tots els documents que siguin a l'interior d'una carpeta xifrada passaran per un procés de xifratge automàticament. Per poder accedir als continguts d'un arxiu xifrat caldrà desxifrar-lo.

Només hi ha una clau de xifratge per a cada fitxer xifrat. L'usuari que hagi xifrat un arxiu hi podrà accedir sempre que tingui la clau privada amb què el va xifrar o disposi d'un servei de gestió d'identificadors digitals.

L'*EFS* és el procés que s'encarrega del xifratge i el desxifratge.

Per defecte, la configuració de l'*EFS* permet que els usuaris xifrin arxius sense necessitat de tenir permisos especials.

Els fitxers es xifren mitjançant la clau privada/pública que l'*EFS* genera de manera automàtica per a cada usuari.

Si s'elimina un compte d'usuari amb el qual s'haguessin xifrat arxius o carpetes, s'hauria de fer servir un agent de recuperació.

Els **agents de recuperació** tenen accés als arxius de claus de xifratge necessaris per desbloquejar les dades que hi ha en fitxers xifrats, però no tenen accés a les claus privades.

Els agents de recuperació *EFS* es configuren en dos àmbits:

- **Domini:** per defecte, l'administrador del domini és l'agent de recuperació. Poden delegar els privilegis d'agent de recuperació a administradors de seguretat.
- **Equip local:** si l'equip forma part d'un grup de treball o d'una configuració independent, l'administrador de l'equip local serà l'agent de recuperació.

Per fer una còpia de seguretat dels certificats, primer caldrà afegir a la consola d'administració del Microsoft el complement *Certificats*:

El *PFX* (*personal information exchange*, intercanvi d'informació personal) és el format amb el qual s'emmagatzemen els certificats personals.

1. Cliqueu a *Inici*.
2. Escriu *mmc* en el quadre de text *Iniciar recerca* i polseu *ENTER*. Això ha de posar en marxa la consola d'administració.
3. Feu clic a *Afegir o eliminar complement* dins el menú *Arxiu*.
4. Seleccioneu *Certificats* a la llista *omplements disponibles* i cliqueu a *Afegir*.
5. Escolliu l'opció *El meu compte d'usuari* i cliqueu a *Finalitzar*. Premeu *Acceptar* per tancar el quadre de diàleg.

Ara ja serà possible fer una còpia de seguretat dels certificats. A continuació, caldrà seguir els passos següents:

1. Expandiu *Certificats: Usuari actual i personal* i seleccioneu *Certificats*.
2. Cliqueu amb el botó dret del ratolí al certificat que vulgueu guardar. Seleccioneu *Totes las tasques* i *Exportar*.

3. S'inicia un auxiliar.
4. Cliqueu a *Següent*.
5. Premeu *Sí, exportar la clau privada* i feu *Següent*.
6. Podeu acceptar els valors per defecte i fer clic a *Següent*.
7. Escriviu la contrasenya del certificat.
8. Seleccioneu la ubicació en què s'ha d'emmagatzemar el fitxer de certificat i cliqueu a *Següent*.
9. Premeu *Finalitzar* per acabar el procés.

Per restaurar un certificat personal caldrà fer el següent:

1. Estar en possessió del fitxer amb el certificat de xifratge (haurà de tenir l'extensió PFX).
2. Aneu a *Certificats* amb *El meu compte d'usuari*.
3. Expandiu *Certificats: usuari actual*.
4. Cliqueu a *Personal* amb el botó dret del ratolí, seleccioneu *Totes les tasques* i *Importar*.
5. S'iniciarà un auxiliar.
6. Feu clic a *Següent* i obriu l'arxiu que conté el certificat personal amb *Obrir*.
7. Premeu *Següent*.
8. Escriviu la contrasenya del certificat personal i feu *Següent*.
9. Cliqueu a *Finalitzar*. El certificat de xifratge ja s'haurà restaurat.

1.8 Auditoria de recursos en sistemes de propietat

Cal auditar tots els sistemes per conèixer l'ús dels recursos que té i l'estat en què es troba, tant pel que fa a la vessant física com pel que fa a la seguretat. L'auditoria de recursos augmenta l'eficàcia de la figura de l'administrador del sistema i permet que les accions d'aquest evitin problemes amb el sistema en el futur.

En el Microsoft Windows Server 2008, les **directives d'auditoria** es fan servir per garantir la integritat del sistema.

En els equips amb directori actiu, les directives d'auditoria es configuren mitjançant les directives de grup del directori actiu. En canvi, en els equips individuals es configuren mitjançant les directives locals.

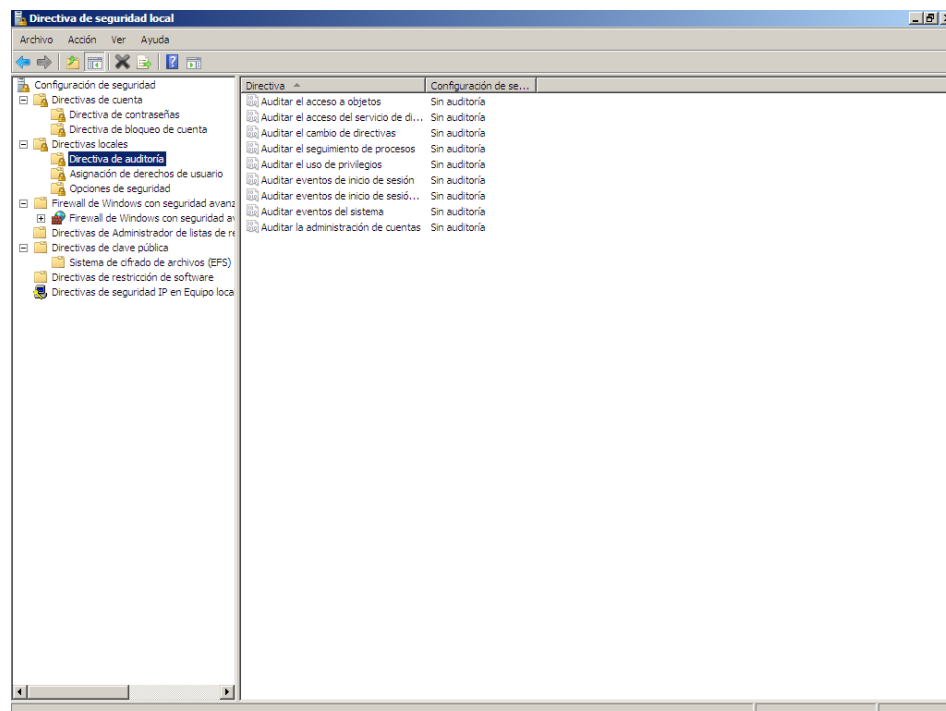
Per seleccionar la directiva d'auditoria heu de seguir els passos següents:

1. Obriu l'editor d'administració de directives de grup.
2. Expandiu *Configuració de l'equip*.
3. Expandiu *Directives*.
4. Expandiu *Configuració de Windows*.
5. Expandiu *Configuració de seguretat*.
6. Expandiu *Directives locals*.
7. Seleccioneu *Directiva d'auditoria*.

Les opcions d'auditoria es mostren en la figura 1.5 i són les següents:

- **Auditar l'accés a objectes:** audita l'ús d'alguns recursos del sistema, com ara els arxius, els directoris, els recursos compartits, les impressores o els objectes del directori actiu.
- **Auditar l'accés del servidor de directori:** audita els esdeveniments que es generen cada vegada que un usuari o un equip accedeix al directori.
- **Auditar el canvi de directives:** audita els canvis en els permisos d'usuari, auditoria i relacions de confiança.
- **Auditar el seguiment de processos:** audita els processos del sistema i els recursos que s'utilitzen.
- **Auditar l'ús de privilegis:** audita la utilització de permisos i privilegis d'usuari.
- **Auditar esdeveniments d'inici de sessió:** audita els esdeveniments lligats a l'inici i el tancament de connexions remotes als sistemes de xarxa.
- **Auditar esdeveniments d'inici de sessió de compte:** audita els esdeveniments relacionats amb l'inici i el tancament de sessions.

FIGURA 1.5. Directives d'auditoria



- **Auditar esdeveniments del sistema:** audita el procés d'arrencada, el tancament i el reinici del sistema, a més de les accions que afecten la seguretat del sistema o el registre de seguretat.
- **Auditar l'administració de comptes:** audita els esdeveniments que es generen quan es creen, es modifiquen o s'eliminen comptes d'usuari, d'equip o de grup.

Per configurar una directiva de seguretat heu de fer el següent:

1. Feu doble clic al damunt de la directiva que us interessi (o cliqueu-hi amb el botó dret i seleccioneu *Propietats*).
2. Seleccioneu *Definir aquesta configuració de directiva*.
3. Podeu marcar les caselles de verificació *Correcte*, *Error* o totes dues. La casella de verificació *Correcte* farà que es registrin els esdeveniments que es facin correctament, mentre que la casella de verificació *Error* farà que es registrin els esdeveniments que fallin.
4. Premeu *Acceptar* per finalitzar.

Si activeu aquesta directiva de seguretat, aconseguireu controlar la manera com s'auditarà l'ús dels fitxers i les carpetes. Només podreu utilitzar aquest tipus d'auditoria si el volum que conté la informació és NTFS. Per auditar arxius i carpetes haureu d'activar l'opció *Auditar l'accés a objectes*.

Cal que configureu l'auditoria d'arxius i carpetes seguint aquests passos:

1. Cliqueu amb el botó dret a sobre de l'arxiu o la carpeta que vulgueu auditar.
2. Premeu *Propietats*.
3. Cliqueu a *Seguretat* i premeu *Opcions avançades*.
4. S'obrirà un quadre que porta per títol *Configuració de seguretat avançada* per i el nom del fitxer o de la carpeta.
5. Premeu, a la fitxa *Auditoria*, el botó *Editar* per estudiar i configurar l'auditoria.
6. Cliqueu a sobre del botó *Aplicar* per especificar on es vigilaran els objectes.
7. Marqueu les caselles de verificació *Correcte*, *Incorrecte* o totes dues per a cadascun dels esdeveniments a vigilar.
8. Feu *Acceptar* per finalitzar.

Si activeu aquesta directiva de seguretat, aconseguireu controlar la manera com s'auditarà el canvi de valors d'una clau, quan s'eliminin les claus i quan es creïn subclaus. Per **auditar el registre** haureu d'activar l'opció *Auditar l'accés a objectes*.

Per configurar l'auditoria del registre, cal que seguiu els passos següents:

1. Obriu la línia d'ordres i escriviu *regedit*.
2. Marqueu la clau que voleu auditar.
3. Seccioneu *Permisos* dins el menú *Editar*.
4. Cliqueu a *Opcions avançades*.
5. Obriu la fitxa *Auditoria* en el quadre de diàleg *Configuració de seguretat avançada*.
6. Feu *Afegir*.
7. Escriviu *Tots* en el quadre de diàleg *Seleccionar Usuari, Equip o Grup*.
8. Feu clic a *Comprovar noms* i premeu *Acceptar*.
9. Seccioneu les accions que voleu supervisar.
10. Cliqueu a *Acceptar* per anar tancant tots els quadres de diàleg que resten oberts.

Si configureu l'opció *Auditar l'accés del servei de directori*, podreu auditar objectes del directori actiu. Per fer-ho, cal que seguiu aquests passos:

1. Aneu a *Usuaris i equips d'Active Directory* i assegureu-vos que l'opció *Característiques avançades* del menú *Veure* està marcada.

2. Cliqueu amb el botó dret del ratolí a l'objecte que voleu auditar i premeu *Propietats*.
3. Accediu a la fitxa *Seguretat* i cliqueu a *Opcions avançades*.
4. Feu clic a la fitxa *Auditoria* en el quadre de diàleg *Configuració de seguretat avançada*.
5. Seleccioneu els usuaris, els grups o els equips dels quals vulgueu auditar les accions mitjançant la llista *Entrades d'auditoria*.
6. Premeu *Eliminar* per eliminar comptes i *Afegir* per afegir-ne.
7. Seleccioneu el nom del compte, si n'afegiu un, en el quadre de diàleg *Seleccionar Usuari, Equip o Grup*.
8. Feu servir la llista *Aplicar a* per especificar on s'auditaran els objectes.
9. Marqueu les caselles de verificació *Correcte*, *Incorrecte* o totes dues per a cadascun dels esdeveniments que vulgueu auditar.
10. Cliqueu a *Acceptar* per finalitzar el procés.

2. Compartir recursos en xarxa i seguretat en sistemes lliures

La compartició de recursos en xarxa és una de les utilitats o raons principals perquè els sistemes operatius es connectin en xarxa. En l'àmbit del sistemes operatius, podem entendre el concepte de compartició de recursos des de diversos punts de vista.

Des del punt de vista del maquinari, compartir recursos fa referència a l'ús del maquinari per dos o més processos dins del sistema operatiu.

En aquesta unitat ens centrarem en la compartició des del punt de vista de les xarxes d'ordinadors.

Compartir recursos en xarxa implica configurar la xarxa de tal manera que els ordinadors que hi estan connectats puguin utilitzar els recursos de la resta, fent servir la xarxa com a mitjà de comunicació.

Es poden compartir tot tipus de recursos, encara que els més habituals són directoris i impressores. En els sistemes operatius lliures hi ha diversos protocols i aplicacions que ens permeten compartir recursos en xarxa, com el protocol NFS i el paquet de programari Samba.

2.1 Protocol NFS

El protocol NFS (*network file system* o sistema de fitxers per xarxa) és un protocol del nivell d'aplicació que s'utilitza en l'àmbit de les xarxes locals per compartir fitxers entre màquines de la mateixa xarxa. El protocol NFS es pot fer servir per defecte en la majoria de sistemes operatius GNU/Linux. Així, NFS fa possible que diversos sistemes GNU/Linux connectats a una mateixa xarxa puguin accedir a fitxers remots, en altres equips de la xarxa, com si es tractés de fitxers locals.

El sistema GNU/Linux només pot treballar amb una jerarquia de directoris. Per tant, si volem accedir a diferents sistemes d'arxius, particions de discos o CD-ROM, entre altres, primer hem de muntar aquests elements en algun punt de la jerarquia.

L'NFS ens proporciona un servei de xarxa que permet a un ordinador client muntar un sistema d'arxius remot, exportat per un altre ordinador servidor, i accedir-hi. Per tant, el protocol NFS funciona clarament sota una arquitectura client-servidor.

2.1.1 Usos del protocol NFS

El protocol NFS pot ser utilitzat amb múltiples finalitats, sempre dins de l'àmbit de compartició de recursos. Per això, en general, el protocol NFS és molt flexible i admet diferents possibilitats o escenaris de funcionament com, per exemple, els següents:

- Un servidor NFS pot exportar més d'un directori i atendre simultàniament diversos clients.
- Un client NFS pot muntar directoris remots exportats per diferents servidors.
- Qualsevol sistema GNU/Linux pot ser alhora client i servidor NFS.

Tenint en compte això, hi ha diversos usos típics de l'NFS en què aquest servei mostra la utilitat que té. En podem destacar les utilitats tradicionals següents:

1. **Centralització dels directoris de connexió dels usuaris (*home directory*).**
Quan en una xarxa local de màquines GNU/Linux es vol que els usuaris puguin treballar indistintament en qualsevol, és adequat situar els directoris de connexió de tots els usuaris en una mateixa màquina i fer que les altres muntin aquests directoris mitjançant NFS. Si aquest ús es combina amb l'autenticació d'usuaris en xarxa per mitjà de l'LDAP, en els sistemes GNU/Linux es pot implementar quelcom similar a un domini del Windows.
2. **Compartició de directoris d'ús comú.** Si diversos usuaris des de diferents màquines treballen amb els mateixos arxius, per exemple, d'un projecte comú, també és útil compartir els directoris en què hi ha aquests arxius. Aquesta opció comporta un estalvi de disc en les màquines locals, ja que les dades estan centralitzades en un lloc, de manera que diversos usuaris hi poden accedir i les poden modificar. Per tant, no és necessari replicar la informació.
3. **Situar programari en un sol ordinador de la xarxa.** És possible instal·lar programari en un directori del servidor NFS i compartir aquest directori via NFS. Si configurem els clients NFS perquè muntin aquest directori remot en un directori local, aquest programari estarà disponible per a tots els ordinadors de la xarxa.

4. Compartició per mitjà de la xarxa de dispositius d'emmagatzematge.

És possible compartir dispositius com ara particions de discos durs, CD-ROM, etc. Això pot reduir la inversió en aquests dispositius i millorar l'aprofitament del maquinari que hi ha en l'organització.

Totes les operacions sobre fitxers són síncrones. Això significa que l'operació només torna un resultat quan el servidor ha completat tot el treball associat a aquesta operació.

Per exemple, en cas d'una sol·licitud d'escriptura, el servidor escriurà físicament les dades en el disc i, si és necessari, actualitzarà l'estructura de directoris abans de tornar una resposta al client. Això garanteix la integritat dels fitxers.

2.1.2 Funcionament de l'NFS

En el sistema client, el funcionament de l'NFS es basa en la capacitat de traduir els accessos de les aplicacions a un sistema d'arxius en peticions al servidor corresponent per mitjà de la xarxa. Normalment aquesta funcionalitat del client està programada en el nucli de GNU/Linux, de manera que no necessita cap tipus de configuració.

Respecte al servidor, l'NFS s'implementa mitjançant dos serveis de xarxa, el **mountd** i l'**nfsd**. Vegem quines accions controla cadascun d'aquests serveis:

- **El servei mountd s'encarrega d'atendre les peticions remotes de muntatge, efectuades per l'ordre *mount* del client.** Entre altres coses, aquest servei s'encarrega de **comprovar** si la petició de **muntatge és vàlida** i de controlar sota quines condicions s'accedirà al directori exportat (només lectura, lectura/escriptura, etc.). Una petició es considera vàlida quan el directori sol·licitat ha estat explícitament exportat i el client té prou permisos per muntar aquest directori.
- **El servei nfsd s'encarrega**, una vegada un directori remot ha estat muntat amb èxit, **d'atendre i resoldre les peticions d'accés del client als arxius que hi ha en el directori.**

2.1.3 Instal·lació i configuració del client NFS

El client NFS no requereix ni instal·lació ni configuració, ja que els directoris remots es poden importar mitjançant l'ordre **mount**. També es pot fer servir el fitxer **/etc/fstab** si es vol que el directori es munti a l'inici. Les opcions de muntatge de cada directori es poden establir tant amb l'ordre **mount** com amb el fitxer **etc/fstab**. Amb aquestes opcions es particularitza el comportament que tindrà el sistema d'arxius una vegada s'hagi muntat en el directori corresponent.

Per exemple, per muntar un sistema de fitxers NFS mitjançant l'ordre *mount*, podem fer servir la línia següent:

```
1 sudo mount -t nfs 192.168.1.15:/home (servidor) /home (client)
```

Si es vol que el directori */home* es munti a l'inici de sessió, es pot afegir aquesta entrada permanent al fitxer */etc/fstab*:

```
1 192.168.1.15:/home /home nfs soft,users,suid,exec
```

L'opció *exec* permet executar programes a la carpeta muntada i l'opció *users* permet que els usuaris puguin utilitzar *mount* per muntar i desmuntar aquest recurs.

Per instal·lar el servidor NFS, cal executar l'ordre següent:

```
1 sudo apt-get install nfs-kernel-server
```

El paquet *nfs-kernel-server* depèn del paquet *nfs-common*, el qual alhora depèn del paquet *portmap*. Per tant, tots tres s'instal·laran conjuntament amb l'ordre anterior.

El servidor necessita, a més dels dos dimonis *mountd* i *nfsd*, un altre dimoni anomenat *portmap*. El funcionament dels dimonis *mountd* i *nfsd* es basa en el dimoni *portmap*. Així, doncs, la configuració d'un servidor NFS només necessita tenir disponibles aquests serveis i iniciar-los en el nivell d'execució 3 (o 5 o bé tots dos) de la màquina.

Per tal de parar, reiniciar, etc. el servei NFS, es poden fer servir els *scripts* del servei que hi ha a la carpeta */etc/init.d*.

Una vegada actius els serveis NFS, el servidor ha d'indicar explícitament quins directoris vol que s'exportin, a quines màquines s'han d'exportar i amb quines opcions s'ha de fer. Per això hi ha un fitxer de configuració denominat */etc/exports*. Vegem un exemple d'aquest fitxer:

```
1 # /etc/exports: the access control list for filesystems which may be exported
2 #to NFS clients. See exports(5).
3 # Example for NFSv2 and NFSv3:
4 #/srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,
5   no_subtree_check)
6 # Example for NFSv4:
7 # /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
8 # /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
```

Cada línia del fitxer */etc/exports* especifica un directori a exportar, juntament amb una llista d'autoritzacions. És a dir, determina quins ordinadors podran muntar aquest directori i amb quines opcions ho podran fer. Cada element de la llista d'ordinadors pot especificar un sol ordinador (mitjançant un nom simbòlic o una adreça IP) o un grup d'ordinadors (mitjançant l'ús de caràcters comodí, com ** o ?*). Quan no s'especifica l'ordinador o el rang, significa que el directori corresponent s'exporta a tots els ordinadors de la xarxa.

Les **opcions de muntatge més importants** que es poden especificar **entre parèntesis** per a cada ordinador o grup són les següents:

- **()**: aquesta opció estableix les opcions que l'NFS assumeix per defecte.
- **ro**: el directori s'exporta com un sistema d'arxius només de lectura (opció per defecte).
- **rw**: el directori s'exporta com un sistema d'arxius de lectura/escriptura.
- **root_squash**: els accessos des del client amb **UID = 0 (root)** es converteixen en el servidor en accessos amb **UID d'un usuari anònim** (opció per defecte).
- **no_root_squash**: es permet l'accés des d'un **UID = 0** sense conversió. És a dir, els accessos d'arrel (*root*) en el client es converteixen en accessos d'arrel en el servidor.
- **all_squash**: tots els accessos des del client, amb qualsevol UID, es transformen en accessos d'usuari anònim.
- **anonuid, anongid**: quan s'activa l'opció **root_squash** o **allsquash**, els accessos anònims utilitzen normalment l'UID i el GID primari de l'usuari denominat **nobody** si aquest usuari existeix en el servidor (opció per defecte). Si es volen utilitzar altres formes d'identificació, els paràmetres **anonuid** i **anongid** estableixen, respectivament, quins UID i GID tindrà el compte anònim que el servidor utilitzarà per accedir al contingut del directori.
- **noaccess**: impedeix l'accés al directori especificat. Aquesta opció és útil per impedir que s'accedeixi a un subdirector d'un directori exportat.

És important destacar que cada vegada que es modifica aquest fitxer, el servidor NFS s'ha d'actualitzar mitjançant l'ordre **exportfs -ra** a fi que s'activin els canvis.

En la pàgina de manual *exports* hi ha una llista completa de les opcions de muntatge i el significat que tenen. Per accedir-hi, cal utilitzar l'ordre **man exports**.

És molt important remarcar que **no hi ha cap procés d'acreditació d'usuaris en l'NFS**, de manera que l'administrador ha de decidir amb cautela a quins ordinadors exporta un determinat directori.

Un directori sense restriccions s'exporta, en principi, a qualsevol altre ordinador connectat al servidor per mitjà de la xarxa (també Internet). Si en un ordinador client NFS hi ha un usuari amb un UID igual a *X*, aquest usuari accedirà al servidor NFS, per defecte, amb els permisos de l'usuari amb l'UID igual a *X* del servidor, encara que es tracti d'usuaris distints.

Control NFS

El mecanisme per controlar quines màquines de la xarxa poden disposar dels fitxers compartits i quines no consistiria a utilitzar els fitxers **/etc/hosts.allow** i **/etc/hosts.deny**.

La manca d'autenticació d'usuaris és un dels majors inconvenients del protocol NFS i per aquesta raó cada vegada s'utilitzen més altres sistemes de compartició de fitxers com, per exemple, el Samba.

2.2 Què és el Samba?

Podem definir el Samba de la manera següent:

Paquet de programari que implementa en sistemes basats en Unix, com GNU/Linux, una dotzena de serveis i una dotzena de protocols, entre els quals hi ha el NetBIOS sobre TCP/IP i l'SMB. Aquests serveis i protocols permeten que els equips d'una xarxa local comparteixin fitxers i impressores.

Els dos protocols més importants que formen el paquet de programari Samba són el NetBIOS i l'SMB.

2.2.1 Protocol NetBIOS

NetBIOS sobre NetBEUI

Als anys noranta, els sistemes Windows van utilitzar el protocol NetBIOS sobre el NetBEUI com a sistema que proporcionava serveis de noms, serveis de sessió i serveis de distribució de datagrames sense connexió. El Windows no el suporta des de la versió 2000, tot i que s'hi pot instal·lar.

El NetBIOS (*network basic input/output system*) és un protocol del nivell de sessió (model OSI) que s'utilitza en xarxes locals i que s'encarrega de garantir l'accés a serveis de xarxa entre màquines, independentment del maquinari de xarxa que facin servir.

Principalment, el NetBIOS s'utilitza per identificar amb un nom els equips connectats per mitjà de xarxes locals, amb la finalitat d'establir una sessió i mantenir la connexió entre equips de la xarxa. El NetBIOS no pot transportar per si mateix les dades entre els nodes de la LAN. Per això ha de funcionar amb altres protocols com el TCP/IP, l'IPC/IPX i el NetBEUI.

El NetBIOS ha de ser transportat per altres protocols perquè, en operar en la capa cinc del model OSI, no proveeix un format de dades per a la transmissió. Aquest format, doncs, el proveeixen aquests altres protocols.

El NetBIOS permet comunicació orientada a connexió (TCP) i no orientada a connexió (UDP). Suporta tant difusió (*broadcast*) com transmissió a grups (*multicast*), a més de quatre tipus de serveis diferents:

- Serveis generals
- Servei de noms
- Servei de sessió
- Servei de datagrames

Quan un programa d'aplicació necessita els serveis NetBIOS, el programa executa una interrupció de programari específica. Aquesta interrupció adreça el control del microprocessador al programari de l'adaptador de xarxa, el qual processa

El NetBIOS al Windows

En els sistemes Windows el protocol NetBIOS s'ha fet servir principalment per compartir arxius i impressores, i també per veure els recursos disponibles en "Entorn de xarxa". Bona part de les crítiques de seguretat cap als entorns Windows se centren en el protocol NetBIOS. Per motius de seguretat, aquest protocol s'ha de deshabilitar sempre que no sigui imprescindible.

l'ordre. Quan un programa d'aplicació emet una interrupció NetBIOS, el servei NetBIOS requereix un servei de xarxa. La interfície NetBIOS defineix exactament la manera com els programes d'aplicació poden fer servir la interrupció NetBIOS i els serveis que proporciona.

2.2.2 Protocol SMB

El protocol SMB (*server message block*) el va inventar originalment IBM, però avui dia la versió més comuna és la que Microsoft ha modificat àmpliament. El 1998 Microsoft va reanomenar aquest protocol CIFS (*common Internet file system*) i hi va afegir més característiques.

L'SMB és un protocol del nivell d'aplicació de tipus client-servidor en què l'ordinador que fa de servidor ofereix recursos (arxius, impressores, etc.) que els ordinadors clients poden fer servir remotament per mitjà de la xarxa.

L'SMB forma part dels protocols anomenats petició-resposta, ja que les comunicacions sempre s'inicien des del client com una petició de servei al servidor. El servidor la processa i torna una resposta a aquest client. La resposta del servidor pot ser positiva o negativa, en funció del tipus de petició, la disponibilitat del recurs, els permisos del client, etc.

El protocol **SMB incorpora dos nivells de seguretat**. Són els següents:

- **Share-level:** protecció en el recurs compartit. **S'assigna una contrasenya a cada recurs compartit.** L'accés a cada recurs es permet en funció del coneixement d'aquesta contrasenya. Va ser el primer sistema de seguretat utilitzat amb l'SMB (propi del Windows 3.11/95).
- **User-level:** la protecció s'aplica a cada recurs compartit i es basa en **drets d'accés de l'usuari**. Els usuaris s'han **d'autenticar** en el servidor. Un cop identificat el client, se li assigna un UID que s'utilitza en els subsegüents accessos al servidor (propi dels dominis Windows NT o 2000).

El protocol SMB s'implementa habitualment amb el NetBIOS sobre el TCP/IP. Aquesta alternativa s'ha convertit en l'estàndard de fet per compartir recursos entre sistemes Windows.

El Samba incorpora tres nivells més de seguretat que l'SMB.

2.2.3 Característiques del Samba

El Samba és una implementació lliure del protocol SMB amb les extensions de Microsoft.

Nom Samba

Inicialment el Samba s'anomenava smbserver, però li van haver de canviar el nom a causa de problemes amb una altra empresa que tenia aquesta marca registrada. Per obtenir el nom nou van buscar una paraula al diccionari de GNU/Linux que contingués les lletres SMB:

```
1 grep -i '^s.*m.*b' /usr/dict/words
2 salmonberry
3 samba
4 sawtimber
5 scramble
```

Essencialment, el Samba el constitueixen dos dimonis anomenats *smbd* i *nmbd*. També fa servir el protocol *windbindd*, encara que no és essencial per al funcionament de l'aplicació. Els dimonis utilitzen el protocol NetBIOS per accedir a la xarxa, de manera que poden conversar amb ordinadors Windows.

El dimoni *smbd* s'encarrega d'oferir els serveis d'accés remot a fitxers i impresores (per fer-ho, implementa el protocol SMB), a més d'autenticar i autoritzar usuaris. El dimoni *smbd* ofereix les dues maneres de compartició de recursos del Windows: compartició basada en usuaris (*user-level*) o compartició basada en recursos (*share-level*).

El dimoni *nmbd* permet que el sistema GNU/Linux participi en els mecanismes de resolució de noms propis del Windows, la qual cosa inclou el següent:

- L'anunci en el grup de treball.
- La gestió de la llista d'ordinadors del grup de treball.
- La contestació a peticions de resolució de noms.
- L'anunci dels recursos compartits.

D'aquesta manera, els sistemes GNU/Linux poden aparèixer en l'"Entorn de xarxa" de les màquines Windows, com qualsevol altre sistema Windows, i publicar la llista de recursos que ofereix a la resta de la xarxa.

El dimoni *windbindd* proporciona el servei windbind, el qual resol els problemes d'inici de sessió unificats. El servei *windbind* es fa servir per resoldre informació d'usuaris i grups corresponent a un servidor Windows NT. El Winbind proporciona tres funcions separades:

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

El funcionament en conjunt d'aquests serveis permet transferir fitxers i informació entre sistemes GNU/Linux i Windows, els quals donen suport als protocols SMB/CIFS.

Gràcies al Samba, en una xarxa hi pot haver equips amb Windows i equips amb GNU/Linux de manera que puguin intercanviar informació en carpetes compartides i compartir impressores, tal com es faria si tots els equips fossin Windows o GNU/Linux.

L'avantatge principal del paquet de programari Samba és que és pràcticament equivalent a qualsevol servidor SMB/CIFS (Windows NT o 2000, servidor Netware, servidor NFS UNIX, etc.) i, a més, és programari lliure i gratuït. En la taula 2.1 es mostren els diversos rols o serveis per als quals es pot utilitzar el Samba.

TAULA 2.1. Possibles rols d'un servidor Samba

Usos del Samba	
Servidor de fitxers	Sí
Servidor d'impressores	Sí
Servidor DFS de Microsoft	Sí
Controlador primari de domini (PDC)	Sí
Controlador de còpia de seguretat o <i>backup</i> del domini (BDC)	No
Controlador de domini directori actiu	No
Autenticació Windows 95/98/Me	Sí
Autenticació Windows NT/2000/XP	Sí
Local master browser	Sí
Local backup browser	Sí
Master browser de domini	Sí
Servidor WINS primari	Sí
Servidor WINS secundari	No
Autenticació GNU/Linux	Sí
Integració LDAP	Sí

Podeu trobar més informació sobre la compartició de recursos entre sistemes GNU/Linux i Windows en la unitat "Integració de sistemes operatius"

Primordialment, el Samba permet que màquines GNU/Linux i Windows coexisteixin en la mateixa xarxa. De totes maneres, també es pot fer servir per compartir recursos en una xarxa formada íntegrament per màquines amb sistemes GNU/Linux.

2.3 Seguretat en el Samba

Abans d'iniciar el procés d'instal·lació i configuració del servidor i del client Samba, analitzarem els mecanismes de seguretat que ens proporciona el paquet de programari.

El Samba, a més dels nivells de seguretat que proporciona el protocol SMB (*share* i *user*), incorpora tres subnivells de seguretat en el nivell d'usuari. Així, en total podem fer servir els nivells de seguretat següents:

- **share:** cada recurs compartit utilitza una paraula de pas. Tothom que sàpiga aquesta paraula de pas pot accedir al recurs.
- **user:** cada recurs compartit del grup de treball està configurat per permetre l'accés a un grup específic d'usuaris. En cada connexió inicial a un servidor Samba autentica l'usuari.
- **server:** el sistema és idèntic a l'anterior, però s'utilitza un altre servidor per obtenir la informació dels usuaris.
- **domain:** el Samba es converteix en membre d'un domini del Windows NT i utilitza un PDC (*primary domain controller*) o un BDC (*backup domain controller*) per implementar l'autenticació. Un cop autenticat l'usuari manté un testimoni o *token* amb la informació de l'usuari, a partir de la qual es podrà determinar a quins recursos té accés.
- **ADS:** el Samba es comporta com a membre d'un domini de directori actiu i, per tant, requereix un servidor W2000 Server o W2003 Server.

2.3.1 Share-level security

En el nivell de seguretat *share*, el client s'autentica de manera separada per a cada recurs al qual vol accedir. El funcionament d'aquest nivell de seguretat determina que cada recurs compartit tingui associat una paraula de pas amb independència de l'usuari que es connecti.

Tot i que els sistemes Windows associen la contrasenya a un recurs, el Samba utilitza l'esquema d'autenticació de GNU/Linux, en què la parella a autenticar és usuari-contrasenya i no pas recurs-contrasenya.

El client envia una paraula de pas cada cop que vol accedir a un recurs, però no envia cap usuari. Els sistemes GNU/Linux, no obstant això, sempre han d'utilitzar un usuari per autenticar-se. Així, doncs, quin usuari s'envia per fer la connexió?

Depèn dels paràmetres especificats en la configuració global del servidor, de manera que hi ha diverses possibilitats. Per exemple:

- Si s'utilitza el paràmetre **guest only** en la configuració del recurs compartit al Samba, aleshores només es fa servir l'usuari convidat especificat amb el paràmetre **guest account**. Per defecte, *nobody*.
- Els sistemes Windows moderns i el Samba envien com a usuari per defecte l'usuari que està utilitzant, en el moment d'accedir al recurs, la màquina client.

- També es poden enviar a altres usuaris, com un inici de sessió previ, el nom del recurs al qual es vol accedir, el nom NetBIOS del client o els usuaris del paràmetre *user list*, depenent de les diferents configuracions.

El *guest only* i el *guest account* són paràmetres que hi ha en el fitxer de configuració */etc/samba/smb.conf*, els quals analitzem en l'apartat "Configuració d'un servidor Samba".

Per tant, en iniciar una sessió, els clients passen un usuari al servidor (sense contrasenya). El Samba emmagatzema aquest usuari en una llista de possibles usuaris. Quan el client especifica una contrasenya i accedeix a un recurs concret, el Samba apunta el nom del recurs juntament amb els usuaris vàlids que apareguin en el fitxer */etc/samba/smb.conf* en la llista anterior. Seguidament, es comprova la paraula de pas de cadascun dels possibles usuaris. Si hi ha coincidència, aleshores s'autentica amb aquest usuari.

Quan aquesta llista no està disponible, aleshores el Samba envia una petició al sistema GNU/Linux per trobar l'usuari a qui correspon la contrasenya. Això es fa mitjançant l'NSS i la configuració del fitxer */etc/nsswitch.conf*.

2.3.2 User-level security

L'opció *user* és l'opció per defecte i també és la més simple. El client s'identifica en el nivell de sessió amb un usuari i una paraula de pas. El servidor pot acceptar o denegar la sessió, però no necessàriament ha de saber a quins recursos vol accedir el client. En aquest nivell, doncs, per controlar l'accés als recursos el servidor només es pot basar en els elements següents:

- L'usuari i la paraula de pas.
- El nom de la màquina client.

Si s'accepta la sessió, el client pot accedir als recursos remots sense haver de tornar a especificar la paraula de pas. En aquest mètode és imprescindible que els usuaris apareguin com a usuaris de GNU/Linux i del Samba.

Aquest mètode de seguretat no és gaire recomanable si es volen compartir recursos de xarxa de manera anònima. De totes maneres, hi ha la possibilitat de generar un mode híbrid entre els nivells *user* i *share* mitjançant el paràmetre *map to guest* de les opcions globals del fitxer */etc/samba/smb.conf*. Aquest paràmetre pot tenir diversos valors i, per tant, el servidor també pot tenir diversos comportaments. Així, si establim un valor com *Bad User*, estem configurant un mètode en el qual, si la contrasenya de l'usuari falla, se'l rebutjarà, però si l'usuari no existeix, passarà automàticament a ser un usuari convidat, és a dir, s'activarà com a usuari *guest*.

2.3.3 Domain security mode (user-level security)

En el cas *domain*, la base de dades d'usuaris està centralitzada en un controlador de domini i tots els membres d'un domini la comparteixen. Un servidor controlador primari de domini (PDC) és el responsable de mantenir la integritat de la base de dades de comptes de seguretat. Els *backup domain controllers* (BDC) només proveeixen serveis d'autenticació i inici de sessió o *login*.

Aleshores, amb aquest sistema de seguretat el servidor Samba és converteix en un servidor membre del domini, controlador primari de domini (PDC) o no. Per aquesta raó, totes les màquines que participen en el domini han de tenir un compte de màquina en la base de dades de seguretat.

El nivell de seguretat de domini utilitza un sistema de seguretat basat en l'usuari (*user-level security*), en el qual fins i tot les màquines s'han de validar en l'arrencada del sistema. El compte de màquina és un compte d'usuari més del Samba. L'única diferència que hi ha respecte al compte d'usuari és que el de màquina acaba en \$. D'aquesta manera, el nom del compte serà *NETBIOS_NAME\$*.

La contrasenya es genera de manera aleatòria i només la coneixen els controladors de domini i la màquina membre. Si la màquina no es pot validar en iniciar el sistema, els usuaris no podran entrar al domini mitjançant aquesta màquina, ja que es considerarà que no és de confiança (*not trusted machine*).

Hi ha tres configuracions possibles de membres de domini:

- *Primary domain controller* (PDC).
- *Backup domain controller* (BDC).
- *Domain member server* (DMS).

2.3.4 ADS security mode (user-level security)

Les màquines amb una versió del Samba posterior a la 2.2 es poden unir a un domini de directori actiu. Això és possible si el servidor funciona en mode natiu, ja que el directori actiu en aquest mode accepta perfectament membres de domini de l'estil NT4.

A partir de la versió 3 del Samba, a més, el servidor Samba es pot afegir com a membre natiu de directori actiu. Això pot ser útil si hi ha una política de seguretat que prohibeix els protocols d'autenticació d'NT.

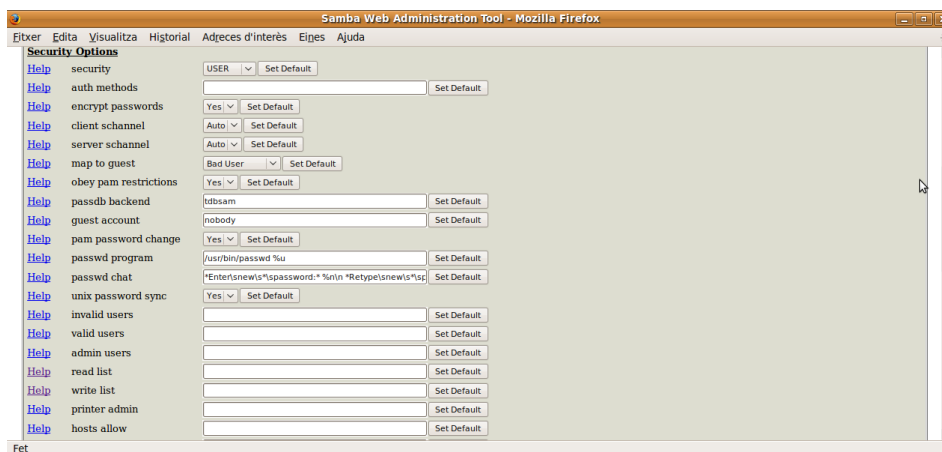
2.3.5 Server security (user-level security)

Aquest mode es manté per compatibilitat enrere i existeix perquè abans era el mode que s'utilitzava quan el Samba no podia actuar com un PDC. No és gens recomanable fer servir aquesta opció perquè té moltes deficiències.

2.3.6 Opcions de seguretat en l'apartat GLOBALS del fitxer de configuració

En el fitxer de configuració del Samba `/etc/samba/smb.conf` es poden especificar una gran quantitat de paràmetres per garantir tant la seguretat d'accés al servidor com la seguretat d'accés als recursos compartits. Aquests paràmetres es mostren en les seccions *GLOBALS* i *SHARES* de l'eina gràfica Swat. En la figura 2.1 es mostra un exemple de les diverses opcions de seguretat amb l'aplicació Swat.

FIGURA 2.1. Opcions de seguretat de Samba



El significat d'alguns d'aquests paràmetres el veurem en l'apartat "Configuració del servidor Samba".

2.4 Instal·lació del servidor i del client Samba

El paquet de programari Samba es compon de moltes aplicacions i molts paquets amb diverses finalitats. Els paquets més utilitzats són els següents:

- **samba**: servidor d'arxius i impressores de xarxa local per a Unix/GNU/Linux.
- **smbclient**: client simple de xarxa local per a Unix/GNU/Linux.
- **samba-common**: arxius comuns del Samba que utilitzen els clients i els servidors.
- **swat**: eina d'administració del Samba via web.

Si utilitzem l'ordre `apt-cache search samba` trobarem tots els paquets que conté el Samba.

- **samba-doc**: documentació del Samba.
- **smbfs**: ordres per muntar i desmuntar unitats de xarxa Samba.
- **winbind**: servei per resoldre informació d'usuaris i grups de servidors Windows.

Tots aquests paquets es poden trobar en els dipòsits de l'Ubuntu.

smbclient

El més probable és que, per defecte, el gestor de paquets ja estigui instal·lat en el sistema. Si el tornem a instal·lar, ens ho dirà i potser l'actualitzarà si en troba una versió més recent.

Per instal·lar el servei i el client Samba a l'Ubuntu 9.04 hi ha dues possibilitats. La primera consisteix a fer-ho de la manera tradicional, és a dir, utilitzar els gestors de paquets del sistema directament. Farem servir l'ordre següent:

```
1 $sudo apt-get install samba smbclient smbfs
```

La segona possibilitat consisteix a utilitzar l'entorn gràfic. Només cal que cliquem, amb el botó dret, al damunt d'una carpeta del nostre equip que vulguem compartir. Seleccionarem l'opció *Opcions de compartició* del menú contextual. A continuació, s'obrirà un quadre de diàleg, marcarem la casella *Comparteix aquesta carpeta* i premerem el botó *Crear compartició* (com es mostra a la figura 2.2).

FIGURA 2.2. Quadre de compartició de directoris de Gnome



Automàticament, la primera vegada que fem aquesta acció, ens dirà que ha d'instal·lar el servei Samba. Si acceptem i introduïm la contrasenya de superusuari, ens preguntarà si deixem que el Nautilus afegeixi els permisos necessaris per poder compartir la carpeta. Si diem que sí començarà la instal·lació dels paquets *samba*, *smbclient* i *samba-common*, entre d'altres. Per tant, aquesta possibilitat d'instal·lació ens instal·la, a més d'altres eines, el servidor i el client Samba conjuntament. Això ens permet compartir els nostres recursos i accedir als recursos compartits d'altres màquines. Durant aquest procés d'instal·lació del Samba, una de les accions que es fa mitjançant la compartició de carpetes és crear un grup d'usuaris anomenat *sambashare*. L'usuari que fa la instal·lació s'afegeix a aquest grup, al qual també han de pertànyer tots els usuaris del sistema que vulguin compartir recursos.

L'ús d'aquest mecanisme d'instal·lació ens permet, a més, seleccionar algunes opcions de configuració del recurs a compartir.

Aquestes opcions ens permeten especificar si els usuaris que accedeixen al directori poden escriure (crear elements a dins) o no i si es permet l'accés a usuaris

convidats, sense cap compte d'usuari Samba. Més endavant veurem la manera com especificar aquestes opcions en el fitxer de configuració del servei Samba.

Així, aquest serà el mètode que utilitzarem per compartir carpetes fàcilment mitjançant l'entorn gràfic.

Una vegada instal·lats els paquets relacionats amb el Samba mitjançant alguna de les possibilitats anteriors, podem consultar les ordres o les aplicacions que s'instal·len en el sistema amb l'ordre següent:

```
1 dpkg -L samba | grep bin
2 /usr/bin
3 /usr/bin/eventlogadm
4 /usr/bin/smbstatus
5 /usr/bin/smbcontrol
6 /usr/bin/profiles
7 /usr/bin/tdbbackup
8 /usr/bin/pdbedit
9 /usr/sbin
10 /usr/sbin/smbd
11 /usr/sbin/nmbd
12 /usr/sbin/mksmbpasswd
```

```
1 dpkg -L smbclient | grep bin
2 /usr/bin
3 /usr/bin/findsmb
4 /usr/bin/smbclient
5 /usr/bin/smbget
6 /usr/bin/smbtar
7 /usr/bin/rpcclient
8 /usr/bin/smbpool
9 /usr/bin/smbtree
10 /usr/bin/smbcacs
11 /usr/bin/smbcquotas
```

```
1 dpkg -L smbfs | grep bin
2 /sbin
3 /sbin/mount.cifs
4 /sbin/umount.cifs
5 /usr/bin
6 /usr/bin/smbmount
7 /usr/bin/smbumount
8 /usr/bin/smbmnt
9 /sbin/mount.smbfs
10 /sbin/mount.smb
```

Després d'instal·lar el paquet Samba, el servei Samba arrenca automàticament. Per comprovar-ho, podem consultar amb l'ordre *nmap* si l'equip escolta els ports que utilitza el Samba.

```
1 sudo nmap localhost
2 Starting Nmap 4.76 ( http://nmap.org ) at 2010-02-21 10:14 CET
3 Warning: Hostname localhost resolves to 2 IPs. Using 127.0.0.1.
4 Warning: RateMeter::update: negative time delta; now=1266743641.46884;
5 last_update_tv=1266743641.46961
6 Interesting ports on localhost (127.0.0.1):
7 Not shown: 991 closed ports
8 PORT      STATE SERVICE
9 139/tcp    open  netbios-ssn
10 445/tcp    open  microsoft-ds
```

Per defecte, el servidor Samba fa servir els ports 139 i 445.

Per aturar o reiniciar el servidor, farem servir les ordres

```
1 /etc/init.d/samba stop/
```

o

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

respectivament. Aquestes ordres reiniciaran els dimonis *nmbd*, *smbd* i *windbindd*, necessaris per al funcionament del servei Samba. Haurem de reiniciar el servei cada vegada que vulguem que algun canvi de configuració es faci efectiu.

Per altra banda, podem configurar l'arrencada automàtica del servei Samba quan iniciem el sistema amb l'ordre següent:

```
1 sudo update-rc.d samba defaults
```

Abans de veure el procés de configuració del servidor Samba, observarem com gestiona els usuaris, els grups i els permisos.

2.5 Gestió d'usuaris, grups i permisos del Samba

El Samba és un servei que requereix l'administració dels usuaris per poder-ne gestionar els permisos.

En funció de l'usuari que hi accedeixi, el Samba es comportarà d'una manera o d'una altra. Quan hi accedeix un usuari normal, generalment té uns permisos limitats. En canvi, quan hi accedeix un usuari administrador, ha de disposar de tots els permisos.

Per tal que aquesta administració sigui possible, el Samba disposa de la seva pròpia base de dades d'usuaris Samba. No obstant això, com que els usuaris utilitzen altres recursos del servidor, com carpetes i impressores, cal que aquests usuaris també estiguin creats en el sistema GNU/Linux.

Per poder ser usuari del Samba, cal disposar d'un compte d'usuari a GNU/Linux i d'un compte d'usuari al Samba.

2.5.1 Gestió d'usuaris Samba

La gestió d'usuaris Samba es fa amb l'ordre *smbpasswd*. Amb aquesta ordre podem crear i eliminar usuaris, canviar-ne la contrasenya i unes quantes coses més. Vegem-ne les diferents possibilitats.

1. Creació d'usuaris Samba. Per crear un usuari Samba hem d'utilitzar l'ordre *sudo smbpasswd*. Abans de crear un usuari, però, aquest usuari ha d'existir en el sistema GNU/Linux.

Per exemple, suposem que volem que l'usuari *lluis*, gaudeixi dels serveis del Samba. Primerament haurem de crear l'usuari a l'Ubuntu amb l'ordre següent:

```
1 sudo adduser lluis
```

Després, per habilitar-lo al Samba, executarem aquesta ordre:

```
1 sudo smbpasswd -a lluis
```

L'opció *-a* serveix per indicar al Samba que ha d'afegir l'usuari a la llista d'usuaris Samba. Tot seguit ens preguntarà dues vegades la contrasenya que volem establir a l'usuari. El més raonable és que aquesta contrasenya sigui la mateixa que l'usuari té a GNU/Linux.

2. Eliminació d'usuaris Samba. Per eliminar usuaris Samba també hem d'utilitzar l'ordre *smbpasswd*. Aquesta vegada, però, l'opció és la *-x*. Per exemple, per eliminar l'usuari *lluis*, executarem aquesta ordre:

```
1 sudo smbpasswd -x lluis
```

L'usuari desapareixerà immediatament de la base de dades d'usuaris Samba, però continuarà essent un usuari de GNU/Linux.

3. Altres opcions de *smbpasswd*. L'ordre *smbpasswd* disposa d'altres opcions que considerem interessants. Són les següents:

- **-d:** deshabilitar un usuari.
- **-i:** habilitar un usuari.
- **-n:** establir un usuari sense contrasenya. (Necessita paràmetre *null passwords = yes* en secció *GLOBAL* de l'arxiu de configuració del Samba).
- **-m:** indicar que és un compte de màquina.

Per a més informació es pot consultar la pàgina del manual del *smbpasswd* amb l'ordre *man smbpasswd*.

Abans de veure la manera com el Samba gestiona els permisos d'usuaris i grups, cal tenir clar la diferència que hi ha entre permís i dret en els sistemes operatius.

2.5.2 Permisos i drets Samba

Després d'identificar cada usuari amb accés al servei Samba, es poden especificar els permisos i els drets que té a la xarxa. L'administrador s'encarrega de

determinar l'ús de cada recurs de la xarxa o les operacions que cada usuari pot dur a terme en cada estació de treball.

Per exemple, un usuari pot tenir el dret a accedir a un servidor per mitjà de la xarxa, a forçar l'apagada o el reinici d'un equip remotament, a canviar el sistema d'arrencada, etc. Alhora, cada recurs, servei o utilitat té una informació associada que li indica qui pot utilitzar-lo o executar-lo i qui no. Així, doncs, no hem de confondre dret amb permís. Vegem-ne la diferència:

Un **dret** autoritza un usuari o grup d'usuaris a fer determinades operacions sobre un servidor o una estació de treball.

Un **permís o privilegi** és una marca associada a cada recurs de xarxa (fitxers, directoris, impressores, etc.) que regula quins usuaris i de quina manera hi tenen accés.

D'aquesta manera, els drets fan referència a operacions pròpies del sistema operatiu com, per exemple, el dret a fer còpies de seguretat o a canviar l'hora del sistema. En canvi, els permisos fan referència a l'accés als diferents objectes de xarxa com, per exemple, el permís de llegir un fitxer concret.

Així, doncs, cada recurs té associat un grup de marques (bits) que determina els permisos que té cada usuari depenent del grup al qual pertanyi o de si és el propietari del recurs o no.

Els drets els determinen les accions que cada usuari pot desenvolupar en el sistema. Per exemple, si pertany al grup *root* o al grup *sudo*.

Els drets prevalen sobre els permisos. Per exemple, un operador de consola pot tenir dret a fer una còpia de seguretat de tot un disc, però és possible que no pugui accedir a determinats directoris d'usuaris perquè no tingui permís per fer-ho. D'aquesta manera, podrà fer la còpia de seguretat, perquè el dret de còpia de seguretat preval sobre la restricció dels permisos, però no podrà llegir la informació que hi ha en els directoris si no té permís per fer-ho.

L'assignació de permisos en una xarxa es fa en dues fases:

Dret i permís al Samba

Al Samba, l'opció *valid users*, per exemple, determina els usuaris que tenen dret a accedir al recurs, mentre que l'opció *read only* determina els permisos que té l'usuari amb relació al recurs.

1. En primer lloc, es determina el dret d'accés sobre el servei de xarxa. Per exemple, es pot assignar el dret a connectar-se al servidor Samba. Això evita que es puguin obrir unitats remotes de xarxa sobre les quals després no es tingui privilegis d'accés als fitxers que conté, cosa que podria sobrecarregar el servidor.
2. En segon lloc, s'han de configurar els permisos dels fitxers i els directoris que conté aquest servei de xarxa. Depenent del sistema operatiu de xarxa, les marques associades als recursos varien, encara que en general hi ha les de lectura, escriptura, execució, esborrament, etc. En xarxes en què coexisteixen sistemes operatius de xarxa de diferents fabricants, cal determinar els permisos per a cada sistema.

2.5.3 Gestió de grups i permisos

La gestió de grups, usuaris i permisos és diferent en sistemes GNU/Linux i en sistemes Microsoft Windows. En els sistemes GNU/Linux, la gestió dels permisos que els usuaris i els grups tenen sobre els arxius es fa mitjançant un esquema senzill de tres tipus de permisos (lectura, escriptura i execució) aplicables a tres tipus d'usuaris (propietari, grup propietari i resta d'usuaris).

Aquest esquema es va desenvolupar als anys setanta i avui encara és adequat per a la gran majoria dels sistemes en xarxa que hi ha en qualsevol tipus d'organització, tant si es tracta de xarxes petites com de xarxes grans.

És cert que té algunes limitacions, però té l'avantatge de ser senzill. Això fa que sigui fàcil d'administrar i que el rendiment sigui molt elevat.

En els sistemes Windows, la gestió dels permisos que els usuaris i els grups tenen sobre els arxius es fa mitjançant un esquema complex de llistes de **control d'accés (access control lists, ACL)** per a cada directori i arxiu. El sistema ACL té l'avantatge de ser molt més flexible que el sistema GNU/Linux, ja que es poden establir més tipus de permisos, donar permisos només a uns quants usuaris i grups, denegar permisos, etc. Com s'ha comentat anteriorment, però, en la majoria de casos n'hi ha prou amb les prestacions del sistema GNU/Linux.

D'altra banda, el sistema ACL és més complex d'administrar i més lent, ja que abans d'accedir a les carpetes o als arxius el sistema ha de comprovar les llistes. En sistemes de GNU/Linux, en canvi, es fa una operació lògica dels bits que especifiquen els permisos, de manera que és molt més ràpid.

Per defecte, el Samba utilitza el sistema de permisos de GNU/Linux. Tot i que també pot implementar el sistema ACL i gestionar les llistes mitjançant l'ordre **smbaccls**, és més recomanable fer servir el sistema de gestió de permisos de GNU/Linux.

Quan compartim directoris amb el Samba, en última instància sempre imperen els permisos GNU/Linux.

Per exemple, si tenim compartida una carpeta anomenada *professors* amb permisos d'escriptura per al grup *professors*, tots els usuaris que pertanyin al grup *professors* podran efectuar canvis en la carpeta. No obstant això, si dins d'aquesta carpeta n'hi ha una altra que s'anomena *confidencial*, a la qual el grup *professors* no té permís per entrar, cap professor en podrà veure el contingut, encara que sigui dins d'una carpeta compartida.

Per fer una gestió eficaç d'usuaris, grups i permisos, es recomana fer servir els permisos GNU/Linux, els quals permeten assignar permisos de lectura, escriptura i execució a l'usuari propietari de l'arxiu, al grup propietari de l'arxiu i a la resta d'usuaris del sistema.

Pot ser que hi hagi alguna contradicció entre els permisos del sistema GNU/Linux i els permisos del recurs compartit a Samba.

Per exemple, podem tenir un directori compartit anomenat *magatzem* amb permisos GNU/Linux de lectura, escriptura i execució per a tots els usuaris del sistema. Tanmateix, si en l'arxiu de configuració del Samba aquest recurs té el paràmetre *read only = yes*, no s'hi podran efectuar canvis, ja que està compartit amb permís només de lectura.

Quan els permisos GNU/Linux es contradiuen amb els permisos Samba, el permís efectiu és el més restrictiu.

Per simplificar l'administració dels permisos, es recomana no ser restrictius en els permisos de recurs compartit amb el Samba i aplicar els permisos en el sistema GNU/Linux. D'aquesta manera, a més de ser efectius quan accedim al recurs per mitjà del Samba, també ho serem quan hi accedim d'una altra manera, com per SSH, FTP o mitjançant la consola del servidor.

2.6 Configuració del servidor Samba

La configuració del servidor Samba es fa a partir del fitxer ***/etc/samba/smb.conf***.

La sintaxi de l'arxiu de configuració del Samba és bastant senzilla, ja que està dividit en seccions que es limiten a establir el valor d'uns quants paràmetres i a determinar quines són les carpetes i les impressores compartides, i també els permisos que hi ha. A més, l'arxiu va donant exemples de com hauríem de configurar alguns recursos per compartir-los, com perfils, CD-ROM, etc.

Amb l'edició de l'arxiu */etc/samba/smb.conf* es poden configurar més de tres-cents paràmetres, cosa que dóna lloc a milers de configuracions. Nosaltres ens limitarem a analitzar els paràmetres més rellevants per garantir la seguretat i establir la compartició d'arxius i impressores del servidor.

En l'arxiu */etc/samba/smb.conf* hi ha tres seccions predefinides (*global*, *homes* i *printers*) i tantes seccions addicionals com recursos extra es vulguin compartir. La utilitat i alguns dels paràmetres d'aquestes seccions predefinides es descriuen breument, ja que resulta necessari conèixer-los, per a configurar correctament Samba:

1. [global]. Defineix els paràmetres a escala global del servidor Samba, a més d'alguns dels paràmetres que s'establiran per defecte en la resta de les seccions.

Ordres de configuració del Samba

Encara que utilitzem l'eina gràfica Swat per configurar el Samba, cal conèixer el significat d'uns quants paràmetres del fitxer de configuració */etc/samba/smb.conf*, ja que en determinarem el valor per mitjà del Swat.

En la taula 2.2 es mostren els paràmetres més significatius amb el valor per defecte i exemples:

TAULA 2.2. Opcions principals de la configuració global del Samba

Opció	Significat	Valor per defecte	Exemple
netbios name	Nom (NetBIOS) de l'ordinador Samba	Primer component del nom DNS de l'ordinador.	ALFA
workgroup	Nom del domini (o grup de treball) al qual pertany el Samba.	WORKGROUP	GRUPIOC
security	Nivell de seguretat. Permet determinar el mode de compartició de recursos. Hi ha cinc valors possibles: <i>share</i> , <i>user</i> , <i>domain</i> , <i>server</i> i <i>ads</i> .	user	user
encrypt passwords	Ús de contrasenyes xifrades. L'opció més recomanable és que les contrasenyes s'enviïn xifrades per impedir que altres usuaris puguin descobrir-les, per exemple, capturant paquets de dades (<i>sniffing</i>). Les contrasenyes encriptades del Samba s'emmagatzemen en un altre arxiu. Per defecte, <i>/etc/samba/smbpasswd</i> .	yes	yes
hosts allow	Permet especificar des de quines adreces IP es podrà accedir al servei.	buit	Si posem 192.168. permetem l'accés a totes les màquines de la xarxa l'adreça IP de les quals comenci per 192.168.
host deny	Igual que <i>hosts allow</i> , però per especificar els rangs d'adreces no permesos.	buit	Si posem 10.10. deneguem l'accés a totes les màquines de la xarxa l'adreça IP de les quals comenci per 10.10.
.			

TAULA 2.2 (continuació)

Opció	Significat	Valor per defecte	Exemple
map to guest	<p>Estableix en quines condicions un accés al Samba s'ha de considerar en mode convidat. Pot tenir quatre valors possibles.</p> <p>Never: es rebutjarà l'usuari amb una contrasenya incorrecta.</p> <p>Bad User: es rebutjarà l'usuari amb una contrasenya incorrecta, però si l'usuari no existeix, passarà a ser un usuari convidat. Bad Password: l'usuari amb una contrasenya incorrecta es tractarà com a convidat. És perillós en possibles equivocacions a l'hora d'introduir la contrasenya. Bad UID: només s'utilitza si els modes de seguretat són <i>domain</i> o <i>ads</i>. L'usuari que s'autentiqui correctament, però que no sigui un usuari GNU/Linux, es tractarà com a convidat.</p>	Never	Bad User, implementa un sistema híbrid si el mode de seguretat és <i>user</i> .
usershare allow guests	Permet la compartició de recursos amb usuaris convidats.	yes	yes
guest account	Nom d'usuari amb el qual els usuaris convidats es validaran en el sistema.	nobody	nobody
valid users	Defineix quins usuaris o grups poden accedir als recursos compartits. Es poden especificar múltiples usuaris separats per comes o noms de grup amb l'arrova (@) al davant.	buit	raul,lluis, @administradors
invalid users	Igual que <i>valid users</i> , però per als usuaris que no poden accedir als recursos.	buit	ana, angela,@alumnes
admin users	Defineix quins usuaris poden accedir amb permisos d'administració (superusuaris) als recursos compartits.	buit	ioc,@administradors
write list	Defineix quins usuaris poden accedir amb permisos d'escriptura als recursos compartits.	buit	lluis, @professors
log file	Fitxer en què s'emmagatzemen els registres del Samba.	/var/log/samba/log.%m (%m significa el nom NetBIOS de la màquina client).	ídem

2. [homes]. En aquesta secció es defineix automàticament un recurs de xarxa per a cada usuari conegut pel servidor Samba. Aquest recurs, per defecte, està associat al directori de connexió de cada usuari en l'ordinador en el qual el servidor Samba està instal·lat, és a dir, el directori de l'usuari (*home directory*). Aquesta secció és opcional, és a dir, si no existeix, no es compartiran les carpetes dels usuaris del servidor. S'utilitza quan es volen crear perfils mòbils per tal que, quan l'usuari s'identifiqui en qualsevol dels equips de la xarxa, el perfil s'escanegi automàticament.

El funcionament del servei Samba determina que, quan es faci una sol·licitud de connexió a un recurs compartit, s'escanegin les seccions que hi hagi en el fitxer */etc/samba/smb.conf* mitjançant la cerca del nom del recurs. Si es troba una coincidència, s'utilitzen els paràmetres de la secció, amb el mateix nom que el recurs sol·licitat, per determinar les propietats i la configuració del recurs.

Si no es troba cap coincidència, el nom de la secció sol·licitada es tracta com un nom d'usuari i se'l cerca en l'arxiu de contrasenyes locals. Si el nom existeix i la contrasenya és correcta, es crea un recurs amb el nom d'usuari, el directori de l'usuari s'estableix com a camí o *path* del recurs i la resta de paràmetres del recurs es copien dels que s'han especificat en la secció [homes], si n'hi ha. Si l'usuari no es troba en l'arxiu de contrasenyes locals, es rebutja la connexió al recurs.

La configuració normal de la carpeta de l'usuari (*home*) serà la següent:

```
1 [home]
2 path=/home/%u
3 read only=no
```

Aquí, *%u* és el nom de l'usuari amb el qual ens hem connectat al recurs.

Aquesta és una manera ràpida i senzilla de donar accés als directoris a un gran nombre de clients amb un esforç mínim.

Aquesta secció pot especificar tots els paràmetres de les seccions dels recursos nous a compartir, encara que alguns paràmetres tindran més sentit que d'altres.

Hem de tenir en compte que si permetem que usuaris convidats accedeixin a la secció [homes], tots els directoris d'inici seran visibles i/o modificables si no hem especificat el paràmetre que només permet la lectura, cosa que, des del punt de vista de la seguretat, és poc recomanable. Per tant, per accedir al directori de l'usuari, hem d'especificar directament que ens volem connectar al directori d'inici concret de l'usuari, ja que cal, per seguretat, que els usuaris no puguin veure els directoris de la resta (*browsable = no*).

3. [printers]. Aquesta secció funciona com [homes], però per a les impressores.

Si es troba una secció [printers] en l'arxiu de configuració, es permet que els usuaris es connectin a qualsevol impressora especificada en el fitxer */etc/printcap* de l'ordinador central o *host* local.

Quan es fa una sol·licitud de connexió a un recurs, s'escanegen les seccions que hi ha en el fitxer */etc/samba/smb.conf*. Si es troba alguna coincidència amb el nom

del recurs sol·licitat, s'utilitzen els paràmetres de la secció amb el mateix nom per determinar les propietats i la configuració del recurs. Si no hi ha coincidències, però hi ha una secció [homes], se segueix el procés que s'ha descrit en la secció anterior. En cas que no hi hagi cap secció [homes], el nom de la secció (recurs) sol·licitada es tracta com un nom d'impressora i s'analitza l'arxiu */etc/printcap* per comprovar si aquest nom és un nom vàlid d'impressora compartida. Si es troba una coincidència, es crea una secció nova amb el nom de la secció buscada i amb els paràmetres especificats en la secció [printers] per defecte.

Normalment el path especificat en la secció [printers] és un directori de cua d'escriptura accessible per tots els usuaris amb un sticky bit.

Si no es troba cap coincidència, la connexió al recurs es rebutja.

A fi que el comportament sigui aquest, el paràmetre **printable** de la secció [printers] ha de tenir el valor *yes*, ja que si s'especifica el contrari, és a dir, el valor *no*, el servidor es negarà a carregar el fitxer de configuració.

Un exemple típic de configuració d'aquesta secció és el següent:

```
1 [printers]
2 path = /var/spool/samba
3 guest ok = yes
4 printable = yes
```

4. Recursos nous a compartir. Cada vegada que es vol compartir un recurs (un directori, una impressora, etc.), cal crear una secció nova amb un encapçalament entre claudàtors. L'encapçalament d'aquesta secció es correspondrà amb el nom que el recurs tindrà a la xarxa (el nom mitjançant el qual es podrà accedir al recurs des d'una altra màquina). Generalment es fa servir el mateix nom de la impressora o la carpeta a compartir per tal que sigui més aclaridor.

Per exemple, si volem compartir la carpeta */home/samba/alumnes*, crearem una secció [alumnes] en què aquest recurs compartit es configurarà amb els paràmetres específics.

En la taula 2.3 es descriuen unes quantes opcions aplicables a cada recurs compartit. També es poden establir en la secció global, cas en què s'utilitzaran com a valors per defecte per a cada recurs compartit:

TAULA 2.3. Opcions principals de la configuració dels recursos compartits (shares) del Samba

Opció	Significat	Valor per defecte	Exemple
read only/writable	Defineix si es permet l'escriptura en el recurs o no, només té sentit en carpetes compartides.	yes	yes
browseable / public	Determina si el recurs apareix en la llista de recursos compartits en explorar el servidor Samba.	yes	yes
path	Especifica la ruta absoluta al directori compartit pel recurs.	buit	/home/ioc/professors
comment	Descriu el recurs mitjançant una cadena de caràcters.	buit	Directori en què els professor deixen els apunts.
.			

TAULA 2.3 (continuació)

Opció	Significat	Valor per defecte	Exemple
quest ok	Determina si es permet accedir com a convidat al recurs.	no	yes
quest only	Especifica que tots els accessos al recurs s'accepten en mode convidat.	no	no
create mask	Estableix la màscara de creació d'arxius, que determinarà els permisos dels usuaris. Té la mateixa funció que l'opció <i>directory mask</i> per a la creació de directoris.	0770	0775
hosts allow	Proporciona una llista d'ordinadors des dels quals es permet accedir al recurs. S'hi afegixen els que s'han especificat en la secció [global].	buit(vol dir tots els ordinadors)	192.169.
hosts deny	Proporciona una llista d'ordinadors des dels quals no es permet accedir al recurs. En cas de conflicte, preval el que s'indica en l'opció <i>hosts allow</i> de la secció [global].	buit(vol dir cap ordinador)	10.0.
valid users	Proporciona una llista d'usuaris que poden accedir al recurs. En cas de conflicte, preval el que s'indica en la secció [global].	buit(vol dir tots els usuaris)	pere, @pas
invalid users	Proporciona una llista d'usuaris que no poden accedir al recurs. En cas de conflicte, preval el que s'indica en la secció [global].	buit(vol dir cap usuari)	profe,@admin
read list	Proporciona una llista d'usuaris que només tindran permisos de lectura en el recurs. Si el paràmetre és <i>read only = yes</i> , per defecte tots els usuaris només tindran permís de lectura.	buit	@alumnes
write list	Proporciona una llista d'usuaris que tindran permís de lectura i escriptura en el recurs. Ignora l'opció <i>read only = yes</i>	buit	@professors
printable	Permet determinar, en cas d'impressores, si el client pot obrir, escriure i enviar fitxers de gestió o <i>spool</i> de cues al directori especificat per tal d'imprimir-los.	yes	yes

TAULA 2.3 (continuació)

Opció	Significat	Valor per defecte	Exemple
printing	Aquesta opció determina l'estil o el sistema d'impressió utilitzat pel Samba.	cups	cups

Recomanacions durant la configuració del Samba:

- És convenient crear en el directori */home* una carpeta anomenada *samba* que contingui totes les carpetes compartides. La finalitat és tenir totes les dades d'usuari dins del directori de l'usuari i que fer les còpies de seguretat sigui senzill.
- És convenient crear una còpia de seguretat de l'arxiu */etc/samba/smb.conf* abans de fer cap canvi. La finalitat és poder tornar a l'estat anterior en cas que fem una modificació incorrecta de l'arxiu que impedeixi que el servei arrenqui. El Samba analitza cada 60 segons l'arxiu */etc/samba/smb.conf* i, si hi ha hagut canvis, es fan efectius.
- Per comprovar que el nostre arxiu */etc/samba/smb.conf* és correcte, podem utilitzar l'ordre *testparm*, la qual analitza cada línia per localitzar-hi errors.
- Per tenir una descripció detallada de tots els paràmetres, es pot consultar la pàgina del manual d'*/etc/samba/smb.conf* amb l'ordre *man smb.conf*.

Per altra banda, el Samba ofereix una interfície d'edició d'aquest fitxer basada en web denominada *Swat*. Aquesta eina permet configurar el Samba utilitzant un navegador de xarxa, tant de forma local com remota. És interessant i imprescindible veure la manera de configurar gràficament el servidor Samba amb l'eina *Swat*.

2.6.1 Configuració gràfica del servidor Samba amb el Swat

El Swat (Samba Web Administration Tool) és una aplicació amb una interfície gràfica basada en web que permet administrar i configurar qualsevol servidor Samba de manera senzilla i visual, sense haver d'editar ni modificar cap fitxer de configuració a mà.

Eines gràfiques de configuració per al Samba

Hi ha diverses eines que ens ajuden a gestionar gràficament el Samba o aspectes que hi estan relacionats. D'aquestes eines, en podem destacar cinc: el Gosa, el LAM, l'ebox, el Webmin i l'Swat. Nosaltres veurem l'Swat perquè està totalment orientat a la configuració amb interfície gràfica del servidor Samba.

Per fer servir l'Swat com a eina d'administració de qualsevol servidor Samba, el servidor ha de tenir prèviament instal·lat i funcionant com a mínim un servei web. Per obtenir els requisits necessaris per accedir via web al servidor podem instal·lar-hi el paquet de programari LAMP de manera ràpida i senzilla amb l'eina *tasksel*. Una vegada instal·lat aquest paquet, disposarem del servei de base de dades MySQL i de l'interpret de PHP, a més del servei web Apache.

Per instal·lar l'Swat farem servir dos paquets: el paquet *swat* i el paquet *inetutils-inetd*. Utilitzarem l'ordre següent:

```
1 $sudo apt-get install swat inetutils-inetd
```

Una vegada instal·lat l'swat, l'hem d'activar a *inetd* amb aquesta ordre:

```
1 $sudo update-inetd --enable 'swat'
```

Finalment, hem d'establir una contrasenya a l'usuari primari (*root user*) per tal de poder-nos validar a l'inici de l'aplicació:

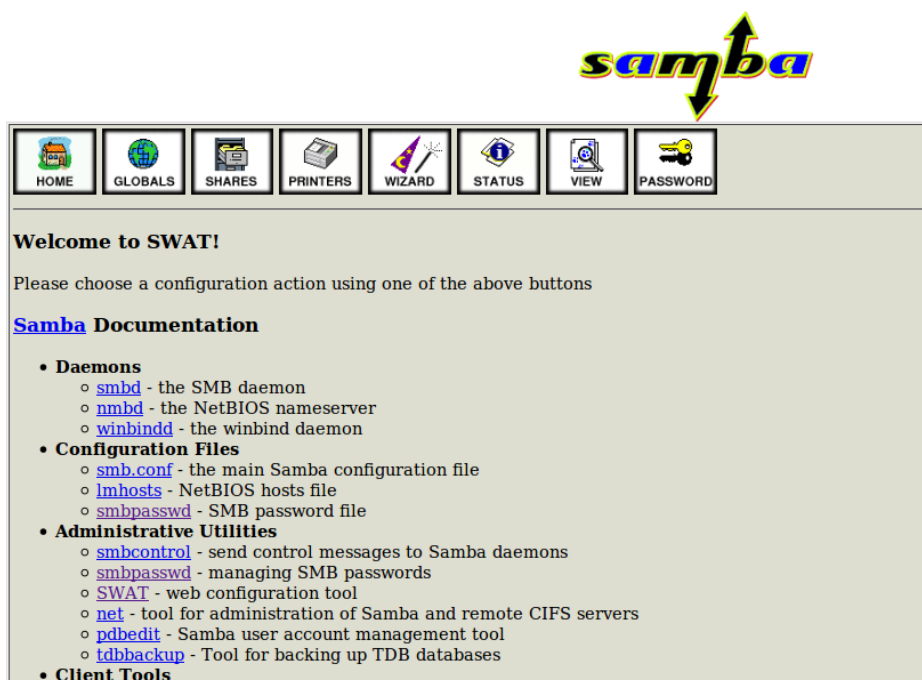
```
1 sudo --s  
2 passwd
```

Per accedir a la interfície gràfica de l'swat, hem d'obrir un navegador. Si som en el mateix servidor, en la barra de cerques hi hem d'escriure <http://localhost:901>.

L'aplicació ens demanarà un nom d'usuari i una contrasenya. Si volem accedir a totes les funcionalitats del Samba, hem d'entrar com a usuaris primaris i fer servir la contrasenya que hem establert abans.

En accedir a l'Swat apareix la pantalla que es mostra en la figura 2.3.

FIGURA 2.3. Pantalla inicial de Swat



Com podem observar en la part superior de la pantalla, tenim una sèrie de botons que ens permeten seleccionar diferents opcions de gestió i configuració. Ens interessa conèixer què ens ofereix cada botó:

1. HOME. Aquest botó ens porta a la pàgina inicial de l'aplicació, la qual ens dóna la benvinguda i ens proporciona una gran quantitat d'enllaços a la documentació més actualitzada del Samba.

inetd

L'*inetd* és un dimoni que atén les sol·licituds de connexió que arriben al nostre equip i està a l'expectativa de tots els intents de connexió que es fan en la màquina. L'*inetd* s'utilitza principalment per llançar processos que contenen altres dimonis, generalment serveis. Els serveis de xarxa que presta la màquina estan descrits a */etc/inetd.conf*.

Si volem accedir de manera remota al servidor Samba, hauríem de canviar *localhost* per l'adreça IP, el nom de la màquina o el nom de domini.

2. GLOBALS. Aquest botó ens porta a una pàgina que ens permet configurar tots els paràmetres que hi ha en la secció **[global]** del fitxer */etc/samba/smb.conf*. Al començament de la pàgina podem seleccionar si volem configurar els paràmetres bàsics o avançats. Segons l'opció que seleccionem, ens apareixeran més o menys paràmetres als quals podrem establir el valor corresponent. Cal recordar que el fitxer */etc/samba/smb.conf* pot tenir més de tres-cents paràmetres, de manera que només en modificarem els més bàsics. Sempre que fem algun canvi hem de prémer el botó **Commit Changes** perquè s'emmagatzemi al fitxer de configuració del Samba. Si no ho fem, els canvi es perdrà en seleccionar un altre botó.

Dins d'aquesta secció, els paràmetres es divideixen en grups d'opcions segons l'àmbit del servei amb el qual estan relacionats. Per al nostre exemple, modificarem els paràmetres del grup **Base Options**. En el paràmetre **workgroup** establim el nom del grup de treball del servidor i en el paràmetre **netbios name**, el nom amb el qual es coneixerà el servidor. En la resta d'opcions deixarem el valor que tenen per defecte. La configuració quedarà com es mostra en la figura 2.4.

FIGURA 2.4. Paràmetres globals de Samba mostrats al Swat

Global Parameters

Current View Is: ☒ Basic ☐ Advanced
Change View To:

Base Options

Help	workgroup	GRUPOIOC	<input type="button" value="Set Default"/>
Help	realm		<input type="button" value="Set Default"/>
Help	netbios name	ALFA	<input type="button" value="Set Default"/>
Help	netbios aliases		<input type="button" value="Set Default"/>
Help	server string	%h server (Samba, Ubuntu)	<input type="button" value="Set Default"/>
Help	interfaces		<input type="button" value="Set Default"/>

Security Options

Help	security	USER	<input type="button" value="Set Default"/>
Help	auth methods		<input type="button" value="Set Default"/>
Help	encrypt passwords	Yes	<input type="button" value="Set Default"/>
Help	client schannel	Auto	<input type="button" value="Set Default"/>
Help	server schannel	Auto	<input type="button" value="Set Default"/>
Help	map to guest	Bad User	<input type="button" value="Set Default"/>

3. SHARES. Si premem aquest botó, l'aplicació ens mostrarà una pantalla en la qual podrem crear i esborrar els recursos compartits que gestiona el servidor Samba. A més, ens permetrà establir diverses opcions dels directoris compartits i dels arxius que contenen, com tipus d'accés, usuaris que hi poden accedir o permisos, entre altres. Al costat de cada opció tenim un enllaç, **Help**, que ens obrirà una altra finestra en què ens explicarà el significat, l'ús i la sintaxi de cada ordre. En el nostre exemple crearem, com es mostra en la figura 2.5, una carpeta que només serà de lectura, anomenada *professors*. Com a comentari, hi posarem "Carpeta amb apunts per als alumnes".

FIGURA 2.5. Pàrmetres de la secció SHARES

Choose Share	Professors ▼	Delete Share
Create Share	<input type="text"/>	
Commit Changes	Reset Values	

Base Options

[Help](#) comment [Set Default](#)

[Help](#) path [Set Default](#)

Security Options

[Help](#) invalid users [Set Default](#)

[Help](#) valid users [Set Default](#)

[Help](#) admin users [Set Default](#)

[Help](#) read list [Set Default](#)

[Help](#) write list [Set Default](#)

[Help](#) read only [Set Default](#)

[Help](#) guest ok [Set Default](#)

[Help](#) hosts allow [Set Default](#)

[Help](#) hosts deny [Set Default](#)

Browse Options

[Help](#) browseable [Set Default](#)

Miscellaneous Options

[Help](#) available [Set Default](#)

Amb el Samba no solament podem compartir directoris i impressores, sinó que també podem compartir altres dispositius, com CD-ROM, particions de disc, etc.

FIGURA 2.6. Dades d'exemple per a la compartició del CD-ROM

Base Options

[Help](#) comment [Set Default](#)

[Help](#) path [Set Default](#)

Security Options

[Help](#) invalid users [Set Default](#)

[Help](#) valid users [Set Default](#)

[Help](#) admin users [Set Default](#)

[Help](#) read list [Set Default](#)

[Help](#) write list [Set Default](#)

[Help](#) read only [Set Default](#)

[Help](#) guest ok [Set Default](#)

[Help](#) hosts allow [Set Default](#)

[Help](#) hosts deny [Set Default](#)

Browse Options

[Help](#) browseable [Set Default](#)

Miscellaneous Options

[Help](#) available [Set Default](#)

En la imatge següent mostrem un exemple de compartició, amb tots els usuaris i les màquines de la xarxa, de la unitat de CD-ROM d'un servidor Samba. Així, doncs, les opcions de la secció *SHARES* serien les que apareixen en la figura 2.6.

4. PRINTERS. En aquesta secció podem especificar les impressores a compartir. A més, també hi podem determinar quins paràmetres de compartició volem aplicar a cada impressora: si els convidats hi poden accedir, quins ordinadors centrals poden accedir o no a cada impressora, si està disponible o visible per als usuaris que hi accedeixen al servidor, etc.

Si no tenim cap impressora compartida a la llista, al costat del botó **Choose Printer** ens mostra, per defecte, el recurs *print\$*. Aquest recurs conté controladors d'impressores perquè els clients hi pugin accedir si no els troben disponibles localment. El recurs *print\$* és opcional i pot ser que no es faci servir. En la figura 2.7 es mostra un exemple de la secció.

FIGURA 2.7. Paràmetres de la secció PRINTERS

The screenshot shows the Samba configuration window for the PRINTERS section. At the top, there are buttons for 'Choose Printer', 'Delete Printer', 'Create Printer', 'Commit Changes', and 'Reset Values'. Below these are several sections of options:

- Base Options:**
 - comment:** 'All Printers' (with a 'Set Default' button)
 - path:** '/var/spool/samba' (with a 'Set Default' button)
- Security Options:**
 - printer admin:** (empty text field, with a 'Set Default' button)
 - guest ok:** 'No' (dropdown menu, with a 'Set Default' button)
 - hosts allow:** (empty text field, with a 'Set Default' button)
 - hosts deny:** (empty text field, with a 'Set Default' button)
- Printing Options:**
 - printable:** 'Yes' (dropdown menu, with a 'Set Default' button)
- Browse Options:**
 - browseable:** 'No' (dropdown menu, with a 'Set Default' button)
- Miscellaneous Options:**
 - available:** 'Yes' (dropdown menu, with a 'Set Default' button)

5. WIZARD. Aquesta secció ens permet determinar el rol del nostre servidor Samba dins d'una xarxa Windows. Podem especificar quin tipus de servidor serà: només servidor, membre del domini o controlador de domini. També podem determinar si farem servir WINS o no, i si el nostre servidor farà de servidor WINS o de client d'un altre servidor WINS.

També ens ofereix la possibilitat de mostrar el directori dels usuaris Samba, per tal que s'hi pugui accedir des dels equips de la xarxa local o el grup de treball.

6. STATUS. Aquest botó ens permet controlar el funcionament del servidor Samba. Amb el botó *Auto Refresh* podem especificar que ens mostri la informació de la situació del servidor (connexions d'usuaris actives, recursos compartits actius i recursos utilitzats o oberts) amb la freqüència que especifiquem en el camp *Refresh Interval*.

A més, des d'aquesta secció podem aturar o reiniciar els distints dimonis del servei Samba (*smbd*, *nmbd* i *winbindd*) i terminar (matar) les connexions establertes pels

usuaris.

7. VIEW. Si seleccionem aquest botó ens mostrarà el contingut de l'arxiu */etc/samba/smb.conf*, per tal que puguem veure la configuració actual del servidor Samba.

8. PASSWORD. Si seleccionem aquest botó ens portarà a una pàgina en la qual trobem dues seccions: *Server Password Managment* i *Client/Server Password Managment*. La primera secció ens permet crear, esborrar, desactivar i reactivar usuaris Samba en la màquina local, mentre que la segona la podem fer servir per canviar la contrasenya d'un compte d'usuari local.

2.7 Utilització del client Samba

El client Samba ens proporciona una ordre per accedir als recursos compartits dels servidors Samba disponibles per mitjà de la xarxa: *smbclient*. L'ordre *smbclient* és una petita aplicació que ens permet accedir als servidors Samba com a clients, com si es tractés d'una mena d'accés FTP. S'utilitza sobretot per saber quins recursos Samba ens ofereix una màquina remota. Per exemple, la sintaxi per llistar els recursos d'una màquina remota és la següent:

```
1 smbclient -U usuario -L NET_BIOS_NAME
```

En cas que no hi tinguem accés, ens mostrarà el missatge següent:

```
1 $smbclient -U luis -L IOC
2 Password:
3 session setup failed: NT_STATUS_LOGON_FAILURE
```

També hi podem accedir de manera anònima:

```
1 smbclient -N -L IOC
2 Anonymous login successful
3 Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.3.2]
4 Sharename      Type            Comment
5 -----
6 material ioc    Disk
7 apunts          Disk
8 IPC$            IPC             IPC Service (ioc-laptop server (Samba, Ubuntu))
9 print$          Disk            Printer Drivers
10 homes          Disk
11 Anonymous login successful
12 Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.3.2]
13 Server          Comment
14 -----
15 ALFA             ioc-laptop server (Samba, Ubuntu)
16 Workgroup        Master
17 -----
18 WORKGROUP        ALFA
```

Per connectar-nos al recurs que ens interessa, haurem de fer servir aquesta ordre:

```
1 smbclient //NETBIOS_NAME/Recurs
```

Si el recurs està protegit amb contrasenya, hi haurem d'afegir l'opció `-U` amb el nom d'usuari. Després d'executar l'ordre, ens demanarà la contrasenya. L'ordre quedarà així:

```

1 smbclient -U clientsamba //IOC/apunts
2 Enter clientsamba's password:
3 Domain=[IOC] OS=[Unix] Server=[Samba 3.3.2]
4 smb: \>

```

Quan accedim al recurs compartit, disposem d'una línia d'ordres. Tot i així, també podem executar les ordres típiques del servei FTP, com *put* o *get*, entre altres. Per tal que ens mostri totes les ordres que podem utilitzar, hem d'executar l'ordre *help*:

```

1 smb: \> help
2 ?          altname      archive      blocksize   cancel
3 case_sensitive cd          chmod        chown       close
4 del         dir          du           exit        get
5 getfacl     hardlink    help         history     lcd
6 link        lock         lowercase    ls          mask
7 md          mget        mkdir        more        mput
8 newer       open         posix        posix_open  posix_mkdir
9 posix_rmdir posix_unlink print         prompt      put
10 pwd         q           queue        quit        rd
11 recurse     reget       rename       reput       rm
12 rmdir       showacls    setmode      stat        symlink
13 tar         tarmode     translate    unlock      volume
14 vuid        wdel        logon        listconnect showconnect

```

També podem fer servir les ordres de navegació per al sistema de fitxers de GNU/Linux (*cd*, *ls*) i algunes de les ordres habituals de modificació de fitxers (*rm*, *mkdir*, *del* o *rename*), sempre que tinguem permisos.

Suposem, per exemple, que ens volguéssim connectar a la carpeta de l'usuari (*home*) *clientsamba* i que tinguéssim la secció *HOMES* habilitada en el servidor Samba. En aquest cas, hauríem de fer servir l'ordre següent:

```

1 smbclient -U clientsamba //IOC/clientsamba
2 Enter clientsamba's password:
3 Domain=[IOC] OS=[Unix] Server=[Samba 3.3.2]
4 smb: \> ls
5 .                D          0   Sun Mar 21 19:16:12 2010
6 ..               D          0   Mon Mar 22 11:09:38 2010
7 .profile         H        675  Sun Mar 21 19:16:12 2010
8 examples.desktop H        357  Sun Mar 21 19:16:12 2010
9 .bash_logout     H        220  Sun Mar 21 19:16:12 2010
10 .bashrc          H       3115 Sun Mar 21 19:16:12 2010
11                  61335 blocks of size 131072. 26464 blocks available

```

Tot i que l'ordre *smbclient* és molt útil, aquesta manera de treballar pot resultar una mica enutjosa. Hi ha, però, la possibilitat de muntar les unitats de xarxa a les quals volem accedir en directoris del nostre sistema, com si es tractés de directoris locals. Per això haurem de tenir instal·lat el paquet *smbfs*.

2.8 Muntar unitats de xarxa

GNU/Linux disposa de suport per al sistema de fitxers SMB. Així, GNU/Linux, de la mateixa manera que pot muntar un directori exportat via NFS en un directori local, pot muntar un recurs SMB ofert per un servidor SMB, com un sistema Windows o un servidor Samba.

No obstant això, com ja hem comentat, hi ha una diferència entre l'NFS i l'SMB. L'NFS no requereix que l'usuari que fa la connexió s'autentiqui. Aquest servidor fa servir el UID de l'usuari de l'ordinador client per accedir als fitxers i als directoris exportats.

Un servidor SMB, per contra, sí que requereix que l'usuari s'autentiqui, i per això necessita un nom d'usuari i una contrasenya. Per muntar un recurs SMB podem fer servir les ordres *smbmount* o, directament, l'ordre *mount* si li indiquem un tipus de sistema d'arxius específic (en aquest cas, *smbfs*). La sintaxi d'aquestes dues ordres seria la següent:

```
1 smbmount -username=usuari -password=contrasenya -workgroup=MEUGRUP //  
   servidor_Samba/recurs  
2 /punt_de_muntatge/  
3  
4 mount -t smbfs -o username=usuari,password=contrasenya,workgroup=MEUGRUP  
5 //servidor_Samba/recurs /punt de muntatge
```

Si el servidor no requereix que l'usuari s'autentiqui (permet accés a convidats), els paràmetres *username*, *password* i *workgroup* es poden obviar.

Si en les ordres anteriors s'omet l'opció *password*, el sistema sol·licita a l'usuari que introdueixi una contrasenya. Si el servidor SMB permet l'accés a l'usuari, s'aconsegueix accedir al recurs (en aquest cas, *servidor_Samba/recurs*) a partir del directori local que hem establert com a punt de muntatge.

En el muntatge de sistemes d'arxius, també podem optar per registrar el muntatge en el fitxer */etc/fstab*. Així, els directoris es poden muntar automàticament en l'arrencada del sistema. No obstant això, en el cas del sistema d'arxius *smbfs*, aquest registre presenta un problema, ja que el muntatge sempre implica la petició d'una contrasenya. Aquesta contrasenya es pot especificar en les opcions de muntatge o bé es pot sol·licitar per teclat en el moment de fer el muntatge.

Òbviament, aquesta última opció dificulta el muntatge automàtic en l'arrencada, tret que escrivim la contrasenya en el fitxer */etc/fstab*. Això, per motius de seguretat, no és gaire recomanable, ja que qualsevol usuari pot llegir aquest arxiu. L'alternativa consisteix a utilitzar un fitxer d'identificacions d'usuaris (opció de muntatge *credentials=FITXER*) en què s'haurà d'escriure el nom i la contrasenya de l'usuari.

A pesar que en aquest fitxer la contrasenya també s'escriu en text pla, constitueix una mesura de seguretat suficient, ja que aquest fitxer només el pot llegir l'usuari

Realment, l'ordre **mount -t smbfs** es reencamina a *smbmount*.

El nom típic del fitxer d'identificacions d'usuaris és *.smbpasswd* i s'emmagatzema a la carpeta de l'usuari (*home*).

que fa el muntatge, com ara el primari (*root*).

Vegem un exemple del fitxer */etc/fstab* configurat per muntar recursos Samba remots en l'arrencada del sistema:

- **Muntar de manera permanent un recurs anònim.**

```
1 //ALFA/apuntes /mnt smbfs user,auto,guest,ro,gid=100 0 0
```

- **Muntar de manera permanent un recurs protegit.**

```
1 //ALFA/Material_ioc /mnt smbfs username=clientsamba,password=ioc 0 0
```

- **Muntar un recurs protegit amb el fitxer d'identificadors d'usuaris.**

```
1 //ALFA/professor /mnt smbfs credentials=/home/clientsamba/.smbpasswd 0 0**
```

Un inconvenient addicional és que, si les unitats es munten d'aquesta manera, l'únic usuari que hi podrà escriure serà el primari. Si volem que múltiples usuaris tinguin permís de lectura i escriptura en la unitat muntada, haurem de crear un grup (anomenat, per exemple, *sambausersgroup*) i afegir-hi els usuaris. El fitxer */etc/fstab* quedarà així:

```
1 //ALFA/professor /mnt smbfs credentials=/home/clientsamba/
2 .smbpasswd,gid=sambausersgroup 0 0
```

Per altra banda, també pot ser molt útil permetre que els usuaris que no tinguin permisos de superusuari puguin muntar unitats Samba remotes. Per fer-ho, haurem de seguir una sèrie de passos:

1. Crear un grup i afegir-hi els usuaris.

```
1 sudo groupadd samba
2 sudo adduser user samba
```

2. Editar *sudo* per permetre que els usuaris del grup puguin muntar unitats Samba.

```
1 sudo visudo
2 ## Members of the admin group may gain root privileges
3 %admin ALL=(ALL) ALL
4 %samba ALL=(ALL) /bin/mount,/bin/umount,/sbin/mount.cifs,/sbin/umount.cifs
```

Ara tots els usuaris del grup afegit podran muntar unitats Samba remotes.

Es recomana consultar la pàgina de manual *smbmount* per obtenir més detalls sobre les opcions de muntatge. Ho podem fer mitjançant l'ordre ***man smbmount***.

2.9 Accés gràfic als recursos compartits

L'Ubuntu ens permet accedir gràficament als recursos disponibles dels grups de treball (paràmetre *workgroup* del Samba) que hi ha a la xarxa local amb el navegador Nautilus, per mitjà del menú **Llocs > Xarxa**.

En seleccionar aquesta opció del menú, se'ns obrirà una finestra del Nautilus en què ens apareixeran tots els grups de treball (dominis) que hi hagi a la xarxa local. Si fem doble clic a cadascun dels grups, ens mostrarà els servidors Samba disponibles. Per veure els recursos que comparteix cada servidor, haurem de fer doble clic al damunt de la icona amb el nom. Aleshores, o bé hi podrem accedir lliurement perquè el servidor permet l'accés a usuaris convidats o bé haurem d'especificar el nom d'usuari Samba i la contrasenya adequada. En accedir a qualsevol servidor Samba, automàticament es muntaran totes les carpetes compartides del servidor, cosa que ens permetrà gestionar més fàcilment els recursos als quals tinguem accés. L'accés a cada recurs pot ser lliure o pot requerir un nom d'usuari Samba i una contrasenya. Si ens fixem en la figura 2.8 i figura 2.9 podrem entendre més bé tot el que hem comentat.

FIGURA 2.8. Accés gràfic als workgroups de la xarxa

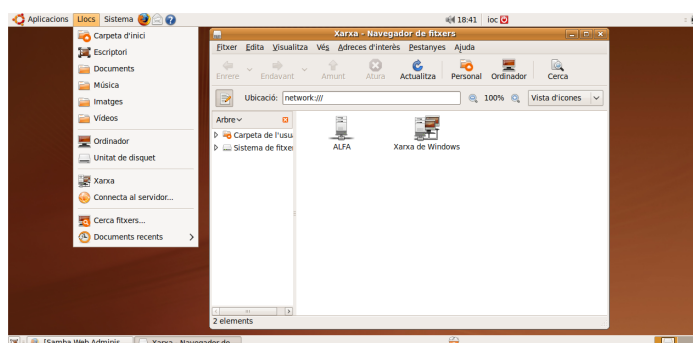
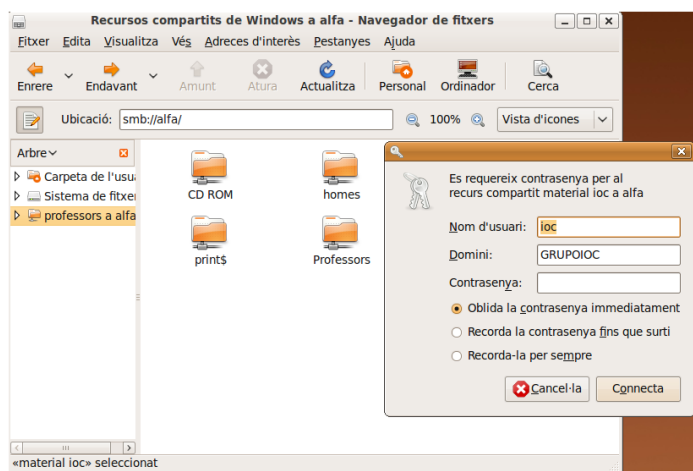


FIGURA 2.9. Accés gràfic als recursos de un workgroup concret



Per moure'ns per les carpetes, els servidors i els grups també podem utilitzar, a més dels clics, la barra de cerques *Ubicació*. La sintaxi de les adreces en la barra

Ubicació és la següent:

1 `smb://nom_servidor/recurs`

2.10 Servidor d'impressió CUPS

En els sistemes GNU/Linux hi ha un sistema d'impressió estàndard que ens permet centralitzar, compartir i gestionar impressores instal·lades en una màquina que fa les tasques de servidor d'impressió. L'eina que ens proporciona aquest sistema d'impressió és el CUPS.



El CUPS (*common Unix printing system*, sistema d'impressió comú d'Unix) és un sistema d'impressió modular per a sistemes operatius de tipus Unix/GNU/Linux que permet que un ordinador actuï com a servidor d'impressió.

El CUPS es basa en el protocol IPP (*Internet printing protocol*, protocol d'impressió per Internet), el qual permet compartir impressores per mitjà de xarxes TCP/IP. El CUPS és programari lliure i es distribueix sota llicència GPL i LGPL.

La gran majoria de distribucions GNU/Linux utilitzen el CUPS com a sistema d'impressió per defecte.

Un ordinador que executa el CUPS actua com un servidor que pot acceptar tasques d'impressió des d'altres ordinadors clients, les processa i les envia a la impressora apropiada.

El CUPS és format per una cua d'impressió amb un planificador, un sistema de filtres, el qual converteix les dades que s'han d'imprimir en formats que la impressora conegui, i un sistema de suport (*back-end*) que envia les dades al dispositiu d'impressió.

El CUPS, a més d'utilitzar el protocol IPP com a base per al maneig de tasques d'impressió i cues d'impressió, també proveeix les ordres tradicionals de línia d'ordres d'impressió dels sistemes GNU/Linux.

El CUPS també disposa d'un suport limitat d'operacions sota el protocol SMB, el quals s'utilitza, en aquest cas, per compartir impressores.

2.10.1 Funcionament del CUPS

El CUPS proveeix un mecanisme que permet enviar treballs d'impressió a impressores de manera estandaritzada. La informació s'envia al planificador, el qual envia el treball a un sistema de filtres que el converteix a un format que la

impressora pugui comprendre. Després, el sistema de filtres envia les dades a un *back-end*, un filtre especial que envia les dades destinades a la impressora a un perifèric o una connexió de xarxa. El sistema fa un ús extensiu del llenguatge PostScript i de tractament de les dades a fi de convertir-les a un format que la impressora accepti.

El CUPS té com a avantatge principal que és un sistema d'impressió estandarditzat i modularitzat, capaç de processar diferents formats de dades en el servidor d'impressió. El CUPS permet als fabricants d'impressores i als desenvolupadors de controladors crear més fàcilment controladors que funcionin nativament en el servidor d'impressió.

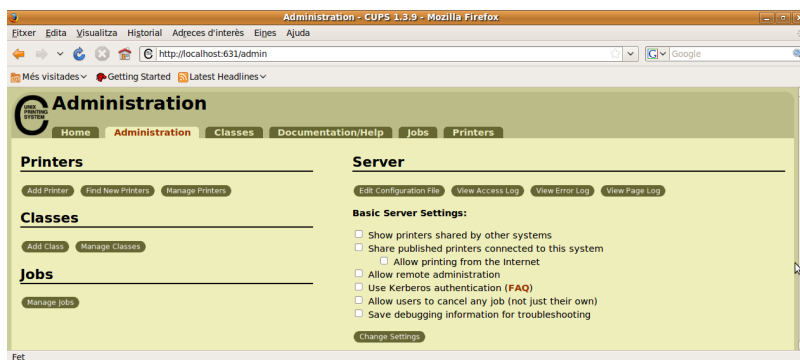
El processament de la informació a imprimir ocorre en el servidor, motiu pel qual permet sistemes d'impressió basats en xarxa molt més senzills que altres sistemes d'impressió Unix. Quan el CUPS es fa servir amb el Samba, les impressores també es poden utilitzar en ordinadors Windows remots per imprimir per mitjà de la xarxa.

2.10.2 Instal·lació i configuració del CUPS

La instal·lació de l'eina CUPS la podem fer mitjançant les ordres de gestió de paquets del sistema amb els paquets adequats. Així, doncs, l'ordre d'instal·lació seria la següent:

```
1 sudo apt-get install cupsys cupsys-client cups-pdf
```

FIGURA 2.10. Pantalla inicial de CUPS



- **cupsys**, és el paquet que ens instal·la el servidor CUPS.
- **cupsys-client**, és el paquet que ens instal·la el client CUPS.
- **cups-pdf**, és el paquet que ens instal·la una eina que ens permet crear fitxers PDF a partir del CUPS, com si fos una impressora. És similar al PDFCreator del Windows.

Per poder-lo configurar i administrar, el servidor CUPS disposa, a més de les ordres de l'interpret d'ordres, d'una interfície web que funciona sobre el port

631. Aquesta interfície web ens permet de manera gràfica afegir, cercar i eliminar impressores i classes d'impressores, controlar els treballs en les cues d'impressió i gestionar diversos paràmetres del servidor. En la figura 2.10 es mostra la pantalla que apareix en carregar la interfície web del CUPS.

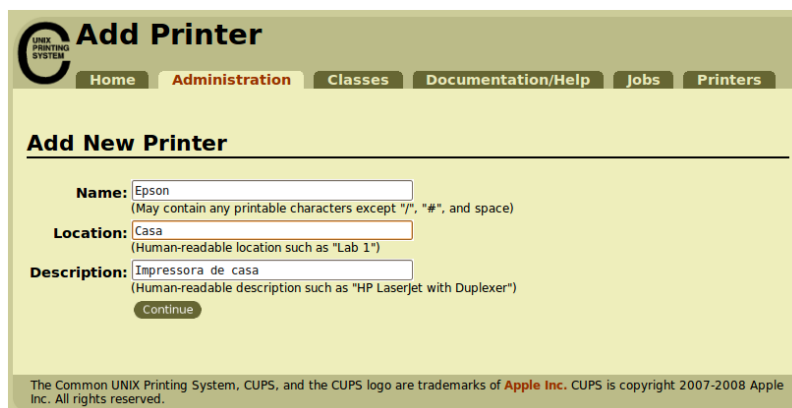
2.10.3 Compartir impressores gràficament amb el CUPS

Per tal de compartir impressores amb el servidor CUPS disposem d'un entorn gràfic, al qual ens podem connectar mitjançant l'explorador d'Internet, que ens facilita el procés. Així doncs, el procés de compartició d'impressores per mitjà del CUPS consta dels passos següents:

1. Instal·lació en el servidor d'impressió de les impressores a compartir. Per instal·lar una impressora en el servidor CUPS hem de seleccionar l'opció **Add printers** de la pestanya *Administration*.

Apareixerà una pantalla, com la que veiem en la figura 2.11, en què ens demanarà un nom, la localització i una descripció per a la impressora que volem instal·lar.

FIGURA 2.11. Pantalla inicial per afegir una nova impressora amb CUPS



Si continuem, una vegada especificats els paràmetres anteriors, ens demanarà el dispositiu o *back-end* al qual volem associar la impressora. Aquest paràmetre es fa servir per transferir correctament les ordres d'impressió als dispositius d'impressió.

Seguidament ens mostrarà la pantalla de la figura 2.12, en què ens demanarà l'URI (*uniform resource identifier*, identificador uniforme de recursos) del dispositiu per poder especificar on és la impressora en el sistema. Hem d'anar en compte perquè, si no especifiquem bé aquest paràmetre, la impressora romandrà inaccessible. Podem consultar en la documentació del CUPS com hem d'especificar l'URI, segons el model de la impressora.

La pantalla següent ens demana pel fabricant de la impressora a fi d'instal·lar els controladors de dispositiu adequats. També ens permet especificar aquests controladors mitjançant un fitxer de text en format PPD (*PostScript printer*

PostScript

El PostScript és un llenguatge de descripció de pàgines que s'utilitza en moltes impressores i, de manera usual, també es fa servir com a format de transport d'arxius gràfics en tallers d'impressió professional.

PostScript printer description

El PPD és un arxiu que crea el fabricant de la impressora per descriure les característiques disponibles per a les seves impressores PostScript. Un PPD conté el codi de PostScript necessari per fer servir les característiques d'una impressora. D'aquesta manera, funciona com un controlador de dispositiu per a les impressores PostScript i proveeix una interfície unificada.

description). Seguidament, ens demanarà pel model d'impressora per instal·lar els controladors més adequats.

FIGURA 2.12. Pantalla d'especificació del lloc de l'impressora al sistema amb CUPS

Una vegada seleccionat el model d'impressora, la instal·larà. Si s'instal·la correctament, apareixerà una pantalla, com la de la figura 2.13, que ens permetrà configurar les opcions generals d'impressió de la impressora.

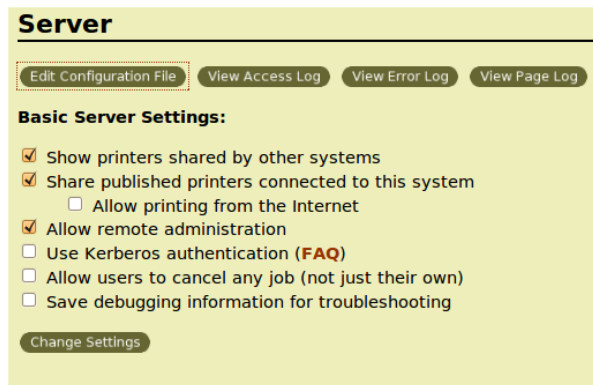
FIGURA 2.13. Pantalla d'opcions generals de configuració de la impressora amb CUPS

CUPS i PPD

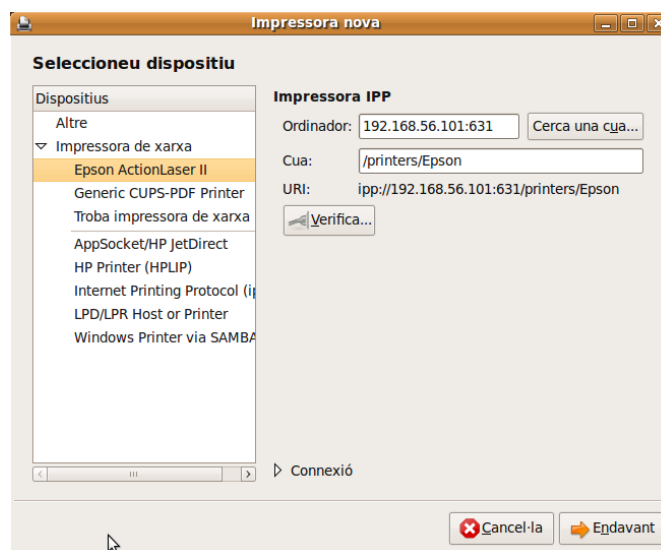
El CUPS fa servir el PPD per a totes les seves impressores. Redirigint la sortida per mitjà d'un filtre, ha estès el concepte per a permetre impressió PostScript en impressores que no són PostScript. Aquest filtre ja no és un PPD estàndard, sinó que més aviat és un "CUPS-PPD".

2. Configuració del servidor per compartir impressores i fer que siguin visibles per mitjà de la xarxa. Per tal que les màquines de la xarxa local puguin accedir a les impressores que gestiona el servidor CUPS, és a dir, per tal que el servidor comparteixi les impressores, haurem de seleccionar, en la secció *Server* de la pestanya *Administration*, les opcions **Show printers shared by other systems** (d'aquesta manera ens mostrarà les impressores per mitjà de la xarxa) i **Share published printers connected to this system** (d'aquesta manera ens permetrà compartir impressores públiques connectades al sistema). Si es pot accedir al servidor des d'Internet i volem que es pugui imprimir, marcarem l'opció **Allow printing from Internet**.

Per altra banda, si volem administrar remotament el servidor, és a dir, accedir a la configuració via web des d'un altra màquina, haurem de marcar l'opció **Allow remote administration**, que també és en la secció *Server* de la pestanya *Administration*. Es mostra en la figura 2.14.

FIGURA 2.14. Exemple de secció Server de CUPS

3. Configuració del client per detectar i utilitzar les impressores compartides pel servidor CUPS. Per tal que el client utilitzi les impressores remotes instal·lades en el servidor CUPS, des de l'Ubuntu, instal·lat en la màquina client, anirem al menú *Sistema > Administració > Impressió*. En seleccionar l'opció *Impressió* del menú, apareixerà una pantalla en què ens mostrarà les impressores que ja tenim configurades. En aquesta pantalla haurem de seleccionar la icona *Nou > Impressora*. Aleshores començarà un procés de cerca de les impressores que detecti l'equip. Al final d'aquest procés se'ns obrirà el quadre *Impressora nova* que veiem en la figura 2.15.

FIGURA 2.15. Quadre per afegir una impressora nova

Si ens ha detectat la impressora que volem instal·lar, només caldrà que premem el botó **Endavant**.

A continuació, apareixerà un quadre en què ens demanarà el nom mitjançant el qual volem que es reconegui la impressora en el sistema. De manera opcional, també ens demanarà una ubicació i una descripció d'aquesta impressora. Després d'especificar les dades anteriors, haurem de fer clic a **Aplica** i així conclourà el procés d'instal·lació.

Finalment, el sistema ens proposarà imprimir una pàgina de prova perquè puguem

estar segurs que la instal·lació s'ha fet correctament.

Si, per contra, en el quadre **Impressora nova** no es mostra la impressora que volem instal·lar, tenim dues possibilitats:

- Seleccionar l'opció **Altre** i especificar tot l'URI de la impressora que volem instal·lar en el format següent:

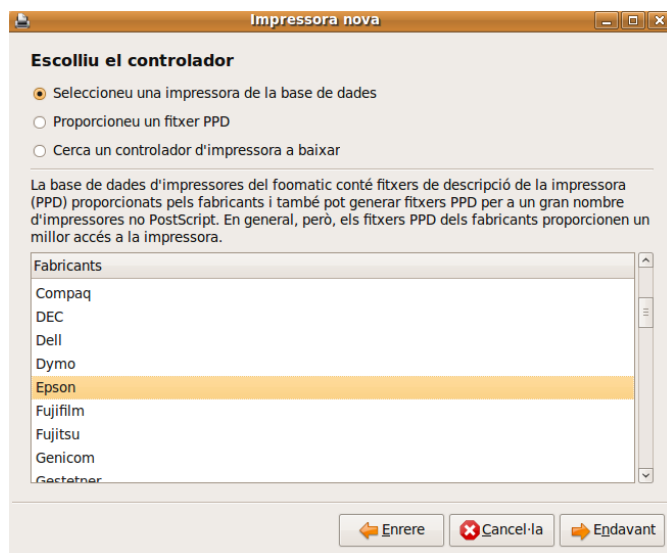
```
1 ipp://nom_o_ip_servidor/printers/nom_impresora
```

- Seleccionar, en la part dreta del quadre, l'opció **Internet printing protocol (IPP)** i especificar en cada quadre de text els valors dels paràmetres demanats: ordinador (nom o adreça IP del servidor), cua (afegir el nom de la impressora).

Una vegada especificats els paràmetres de la impressora que volem instal·lar en una de les dues opcions anteriors, clicarem a **Endavant**.

A continuació, ens mostrarà una pantalla com la de la figura 2.16, en què ens donarà la possibilitat d'escollir entre tres opcions: seleccionar una marca d'impressora de la base de dades de controladors del sistema, proporcionar un fitxer PPD en què especifiquem el controlador o cercar el controlador a baixar. Normalment escollirem la marca de la impressora que volem instal·lar i polsarem el botó **Endavant**.

FIGURA 2.16. Opcions de selecció en instal·lar una impressora nova



Seguidament haurem d'escollir el model concret dins dels controladors de la marca seleccionada anteriorment. Escollirem el més adequat per a la impressora concreta i farem **Endavant**.

A continuació apareixerà un quadre en què ens demanarà el nom mitjançant el qual volem que es reconegui la impressora en el sistema. De manera opoional, també ens demanarà una ubicació i una descripció de la impressora. Després

d'especificar aquestes dades, pulsarem el botó **Aplica** i així conclourà el procés d'instal·lació.

Finalment, el sistema ens proposarà imprimir una pàgina de prova perquè puguem estar segurs que la instal·lació s'ha fet correctament.

2.10.4 Samba i CUPS

El servei Samba integra el servei d'impressió CUPS i està configurat per tal que, per defecte, faci servir aquest sistema. Tot i que el Samba també suporta altres estils o sistemes d'impressió, el paràmetre **printing**, el qual determina el sistema d'impressió, té el valor *cups* per defecte.

La combinació del Samba i el CUPS permet la compartició d'impressores entre màquines GNU/Linux i màquines Windows. En xarxes que són formades totalment per màquines GNU/Linux, proporciona al servei CUPS més control de l'accés a les impressores compartides. Això és degut a les polítiques de seguretat i de gestió d'usuaris del Samba, ja que la configuració global d'aquest servidor, a diferència del CUPS, permet determinar quins usuaris poden accedir als seus recursos i quins no.

Per exemple, si fem servir la compartició d'impressores via CUPS, podem determinar si una màquina de la xarxa pot accedir o no a les impressores, però no quins usuaris concrets de cada màquina hi tenen accés i quins no. Si utilitzem el Samba, en canvi, podem distingir entre els usuaris i/o els grups d'una màquina que tenen accés a les impressores del servidor CUPS i els que no hi tenen accés.

Compartir impressores amb el Samba fent servir el CUPS

La compartició d'impressores via Samba entre sistemes GNU/Linux és molt similar a la compartició d'impressores amb el CUPS. El procés de compartició també consta d'una sèrie de passos.

1. Instal·lació de les impressores a compartir en el servidor Samba. La instal·lació de les impressores la podem fer de la mateixa manera que es fa en el servidor CUPS. Tanmateix, si tenim les impressores connectades físicament al servidor Samba, també la podem fer localment. Se suposa que aquests dos tipus d'instal·lació ja es coneixen.

2. Configuració del servidor Samba per a la compartició de les impressores. L'eina Swat permet portar a terme dues opcions: configurar les opcions de compartició d'impressores amb la secció [printers] o bé afegir cada impressora a compartir com un recurs nou amb els paràmetres que vulguem. En la figura [2.17](#) es mostra la segona opció, és a dir, afegir la impressora com un recurs nou.

FIGURA 2.17. Exemple de compartició d'una impressora amb Swat

Per defecte, el Samba treballa sobre el sistema CUPS.

3. Configuració del client per detectar i utilitzar les impressores compartides pel servidor Samba. La configuració s'assembla molt a la del servidor CUPS, però hi ha unes quantes diferències. Un cop siguem en el sistema Ubuntu instal·lat en la màquina client, anirem al menú *Sistema > Administració > Impressió*. Apareixerà una pantalla en què ens mostrarà les impressores que ja tenim configurades. En aquesta pantalla seleccionarem la icona *Nou > Impressora* i aleshores començarà un procés de cerca de les impressores detectades per l'equip. Al final d'aquest procés, s'obrirà el quadre *Impressora nova*.

Una vegada obert el quadre, tenim dues possibilitats:

- Seleccionar l'opció *Altre* i especificar tot l'URI de la impressora que volem instal·lar en el format següent:

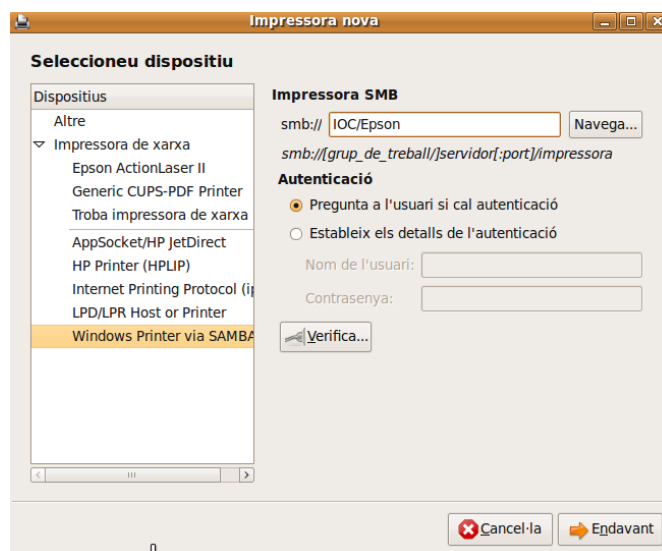
```
1 smb://[grup_de_treball]nom_o_ip_servidor[:port]/nom_impressora
```

- Seleccionar, en la part dreta del quadre, l'opció *Windows Printer via SAMBA* i especificar en cada quadre de text els valors dels paràmetres demanats.

En el quadre de text smb especificarem les dades corresponents amb el format següent:

```
1 smb://[grup_de_treball]nom_o_ip_servidor[:port]/nom_impressora
```

A continuació, determinarem si cal que, a l'hora d'imprimir, el sistema demani les dades d'autenticació a l'usuari o utilitzi les dades especificades en aquesta pantalla (figura 2.18).

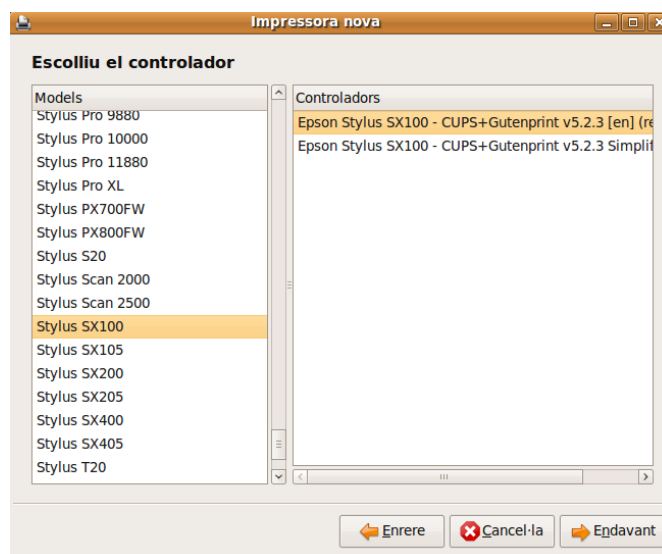
FIGURA 2.18. Pantalla de configuració d'una impressora nova al client

Una vegada especificats els paràmetres de la impressora que volem instal·lar, premerem el botó **Endavant**.

A continuació, ens mostrarà una pantalla en què ens demanarà que seleccionem una marca d'impressora de la base de dades de controladors del sistema, que li proporcionem el controlador en un fitxer PPD o que cerquem el controlador a baixar.

Normalment escollirem la marca de la impressora que volem instal·lar i farem **Endavant**.

A continuació, haurem d'escollir el model concret dins dels controladors de la marca seleccionada anteriorment. Escollirem el més adequat per a la impressora, com veiem a la figura 2.19 i farem **Endavant**.

FIGURA 2.19. Pantalla per escollir el tipus d'impressora

Seguidament, apareixerà un quadre en què ens demanarà el nom mitjançant el

qual volem que es reconegui la impressora en el sistema. De manera opcional, també ens demanarà una ubicació i una descripció d'aquesta impressora. Després d'especificar aquestes dades, haurem de prémer el botó **Aplica** i així conclourà el procés d'instal·lació.

Finalment, el sistema ens proposarà imprimir una pàgina de prova perquè puguem estar segurs que la instal·lació s'ha fet correctament.