Integración de redes con OpenLDAP, Samba, CUPS y PyKota

Sergio González González
Instituto Politécnico de Bragança (http://www.ipb.pt/), Portugal

sergio.gonzalez@hispalinux.es

Integración de redes con OpenLDAP, Samba, CUPS y PyKota

por Sergio González González

Trabajo realizado para la asignatura *Gestão de Sistemas e Redes* y ampliado para la asignatura *Comunicações por Computador II*, ambas pertenecientes a la carrera *Ingeniería Informática* impartida en la Escola Superior de Tecnologia e de Gestão de Bragança (http://www.estig.ipb.pt/) del Instituto Politécnico de Bragrança (http://www.ipb.pt/), Portugal.

Este documento muestra los pasos necesarios para conseguir la integración de una red compuesta por equipos con sistemas operativos GNU/Linux (http://www.linux.org/) y MS Windows. Las herramientas empleadas para conseguir dicha integración han sido: OpenLDAP, Samba, CUPS y PyKota.

Historial de revisiones

Revisión 0.2 15-10-2004 Revisado por: sgg
Revisión del documento, añadido soporte de cifrado en todo el proceso y cambio de licencia de publicación.
Revisión 0.1 19-06-2004 Revisado por: sgg
Documento inicial

Tabla de contenidos

Lista de tablas

Prefacio

introducción

Está leyendo un documento sobre la integración de las tecnologías OpenLDAP, Samba, CUPS y PyKota en un sistema Debian GNU/Linux. Por si no tiene conocimiento de qué realizan cada una de estas tecnologías, de forma muy resumida, se muestra a continuación:

- **OpenLDAP.** es una implementación *open source* del protocolo LDAP (*Lightweight Directory Access Protocol*).
- **Samba.** es una suite que permite la interconexión, a través de la red, de sistemas Windows, Unix y otros sistemas operativos, haciendo uso de los protocolos de red nativos de Windows.
- **CUPS.** acrónimo de *Common Unix Printing System*, es un sistema de impresión portable y extensible para Unix.
- **PyKota.** PyKota es una aplicación GPL para dar soporte de cuotas de impresión a CUPS y LPRng (LPR Next Generation) en sistemas GNU/Linux y similares a Unix.

Si alguna vez ha tenido que realizar labores de administración en redes heterogéneas, en las cuales existan múltiples clientes, y cada uno de ellos pueda tener un sistema operativo distinto, sobre el cual puedan operar una infinidad de usuarios; se habrá dado cuenta de la complejidad que esto conlleva. Por poner un simple ejemplo, si no posee una base de datos de usuarios común a todos los clientes, tendría que dar de alta a cada nuevo cliente en cada una de las máquinas que quisiese utilizar. Piense ahora que ocurriría si, por un cambio de política de su empresa, se tenga que modificar cierto aspecto en todas las cuentas de los usuarios existentes...

Si entramos en la compartición de archivos entre los distintos usuarios, o el almacenamiento de los documentos de un determinado usuario, que puede utilizar múltiples clientes, la cosa se complica. Y si a todo esto se le añade la gestión de las cuotas de impresión de todos y cada uno de los usuarios, se hace necesario buscar un método que facilite, en la medida de lo posible, la labor de administración.

Este documento intenta presentar un método para facilitar la integración de este tipo de redes. La idea es utilizar un directorio LDAP como base de datos común para almacenar la información relativa a los usuarios (bien sea la información personal, la relativa a las cuentas Unix, la relativa a las cuentas Samba/Windows o bien las cuotas de impresión asociadas a un usuario o grupo de usuarios).

Samba proveerá la integración de redes Unix/Windows, de forma que se simplifique sobremanera el intercambio y almacenamiento de información de los usuarios. Samba permitirá, por ejemplo, tener un único *HOME* por usuario, independientemente del cliente que se utilice. También actuará como PDC (Servidor Primario de Dominio) de la red donde se encuentre, entre otras cosas.

Con CUPS y PyKota se implementará el sistema de impresión con soporte para cuotas. Y si a estas dos herramientas se las integra con Samba y LDAP, se estará posibilitando la impresión y el control de impresión a todos los usuarios, independientemente del sistema operativo utilizado.

Organización

Este documento está organizado, principalmente, en 5 grandes bloques: la parte dedicada a OpenLDAP, la parte dedicada a Samba, la parte dedicada a CUPS, la parte dedicada a PyKota y los apéndices.

A continuación se verá una breve descripción para cada una de estas partes:

OpenLDAP

Este apartado (Parte I en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*) está formado por 5 capítulos:

- Capítulo 1: capítulo introductorio al protocolo LDAP y su funcionamiento, así como la descripción de los demonios **slapd** y **slurpd**, pertenecientes al proyecto OpenLDAP. Finalmente se proporciona información relativa al proyecto OpenLDAP.
- Capítulo 2: la instalación de OpenLDAP, la ejecución del demonio slapd y la conexión con el servidor LDAP, son los temas tratados en este capítulo.
- Capítulo 3: primeras modificaciones realizadas sobre la instalación de OpenLDAP: cambio de usuario de ejecución para el demonio slapd, especificación de las interfaces donde escuchar y permisos que debería tener los archivos de configuración.
- Capítulo 4: la conexión segura con el servidor OpenLDAP se trata en este capítulo, que va desde la creación de los certificados, pasando por la configuración de OpenLDAP para que soporte conexiones cifradas, para finalizar con una serie de pruebas sobre el sistema.
- Capítulo 5: modificaciones y software necesario para que un sistema Unix permita la autentificación de usuarios a partir de un directorio LDAP.

Samba

Este apartado (Parte II en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*) está formado por 7 capítulos:

- Capítulo 6: capítulo que describe, en primer lugar las capacidades de Samba, luego describe los aspectos más importantes de las redes SMB/CIFS y dominios de Windows, para finalizar con un breve informe sobre el proyecto Samba.
- Capítulo 7. Instalación de los paquetes necesarios para la ejecución de un servidor Samba.
- Capítulo 8. Breve capítulo dedicado a las modificaciones que se han de realizar en la configuración de OpenLDAP, para que Samba pueda hacer uso de dicho directorio para el almacén de su información relativa.
- Capítulo 9. Inicialmente explica la estructura de un archivo de configuración para Samba, para terminar con un repaso por las principales opciones de configuración de Samba, relacionadas con los objetivos de esta documentación.
- Capítulo 10. Modificaciones finales sobre la configuración de OpenLDAP y sobre el sistema que aloja a Samba.

- Capítulo 11, en este capítulo se hacen una serie de pruebas al sistema. Estas consisten en la verificación del archivo de configuración de Samba, la creación de un nuevo usuario y verificación de acceso al sistema con el nuevo usuario.
- Capítulo 12. Este capítulo explica el proceso que se ha de seguir para añadir clientes Windows 95/98/ME, Windows NT, Windows 2000 y Windows XP al dominio de Samba.

CUPS

Este apartado (Parte III en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*) está formado por 3 capítulos:

- Capítulo 13: capítulo que hace un breve recorrido por la historia de CUPS, explicando seguidamente las características del diseño de este sistema de impresión para finalizar con un breve informe sobre el proyecto CUPS.
- Capítulo 14. La instalación de CUPS comienza con un análisis y selección de los paquetes existentes en Debian, seguido de la instalación de los paquetes seleccionados.
- Capítulo 15. Aquí se realiza la configuración de CUPS, preparándolo para el soporte de OpenLDAP, creando nuevas impresoras e instalando los drivers necesarios para los clientes Windows.

PyKota

Este apartado (Parte IV en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*) está formado por 8 capítulos:

- Capítulo 16: capítulo que muestra, inicialmente, una comparativa con otros sistemas de control de cuotas de impresión. Luego repasa las características y funcionalidades de PyKota para terminar con un breve informe sobre el proyecto PyKota.
- Capítulo 17. Este capítulo muestra el proceso que se ha de seguir para obtener un un paquete *deb* de PyKota, a partir de su código fuente.
- Capítulo 18. Instalación del paquete *deb* de PyKota.
- Capítulo 19: retoques realizados en la configuración de OpenLDAP para que soporte el almacenamiento de los datos de PyKota.
- Capítulo 20. Breve repaso sobre los aspectos más importantes para la configuración de PyKota.
- Capítulo 21. Modificaciones realizadas en CUPS para el soporte de cuotas de impresión con PyKota.
- Capítulo 22. Aquí se establecen los precios de impresión así como las cuotas de los usuarios.
- Capítulo 23: capítulo en el que se realiza una prueba sobre el sistema de cuotas de impresión.

Apéndices

Este apartado está formado por 4 grupos de apéndices:

- Parte V en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*, en este apéndice se tratan temas adicionales a la documentación, como funcionalidades extra o distintas a las mostradas en la documentación, como instalar determinado software o la disponibilidad de los scripts utilizados para la realización de esta documentación, entre otras cosas.
- Parte VI en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*, aquí se pueden encontrar los archivos de configuración más importantes de las aplicaciones empleadas en esta documentación.
- Parte VII en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*, licencias relacionadas, de alguna manera, con el software utilizado para la realización de esta documentación, así como la licencia de la documentación en sí.
- Parte VIII en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*, información sobre los derechos de copia de los distintos programas utilizados para la generación de esta documentación.

Convenciones utilizadas en esta documentación

Las siguientes convenciones de texto se utilizan a lo largo de todo el documento:

`nombre-de-un-archivo`: representa el nombre de un archivo.

`nombre-de-un-directorio`: representa el nombre de un directorio.

nombre-aplicacion: indica el nombre de una aplicación.

orden: indica el nombre de una orden, o la ejecución de una orden con algunos parámetros asociados.

cursiva: todo aquel texto que por alguna razón necesita ser remarcado sobre el resto, bien sea por ser un anglicismos, bien por ser el nombre de un usuario del sistema.

“texto-entre-comillas”: todo aquel texto que por alguna razón necesita ser remarcado sobre el resto, bien sea por ser un anglicismos, bien por ser el nombre de un usuario del sistema.

ACRÓNIMO: palabra que representa un acrónimo.

Alt+**F2**: indica la pulsación simultánea de las teclas *Alt* y *F2*.

❶: `resalta una parte de un texto, que posteriormente tendrá una breve explicación.`

Bloque de texto, utilizado para resaltar en algún momento un trozo de texto.

Nota: Indica un apunte sobre el tema que se esté tratando cerca de este texto.

Sugerencia: Sugiere algo relativo al texto cercano.

Importante: Informa de algo a tener en cuenta con respecto al texto cercano.

Aviso

Advierte algo relativo al texto cercano.

`$` *-> prompt del sistema, en este caso representa la ejecución de código como un usuario cualquiera del sistema, no el usuario root.*

`#` *-> prompt del sistema, en este caso representa la ejecución de código como el usuario root.*

`/usr/bin/tree -L 1 /` *-> Representa las órdenes tecleadas por el usuario.*

```
/
|-- bin
|-- boot
|-- cdrom -> media/cdrom
|-- dev
|-- etc
|-- home
|-- initrd
|-- lib
|-- lib64
|-- media
|-- mnt
|-- nonexistent
|-- opt
|-- proc
|-- root
|-- sbin
|-- srv
|-- sys
|-- tmp
|-- usr
|-- var
|-- vmlinuz -> boot/vmlinuz-2.6.8.1-01
`-- vmlinuz.old -> boot/vmlinuz-2.6.7-1-386
```

`21 directories, 2 files` *-> Representa la salida del ordenador, tras la ejecución de una orden por parte de un usuario.*

Ejemplo 1. Ejemplo de ejemplo

Muestra un ejemplo sobre algún tema determinado.

* Listado de código
* Ejemplos de archivos de configuración
* etc.

Agradecimientos

Los primeros pensamientos y agradecimientos van dirigidos a todos y cada uno de los desarrolladores que han hecho posible que el software utilizado para realizar esta documentación exista.

Tampoco hay que olvidar a las dos personas que han hecho que esta documentación se llevase a cabo:

- Rui Pedro Lopes (http://www.ipb.pt/~rlopes/) <`rlopes (en) ipb (punto) pt`>
- Nuno Gonçalves Rodrigues (http://www.ipb.pt/~nuno/) <`nuno (en) ipb (punto) pt`>

La siguiente lista, muestra aquellas personas que de alguna u otra forma, han participado en la realización de esta documentación. El orden utilizado para la presentación es completamente aleatorio.

- Juan Sierra Pons <`juansierrapons (en) yahoo (punto) es`> (*Sugerencia para indicar el orden de los esquemas en el Capítulo 8.*)
- Juan José Muñoz Martín <`juanjo.munoz (en) yecla (punto) es`> (*Gracias a sus correos, aclaración de ciertos aspectos en el Capítulo 4*)

I. OpenLDAP

Capítulo 1. Conceptos teóricos

Introducción

Este capítulo hace una breve introducción al servicio de directorios, profundizando un poco más en la implementación realizada por OpenLDAP.

> **Nota:** Los conceptos teóricos se han basado en la introducción de la entrada bibliográfica OpenLDAPProject01

¿Qué es un servicio de directorios?

Un directorio es una base de datos optimizada para lectura, navegación y búsqueda. Los directorios tienden a contener información descriptiva basada en atributos y tienen capacidades de filtrado muy sofisticada. Los directorios generalmente no soportan transacciones complicadas ni esquemas de vuelta atrás como los que se encuentran en los sistemas de bases de datos diseñados para manejar grandes y complejos volúmenes de actualizaciones. Las actualizaciones de los directorios son normalmente cambios simples, o todo o nada, siempre y cuando estén permitidos. Los directorios están afinados para dar una rápida respuesta a grandes volúmenes de búsquedas. Estos tienen la capacidad de replicar la información para incrementar la disponibilidad y la fiabilidad, al tiempo que reducen los tiempos de respuesta. Cuando la información de un directorio se replica, se pueden producir inconsistencias temporales entre las réplicas mientras esta se está sincronizando.

Hay muchas formas diferentes de proveer un servicio de directorio. Diferentes métodos permiten almacenar distintos tipos de información en el directorio, tener distintos requisitos sobre como la información ha de ser referenciada, consultada y actualizada, como es protegida de los accesos no autorizados, etc. Algunos servicios de directorio son locales, es decir, proveen el servicio a un contexto restringido (como por ejemplo, el servicio *finger* en una única máquina). Otros servicios son globales y proveen servicio a un contexto mucho más amplio (como por ejemplo, Internet). Los servicios globales normalmente son distribuidos, esto significa que los datos están repartidos a lo largo de distintos equipos, los cuales cooperan para dar el servicio de directorio. Típicamente, un servicio global define un espacio de nombres uniforme que da la misma visión de los datos, independientemente de donde se esté, en relación a los propios datos. El servicio DNS (Domain Name System) es un ejemplo de un sistema de directorio globalmente distribuido.

¿Qué es LDAP?

LDAP son las siglas de *Lightweight Directory Access Protocol*. Como su propio nombre indica, es un protocolo ligero para acceder al servicio de directorio, especialmente al basado en X.500. LDAP se ejecuta sobre TCP/IP o sobre otros servicios de transferencia orientado a conexión. La definición detallada de LDAP está disponible en el RFC2251 (http://www.rfc-editor.org/rfc/rfc2251.txt) “The

Lightweight Directory Access Protocol (v3)" y en otro documento que comprende las especificaciones técnicas, RFC3377 (http://www.rfc-editor.org/rfc/rfc3377.txt).

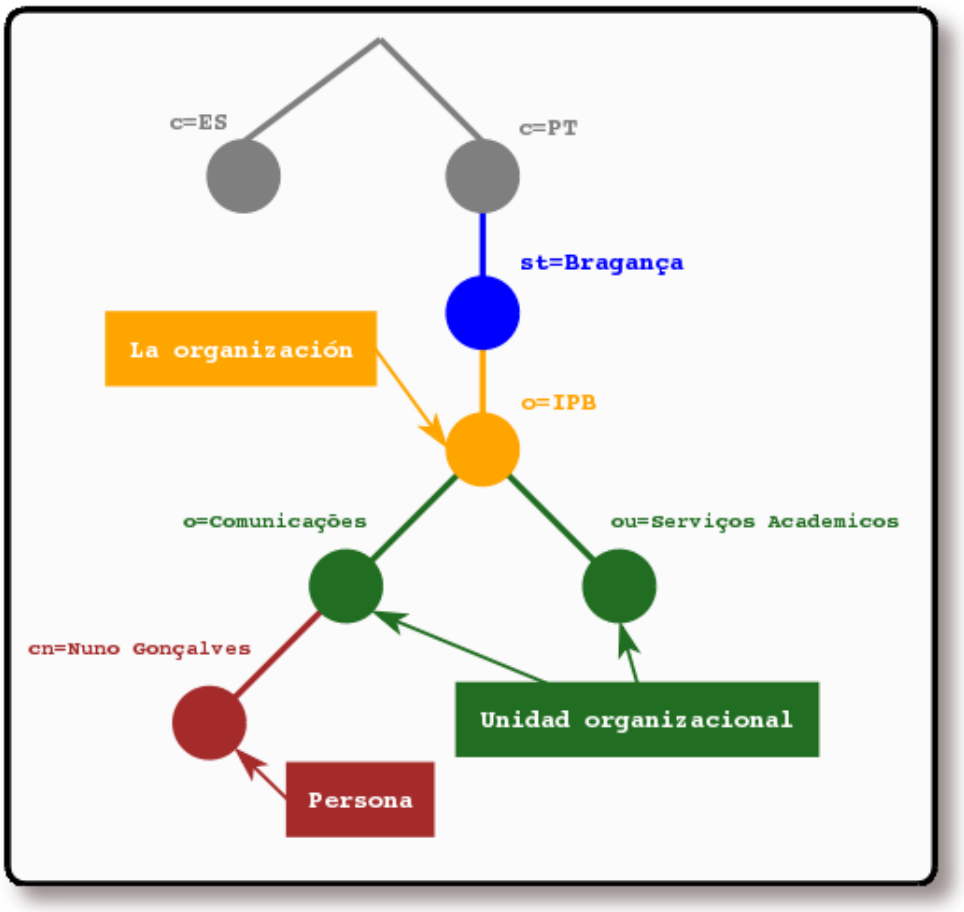
¿Qué tipo de información se puede almacenar en un directorio?

El modelo de información de LDAP está basado en entradas. Una entrada es una colección de atributos que tienen un único y global Nombre Distinguido[1] (DN). El DN se utiliza para referirse a una entrada sin ambigüedades. Cada atributo de una entrada posee un tipo y uno o más valores. Los tipos son normalmente palabras nemotécnicas, como "cn" para *common name*, o "mail" para una dirección de correo. La sintaxis de los atributos depende del tipo de atributo. Por ejemplo, un atributo *cn* puede contener el valor "Sergio González". Un atributo email puede contener un valor "sergio@ejemplo.com". El atributo *jpegPhoto* ha de contener una fotografía en formato JPEG.

¿Cómo se almacena la información?

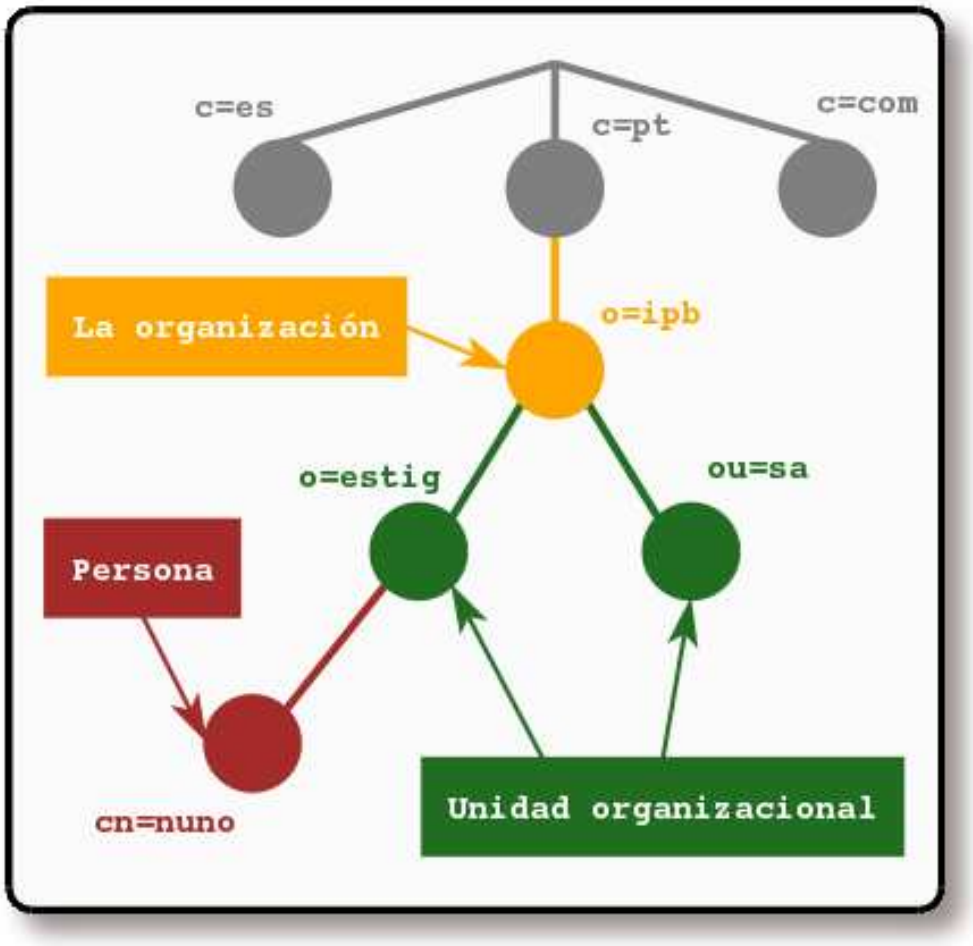
En LDAP, las entradas están organizadas en una estructura jerárquica en árbol. Tradicionalmente, esta estructura reflejaba los límites geográficos y organizacionales. Las entradas que representan países aparecen en la parte superior del árbol. Debajo de ellos, están las entradas que representan los estados y las organizaciones nacionales. Debajo de estás, pueden estar las entradas que representan las unidades organizacionales, empleados, impresoras, documentos o todo aquello que pueda imaginarse. La Figura 1-1 muestra un ejemplo de un árbol de directorio LDAP haciendo uso del nombramiento tradicional.

Figura 1-1. Árbol del directorio LDAP (nombramiento tradicional)[2]



El árbol también se puede organizar basándose en los nombres de dominio de Internet. Este tipo de nombramiento se está volviendo muy popular, ya que permite localizar un servicio de directorio haciendo uso de los DNS. La Figura 1-2 muestra un ejemplo de un directorio LDAP que hace uso de los nombres basados en dominios.

Figura 1-2. Árbol del directorio LDAP (nombramiento de Internet)[3]



Además, LDAP permite controlar que atributos son requeridos y permitidos en una entrada gracias al uso del atributo denominado *objectClass*. El valor del atributo *objectClass* determina que reglas de diseño (*schema rules*) ha de seguir la entrada.

¿Cómo es referenciada la información?

Una entrada es referenciada por su nombre distinguido, que es construido por el nombre de la propia entrada (llamado *Nombre Relativo Distinguido*[4] o RDN) y la concatenación de los nombres de las entradas que le anteceden. Por ejemplo, la entrada para *Nuno Gonçalves* en el ejemplo del nombramiento de Internet anterior tiene el siguiente RDN: *uid=nuno* y su DN sería: *uid=nuno,ou=estig,dc=ipb,dc=pt*. El formato completo para los DN está descrito en el RFC2253 (http://www.rfc-editor.org/rfc/rfc2253.txt), “Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names.”

¿Cómo se accede a la información?

LDAP define operaciones para interrogar y actualizar el directorio. Provee operaciones para añadir y borrar entradas del directorio, modificar una entrada existente y cambiar el nombre de una entrada. La mayor parte del tiempo, sin embargo, LDAP se utiliza para buscar información almacenada en el directorio. Las operaciones de búsqueda de LDAP permiten buscar entradas que concuerdan con algún criterio especificado por un filtro de búsqueda. La información puede ser solicitada desde cada entrada que concuerda con dicho criterio.

Por ejemplo, imagínese que quiere buscar en el subárbol del directorio que está por debajo de *dc=ipb,dc=pt* a personas con el nombre *Nuno Gonçalves*, obteniendo la dirección de correo electrónico de cada entrada que concuerde. LDAP permite hacer esto fácilmente. O tal vez prefiera buscar las organizaciones que posean la cadena *IPB* en su nombre, posean número de fax y estén debajo de la entrada *st=Bragança,c=PT*. LDAP le permite hacer esto también. La siguiente sección describe con mayor detalle que se puede hacer con LDAP y como puede serle útil.

¿Cómo se protege la información de los accesos no autorizados?

Algunos servicios de directorio no proveen protección, permitiendo a cualquier persona acceder a la información. LDAP provee un mecanismo de autentificación para los clientes, o la confirmación de identidad en un servidor de directorio, facilitando el camino para un control de acceso que proteja la información que el servidor posee. LDAP también soporta los servicios de privacidad e integridad.

¿Cómo trabaja LDAP?

El servicio de directorio de LDAP está basado en el modelo *cliente/servidor*. Uno o más servidores LDAP contienen los datos que conforman la información del árbol del directorio[5] (DIT). El cliente se conecta a los servidores y les formula preguntas. Los servidores responden con una respuesta o con un puntero donde el cliente puede obtener información adicional (normalmente otro servidor LDAP). No importa a que servidor LDAP se conecte un cliente, este siempre obtendrá la misma visión del directorio; un nombre presentado por un servidor LDAP referencia la misma entrada que cualquier otro servidor LDAP. Esta es una característica muy importante del servicio global de directorio, como LDAP.

Sobre X.500

Técnicamente, LDAP es un protocolo de acceso a directorio para el servicio de directorio X.500, el servicio de directorio de OSI. Inicialmente, los cliente LDAP accedían a través de puertas de enlace al servicio de directorio X.500. Esta puerta de enlace ejecutaba LDAP entre el cliente y la puerta de enlace, y el Protocolo X.500 de Acceso al Directorio [6] (DAP) entre la puerta de enlace y el servidor X.500. DAP es un protocolo extremadamente pesado que opera sobre una pila protocolar OSI completa y requiere una cantidad significativa de recursos computacionales. LDAP está diseñado para operar sobre TCP/IP proporcionando una funcionalidad similar a la de DAP, pero con un coste muchísimo menor.

Aunque LDAP se utiliza todavía para acceder al servicio de directorio X.500 a través de puertas de enlace, hoy en día es más común implementar LDAP directamente en los servidores X.500.

El demonio autónomo de LDAP, o slapd (8), puede ser visto como un servidor de directorio X.500 ligero. Es decir, no implementa el DAP X.500, sino un subconjunto de modelos de X.500.

Es posible replicar datos desde un servidor de directorio LDAP hacia un servidor DAP X.500. Esta operación requiere una puerta de enlace LDAP/DAP. OpenLDAP no suministra dicha puerta de enlace, pero el demonio de replicación que posee puede ser usado para la replicación, como si de una puerta de enlace se tratase.

¿Cuál es la diferencia entre LDAPv2 y LDAPv3?

LDAPv3 fue desarrollado en los años 90 para reemplazar a LDAPv2. LDAPv3 incorpora las siguientes características a LDAP:

- Autentificación fuerte haciendo uso de SASL
- Protección de integridad y confidencialidad haciendo uso de TLS (SSL)
- Internacionalización gracias al uso de Unicode
- Remisiones y continuaciones
- Descubrimiento de esquemas
- Extensibilidad (controles, operaciones extendidas y más)

LDAPv2 es histórico (RFC3494 (http://www.rfc-editor.org/rfc/rfc3494.txt)). Muchas implementaciones de LDAPv2 (incluyendo slapd (8)) no se adaptan a las especificaciones técnicas de LDAPv2, la interoperabilidad entre las distintas implementaciones de LDAPv2 es muy limitada. Como LDAPv2 difiere significativamente de LDAPv3, la interactuación entre ambas versiones puede ser un poco problemática. LDAPv2 ha de evitarse, por lo que en la implementación de OpenLDAP viene deshabilitado por defecto.

¿Qué es slapd y qué puede hacer?

slapd (8) es un servidor de directorio LDAP que se ejecuta en distintas plataformas. Algunas de las características más interesantes de slapd son:

LDAPv3:

slapd implementa la versión 3 de *Lightweight Directory Access Protocol*. slapd soporta LDAP sobre IPv4, IPv6 y Unix IPC.

Simple Authentication and Security Layer (SASL):

slapd tiene soporte de autentificación fuerte gracias al uso de SASL. La implementación SASL de slapd hace uso del software Cyrus SASL (http://asg.web.cmu.edu/cyrus/), el cual soporta un gran número de mecanismos de autentificación, como: DIGEST-MD5, EXTERNAL, y GSSAPI.

Transport Layer Security:

slapd provee protecciones de privacidad e integridad gracias al uso de TLS (o SSL). La implementación TLS de slapd hace uso del software OpenSSL (http://www.openssl.org/).

Control Topológico

slapd se puede configurar para restringir el acceso a la capa de socket basándose en la información topológica de la red. Esta característica hace uso de los TCP wrappers.

Control de Acceso:

slapd provee facilidades de control de acceso muy potentes, permitiéndole controlar el acceso a la información de su(s) base(s) de datos. Puede controlar el acceso a las entradas basándose en la información de autorización de LDAP, en la dirección IP, en los nombres de dominio y otros criterios. slapd soporta tanto el control de acceso a la información dinámico como estático.

Internacionalización:

slapd soporta Unicode y etiquetas de lenguaje.

Elección del *backend* de la base de datos:

slapd viene con una serie de *backends* para diferentes bases de datos. Estos incluyen DBD, un *backend* de una base de datos transaccional de alto rendimiento; LDBM, un *backend* ligero basado en DBM; SHELL, una interface para scripts de shell; y PASSWD, un *backend* simple para el archivo passwd (5). El *backend* BDB hace uso de Sleepycat Berkeley DB (http://www.sleepycat.com/). LDBM utiliza cualquiera de las siguientes: Berkeley DB (http://www.sleepycat.com/) o GDBM (http://www.gnu.org/software/gdbm/).

Muchas instancias de bases de datos:

slapd se puede configurar para servir a múltiples bases de datos al mismo tiempo. Esto significa que un único servidor slapd puede responder a peticiones de diferentes porciones lógicas del árbol de LDAP, haciendo uso del mismo o distintos *backends* de bases de datos.

IP genérica de módulos:

Si necesita más personalización, slapd le permite escribir sus propios módulos fácilmente. slapd consiste en dos partes diferentes: un *frontend* que maneja las comunicaciones protocolares con los clientes LDAP; y módulos que manejan tareas específicas como las operaciones con las bases de datos. Debido a que estas dos piezas se comunican a través de una API C bien definida, puede escribir sus propios módulos, que extenderán slapd de múltiples maneras. También existen numerosos módulos programables de bases de datos. Estos permiten a slapd acceder a fuentes de datos externas haciendo uso de lenguajes de programación populares (Perl (http://www.perl.com/), shell, SQL (http://www.jcc.com/SQLPages/jccs_sql.htm) y TCL (http://tcl.activestate.com/)).

Hilos:

slapd hace uso de hilos para obtener alto rendimiento. Un proceso único multihilo maneja todas las peticiones entrantes haciendo uso de una *piscina* de hilos. Esto reduce la carga del sistema a la vez que provee alto rendimiento.

Replicación:

slapd se puede configurar para que mantenga copias de la información del directorio. Este esquema de replicación, *un único maestro/múltiples esclavos*, es vital en ambientes con un volumen alto de peticiones, donde un único servidor slapd no podría proveer la disponibilidad ni la confiabilidad necesarias. slapd incluye también un soporte experimental para la replicación de *múltiples maestros*. slapd soporta dos métodos de replicación: Sync LDAP y slurpd (8).

Proxy caché:

slapd puede ser configurado como un servicio proxy de caché LDAP.

Configuración:

slapd es altamente configurable a través de un único archivo de configuración, que permite modificar todo aquello que se necesite cambiar. Las opciones por defecto son razonables, lo que facilita mucho el trabajo.

¿Qué es slurpd y que puede hacer?

slurpd (8) es un demonio que, con la ayuda de slapd, provee el servicio de replicación. Es el responsable de distribuir los cambios realizados en la base de datos slapd principal hacia las distintas réplicas slapd. Este demonio libera a slapd de preocuparse por el estado de las réplicas (si estas se han caído, no están accesibles cuando se ha producido un cambio, etc.); slurpd maneja automáticamente el reenvío de las

peticiones fallidas. slapd y slurpd se comunican a través de un simple archivo de texto, que es utilizado para almacenar los cambios ocurridos.

Información adicional sobre el proyecto

Página principal

El Proyecto OpenLDAP dispone de una página principal, http://www.openldap.org/, desde donde puede obtener mucha información sobre el proyecto. De hecho, para elaborar esta sección ha utilizado la información allí disponible.

Cómo obtener OpenLDAP

El código de OpenLDAP (http://www.openldap.org/software/) es de libre distribución (vea los The OpenLDAP Public License y Apéndice AU para más información) y su código fuente está disponible desde distintas fuentes, como se verá a continuación.

OpenLDAP dispone de distintas ramas de desarrollo, entre las que se encuentran:

- La versión *estable* (a la hora de escribir este documento era la versión 2.1.30), cuya característica es que el software que la compone ha sido ampliamente comprobado y se considera muy confiable.
- La *última liberación para uso general* (a la hora de escribir este documento eran las versiones 2.2.5 y 2.1.30), la cual no ha sido todo lo ampliamente testeada como para considerarla estable.
- La *liberación de pruebas*, ocasionalmente, los desarrolladores de OpenLDAP harán versiones *beta* o *gamma* u otro tipo de liberaciones. La característica de estas, es que sólo tienen el propósito de ser probadas, no son para el uso general.
- *Otras* liberaciones, cuya existencia puede tener múltiples motivos. Normalmente se suelen emplear para actualizar versiones antiguas de OpenLDAP (como por ejemplo las versiones 1.x y 2.0.x).

La forma de acceso al código fuente se detalla a continuación:

- **Acceso al CVS:** para más información visite esta (http://www.openldap.org/software/repo.html) página.
- **Uso de los mirrors:** Si desea bajarse el código fuente ya empaquetado, consulte los mirrors (http://www.openldap.org/software/download/OpenLDAP/MIRRORS) disponibles para hacerlo
- **Obtención directa de la página del proyecto:** Además de los métodos anteriores de obtención del código fuente, el Proyecto OpenLDAP pone a su disposición el código fuente en las siguientes ubicaciones:
  - Acceso por FTP y HTTP (http://www.openldap.org/software/download/OpenLDAP)
  - Acceso por FTP (ftp://ftp.openldap.org/pub/OpenLDAP)

De todas formas, la mayoría de las distribuciones de GNU/Linux disponen de paquetes binarios de OpenLDAP, si los necesitase. Obtenga la información de su distribución para comprobar que posee paquetes de este software.

Documentación

La página principal del Proyecto OpenLDAP dispone de una sección dedicada a la documentación, desde donde se pueden obtener documentos tan interesantes como OpenLDAPProject01, entre otros. Para más detalles, visite: http://www.openldap.org/doc/index.html

Información de soporte

La página dedicada al soporte de OpenLDAP (http://www.openldap.org/support/index.html), informa sobre los distintos métodos existentes para obtener ayuda en un determinado momento. Los métodos más importantes para obtener ayuda son los siguientes:

Faq-O-Matic: Sitio dedicado a las preguntas frecuentes sobre OpenLDAP: http://www.openldap.org/faq/

Listas de correo: El Proyecto OpenLDAP dispone varias listas de correo, entre las que se encuentran algunas como anuncios, bugs o desarrollo, siendo una fuente de información fiable y directa. En la siguiente página encontrará toda la información necesaria para acceder a dichas listas de correo: http://www.openldap.org/lists/

Servicio técnico de terceros: Muchas empresas ofrecen servicio técnico a la comunidad de OpenLDAP, un listado de las mismas se puede obtener desde: www.openldap.org/support/index.html (http://www.openldap.org/support/index.html)

Reporte de bugs

OpenLDAP dispone de un Sistema de seguimiento de tareas (http://www.openldap.org/its/index.html), desde donde se pueden reportar errores y bugs relacionados con OpenLDAP (tanto en lo relativo al software como a la documentación), hacer peticiones de nuevas características y realizar contribuciones al software.

Cómo contactar

Para obtener más información sobre OpenLDAP, puede contactar con el Proyecto en la siguiente dirección:

```
The OpenLDAP Project
c/o The OpenLDAP Foundation
270 Redwood Shores Pwy, PMB#107
Redwood City, California 94065
USA

<Project@OpenLDAP.org>
```

Notas

1. En inglés Distinguished Name.
2. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/openldap-LDAP_directory_tree_traditional_naming.dia).
3. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/openldap-LDAP_directory_tree_internet_naming.dia).
4. En inglés *Relative Distinguished Name*
5. En inglés *directory information tree*
6. En inglés *Directory Access Protocol*

Capítulo 2. Instalación

Consideraciones previas

La instalación y configuración de OpenLDAP se llevará a cabo de tal manera que al finalizarla, el sistema sobre el que se ha instalado debería estar listo para autentificar usuarios a través del servicio de directorios. Este es el objetivo final de este capítulo, en subsiguientes capítulos se irán añadiendo las funcionalidades necesarias para que cumpla con los requisitos del trabajo.

Se ha seleccionado la versión 2.1.30 de OpenLDAP, que acompaña a la versión en desarrollo de Debian GNU/Linux.

> **Nota:** A lo largo de todo el documento se asume que el dominio sobre el que se ejecutará OpenLDAP es “gsr.pt”, perteneciente a la empresa *gsr.pt*.
>
> Para obtener un sistema acorde a estas condiciones, se ha añadido la línea “gsr.pt” en el archivo `/etc/hosts` para intentar simular las condiciones reales.

Pasos para la instalación

Instalación de *slapd* y *ldap-utils*

El primer paso para instalar OpenLDAP, es instalar los paquetes *slapd* y *ldap-utils*. Veamos el procedimiento:

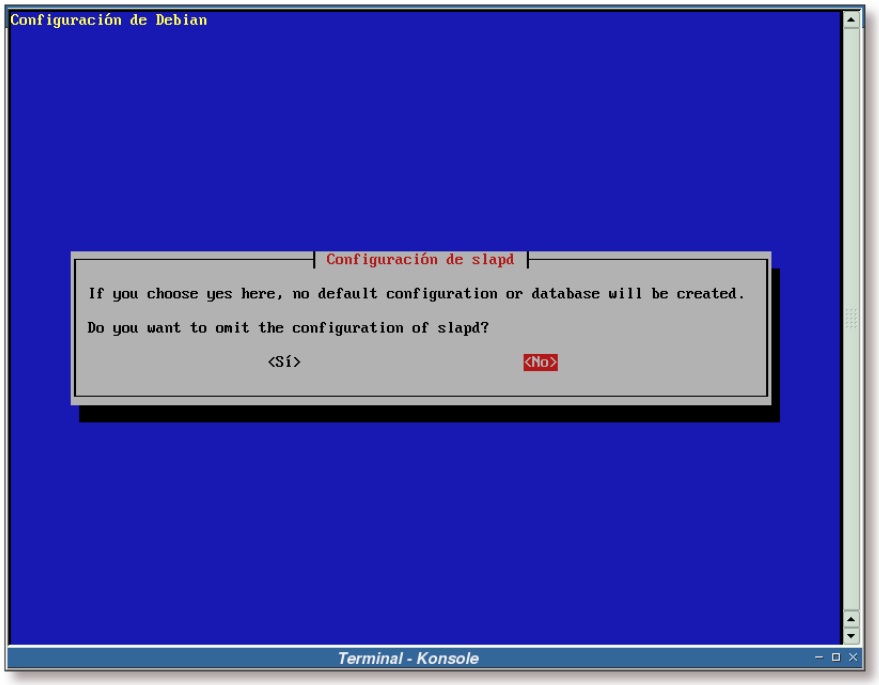
> **Aviso**
>
> Se ha de tener en cuenta que en algunas ocasiones no aparecen todas las capturas de pantalla que se muestran en el Ejemplo 2-1, eso se puede deber a que ya se haya instalado anteriormente **slapd** en el sistema o debido al nivel de preguntas elegido en la configuración de debconf. Si por cualquier motivo no apareciesen, puede forzar la configuración de **slapd** con la orden:
>
> ```
> # /usr/sbin/dpkg-reconfigure --priority=low slapd
> ```

Ejemplo 2-1. Instalación de los paquetes *slapd ldap-utils (primera parte)*

```
# apt-get install slapd ldap-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  ldap-utils slapd
0 actualizados, 2 se instalarán, 0 para eliminar y 1 no actualizados.
```

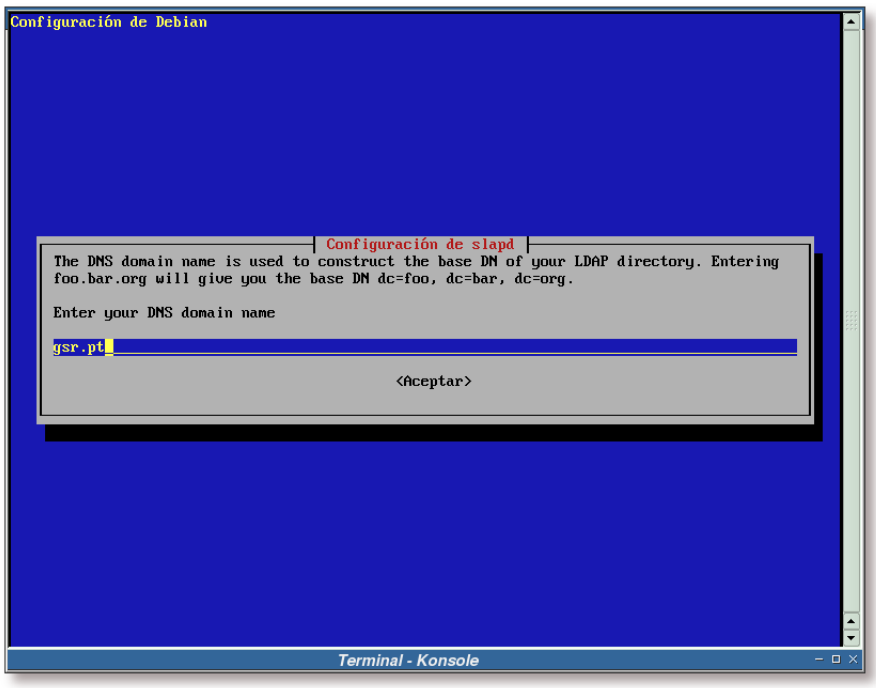
```
Se necesita descargar 0B/1042kB de archivos.
Se utilizarán 2884kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...
```

Figura 2-1. Configuración de slapd mediante debconf



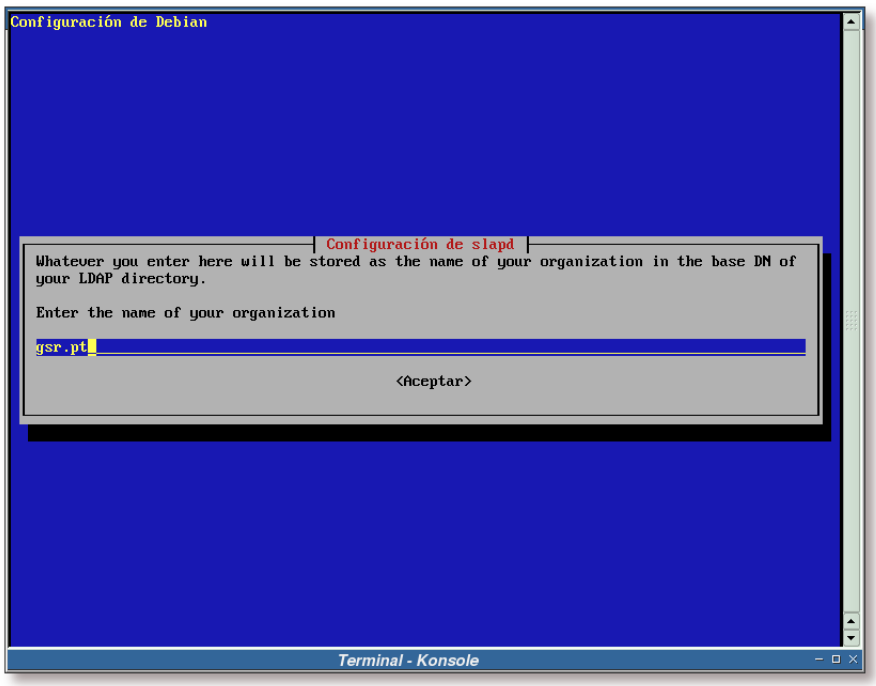
Si se quiere configurar algunos aspectos de **slapd** a través de debconf, responda *No*, en esta pantalla.

Figura 2-2. Configuración de slapd, elección del dominio



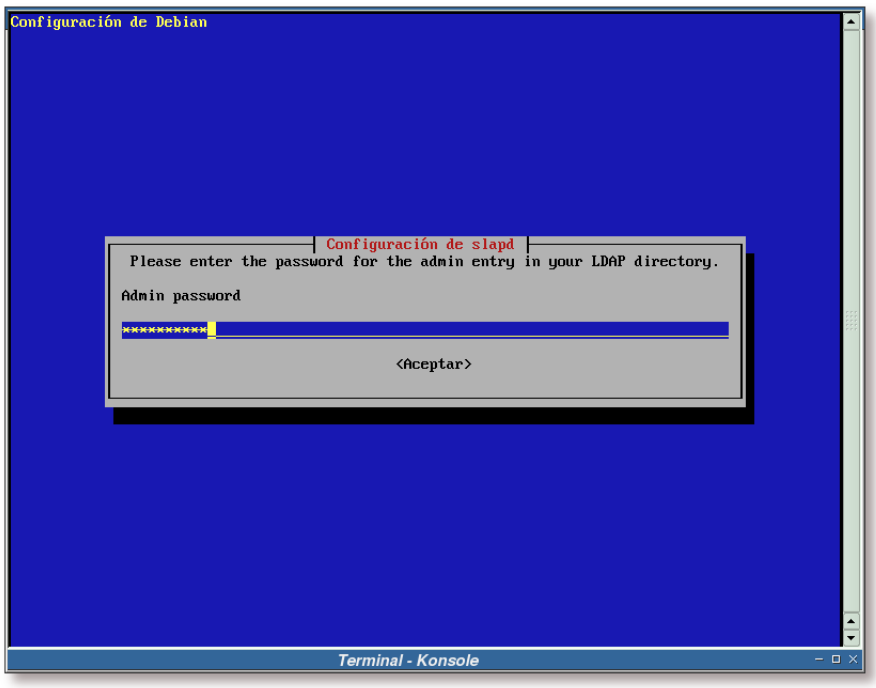
Esta pantalla se pide el dominio sobre el cual se va a ejecutar el servidor **slapd**, en este caso será el dominio *gsr.pt*.

Figura 2-3. Configuración de slapd, nombre de la organización



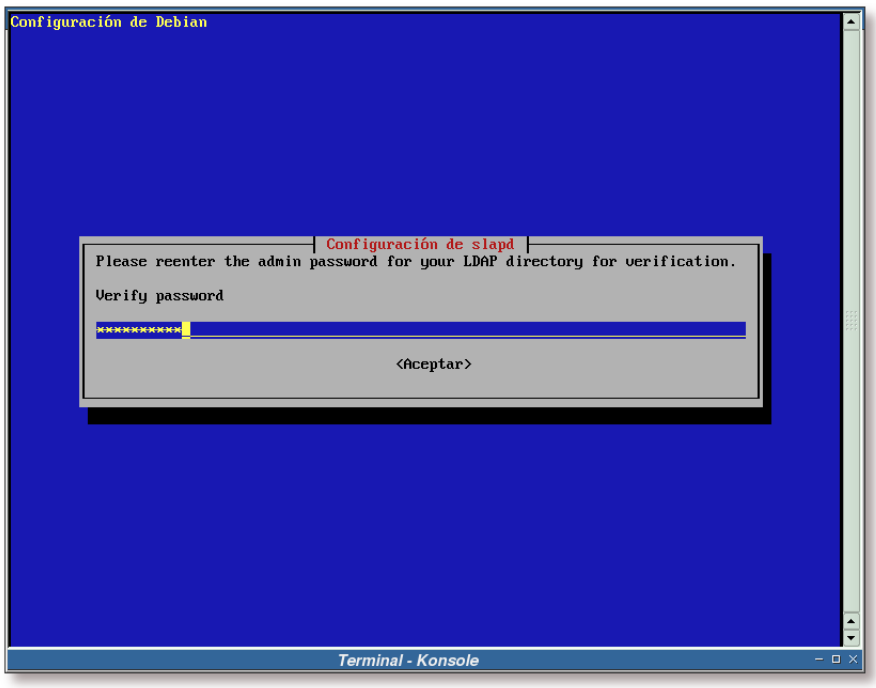
Solicitud del nombre de la organización que está instalando el servidor OpenLDAP. En este ejemplo se dejará el nombre del dominio anteriormente tecleado: *gsr.pt*.

Figura 2-4. Configuración de slapd, clave de administrador



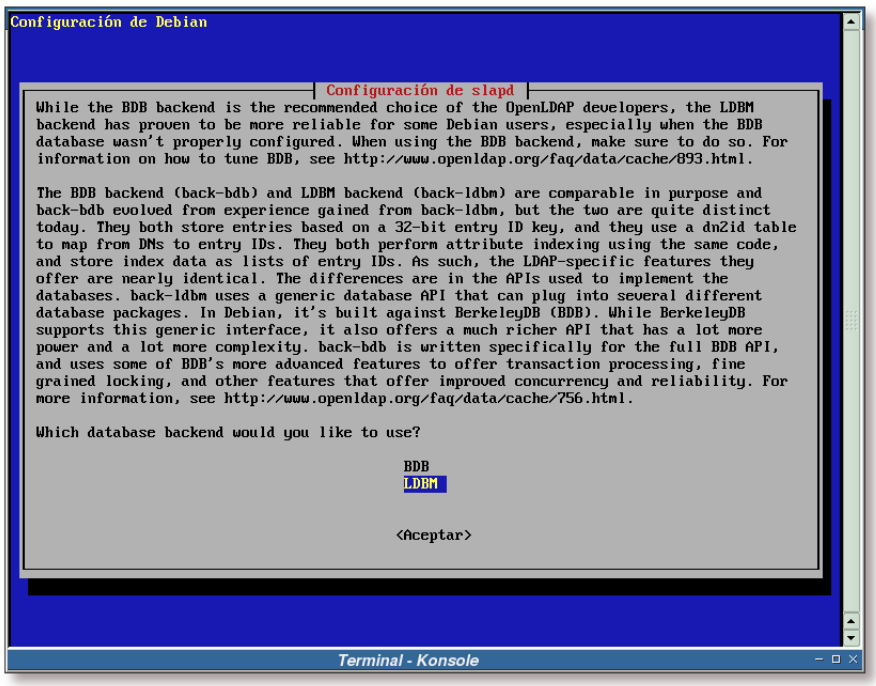
Pantalla de solicitud de la clave para el administrador del servicio LDAP. Este usuario es el superusuario (root) de OpenLDAP, por lo que se debería elegir una buena clave.

Figura 2-5. Configuración de slapd, repetir clave de administrador



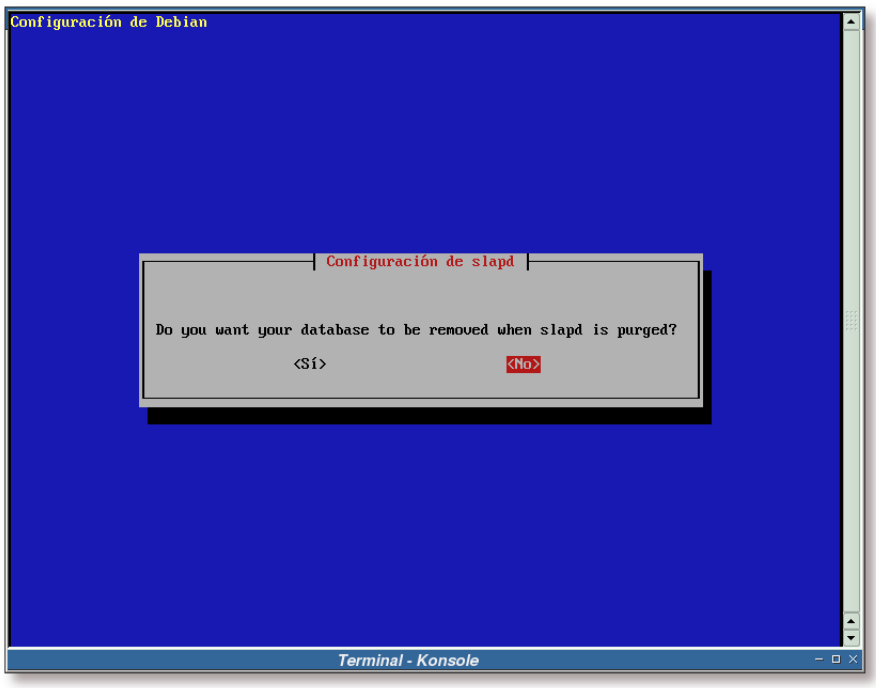
Verificación de la clave del administrador, se ha de teclear la misma que en la pantalla anterior.

Figura 2-6. Configuración de slapd, elección del backend de la BBDD



Elección del backend de la base de datos que utilizará OpenLDAP. En este ejemplo se elegirá LDBM.

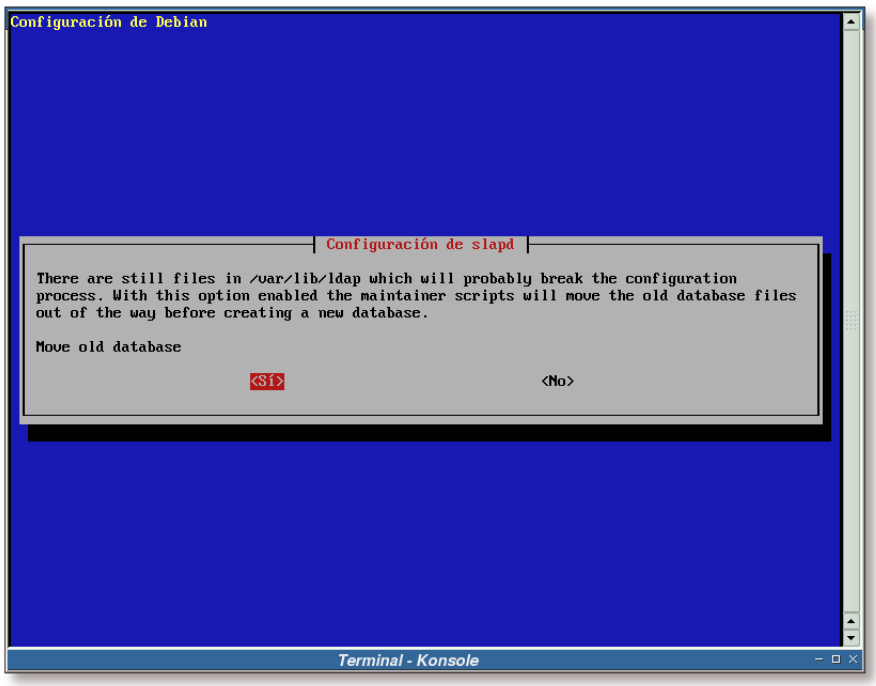
Figura 2-7. Configuración de slapd, ¿conservar los datos al desinstalarlo?



> **Aviso**
>
> Tenga cuidado con la elección de esta pantalla, puede perder los datos almacenados en la base de datos de OpenLDAP si “accidentalmente” se desinstala **slapd**.

Seleccionamos que *No* queremos que se borre la base de datos de OpenLDAP al desinstalarse el servidor **slapd**.

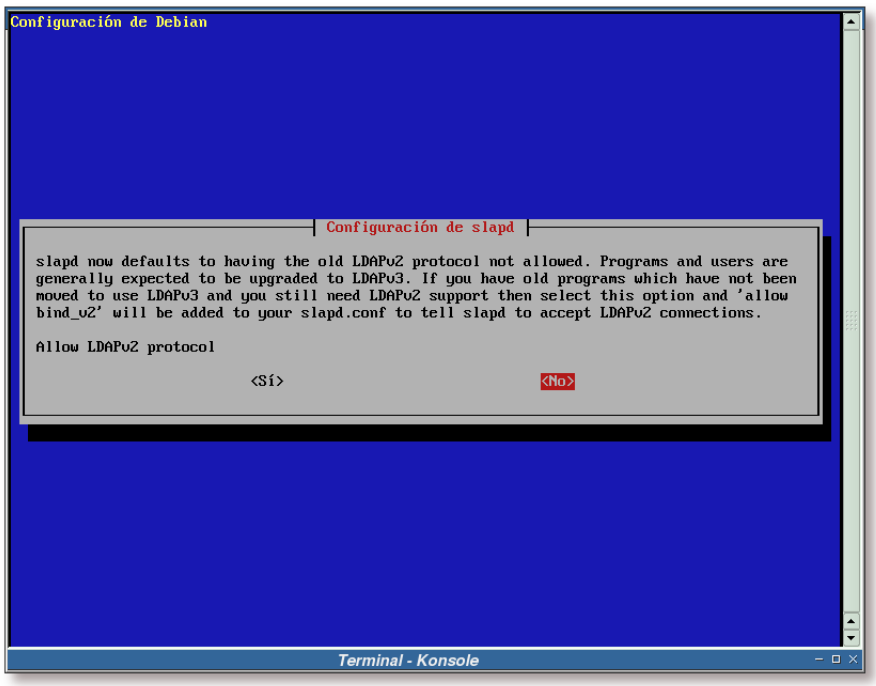
Figura 2-8. Configuración de slapd, ¿mover los datos antiguos?



Nota: Esta pantalla de configuración puede no aparecer cuando instale OpenLDAP en su sistema, no se preocupe por ello. El motivo para que no aparezca es que no existen datos en el directorio `/var/lib/ldap`, esto se puede deber a que esta sea su primera instalación de OpenLDAP o se hayan borrado los datos de dicho directorio, entre otros.

Dependiendo de sus necesidades debería contestar o *Sí* o *No* en esta pantalla. En este ejemplo se contestará que *Sí*, de esta forma los datos existentes en `/var/lib/ldap` se empaquetarán y se moverán moverán a un directorio similar a `/var/backups/var_lib_ldap-*FECHA*/` donde *FECHA* se sustituirá por la fecha que posea el ordenador en ese momento.

Figura 2-9. Configuración de slapd, protocolo LDAPv2



Al igual que la pantalla anterior, la respuesta a esta pregunta dependerá de sus necesidades. En este ejemplo se optará por no mantener la compatibilidad con la versión 2 del protocolo LDAP, opción que se recomienda encarecidamente seleccionar.

Ejemplo 2-2. Instalación de los paquetes *slapd ldap-utils (segunda parte)*

```
find: /var/lib/ldap: No existe el fichero o el directorio

Seleccionando el paquete ldap-utils previamente no seleccionado.
(Leyendo la base de datos ...
252690 ficheros y directorios instalados actualmente.)
Desempaquetando ldap-utils (de .../ldap-utils_2.1.30-3_i386.deb) ...
Seleccionando el paquete slapd previamente no seleccionado.
Desempaquetando slapd (de .../slapd_2.1.30-3_i386.deb) ...
Configurando ldap-utils (2.1.30-3) ...
Configurando slapd (2.1.30-3) ...
Creating initial slapd configuration... done
Creating initial LDAP directory... done
Starting OpenLDAP: slapd.

localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

Observaciones a la instalación

Una vez más, dependiendo de como se encuentre su sistema y los paquetes que tenga instalados en el mismo, se instalarán y sugerirán más o menos dependencias a la hora de instalar OpenLDAP.

La siguiente captura muestra la información relativa a los paquetes que se acaban de instalar (dependencias, sugerencias de instalación, etc).

```
$ /usr/bin/apt-cache show slapd ldap-utils
Package: slapd
Priority: optional
Section: net
Installed-Size: 2392
Maintainer: Torsten Landschoff <torsten@debian.org>
Architecture: i386
Source: openldap2
Version: 2.1.30-3
Provides: ldap-server
Depends: libc6 (>= 2.3.2.ds1-4), libdb4.2, libgcrypt11,
libgnutls11 (>= 1.0.16), libgpg-error0 (>= 0.7),
libiodbc2 (>= 3.51.2-2), libldap2 (>= 2.1.17-1),
libltdl3 (>= 1.5.2-2), libsasl2 (>= 2.1.18), libslp1,
libwrap0, zlib1g (>= 1:1.2.1), debconf (>= 0.5),
coreutils (>= 4.5.1-1) | fileutils (>= 4.0i-1), psmisc,
libldap2 (= 2.1.30-3), perl (>> 5.8.0) | libmime-base64-perl
Recommends: db4.2-util, libsasl2-modules
Suggests: ldap-utils
Conflicts: umich-ldapd, ldap-server, libbind-dev, bind-dev,
libltdl3 (= 1.5.4-1)
Filename: pool/main/o/openldap2/slapd_2.1.30-3_i386.deb
Size: 941934
MD5sum: 497cbd88576c42e89457fa8c1594067f
Description: OpenLDAP server (slapd)
 This is the OpenLDAP (Lightweight Directory Access Protocol) standalone
 server (slapd). The server can be used to provide a standalone directory
 service and also includes the slurpd replication server.

Package: ldap-utils
Priority: optional
Section: net
Installed-Size: 292
Maintainer: Torsten Landschoff <torsten@debian.org>
Architecture: i386
Source: openldap2
Version: 2.1.30-3
Replaces: openldap-utils, slapd (<< 2.1.25), openldapd
Provides: ldap-client, openldap-utils
Depends: libc6 (>= 2.3.2.ds1-4), libdb4.2, libgcrypt11,
libgnutls11 (>= 1.0.16), libgpg-error0 (>= 0.7),
libiodbc2 (>= 3.51.2-2), libldap2 (>= 2.1.17-1),
libltdl3 (>= 1.5.2-2), libsasl2 (>= 2.1.18), libslp1,
zlib1g (>= 1:1.2.1), libldap2 (= 2.1.30-3)
Recommends: libsasl2-modules
Conflicts: umich-ldap-utils, openldap-utils, ldap-client
```

```
Filename: pool/main/o/openldap2/ldap-utils_2.1.30-3_i386.deb
Size: 114684
MD5sum: 01c409b7e225facf2056310fd70afdad
Description: OpenLDAP utilities
 Utilities from the OpenLDAP (Lightweight Directory Access Protocol)
 package. These utilities can access a local or remote LDAP server
 and contain all the client programs required to access LDAP servers.
```

Comprobaciones iniciales de la instalación

Ejecución del demonio

En este punto, ya se debería tener un servidor OpenLDAP instalado y ejecutándose, aunque no esté ajustado todavía a los objetivos que persigue este apartado. Para comprobar que efectivamente el demonio **slapd** se está ejecutando, realizaremos un par de consultas al sistema. La primera consiste en ver si el demonio **slapd** se encuentra en la lista de procesos que actualmente se estén ejecutando en el sistema:

Ejemplo 2-3. Comprobación de que slapd está en la lista de procesos actuales

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

> **Nota:** En la captura de pantalla anterior se ha eliminado la línea que hacía referencia la instrucción tecleada (/bin/ps auxf | /bin/grep slapd) y se ha añadido la línea de información sobre cada parte de la captura, para mejorar la legibilidad.

La segunda comprobación ha realizar, para ver si el demonio se está realmente ejecutando, es verificar que está escuchando en la red[1]:

Ejemplo 2-4. Comprobación de que slapd escucha en la red

```
# /bin/netstat -puta
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:ldap                  *:*                     LISTEN     4453/slapd
```

Conectando con el servidor

Una vez comprobado que el demonio **slapd** se está ejecutando en el sistema, se verificará que la conexión con el mismo está permitida. Para ello, se realizará una búsqueda sencilla en el directorio. Si todo va bien, se debería mostrar algo similar a:

Ejemplo 2-5. Realización de una búsqueda simple con ldapsearch

```
$ /usr/bin/ldapsearch -x -b ” -s base ’(objectclass=*)’ namingContexts
# extended LDIF
#
# LDAPv3
# base <> with scope base
# filter: (objectclass=*)
# requesting: namingContexts
#

#
dn:
namingContexts: dc=gsr,dc=pt

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Posibles problemas de conexión

TCP Wrappers

Se han de tener en cuenta las opciones de configuración pasadas, antes de la compilación de OpenLDAP, para generar los paquetes que se están utilizando. Si nos fijamos en las opciones de configuración que posee OpenLDAP por defecto en Debian GNU/Linux (consulte el Apéndice P) veremos que utiliza la opción --*enable-wrappers*, lo que habilita el soporte de los TCP Wrappers en OpenLDAP.

Si se posee una configuración restrictiva de los TCP Wrappers, puede que sea esta la causa de los problemas de conexión. A continuación se simulará un fallo de conexión debido a un bloqueo de los TCP Wrappers, mostrándola manera de detectarlo y corregirlo.

Se supone la siguiente configuración de los TCP Wrappers (en los Apéndice AO y Apéndice AP se encuentran los archivos finales para los TCP Wrappers):

Ejemplo 2-6. Archivo `/etc/hosts.allow`

```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5), hosts_options(5)
#                   and /usr/doc/netbase/portmapper.txt.gz
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
```

```
#
# If you’re going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper. See portmap(8)
# and /usr/doc/portmap/portmapper.txt.gz for further information.
#
```

Ejemplo 2-7. Archivo `/etc/hosts.deny`

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5), hosts_options(5)
#                  and /usr/doc/netbase/portmapper.txt.gz
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you’re going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper. See portmap(8)
# and /usr/doc/portmap/portmapper.txt.gz for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address. You may wish to enable this to ensure any programs that don’t
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

# Desautorizar a todos los hosts con nombre sospechoso
ALL: PARANOID

# Desautorizar a todos los hosts
ALL:ALL
```

Ahora se realizará la misma búsqueda que en Ejemplo 2-5:

Ejemplo 2-8. Realización de una búsqueda simple con ldapsearch (conexión fallida)

```
$ ldapsearch -x -b ” -s base ’(objectclass=*)’ namingContexts
ldap_bind: Can’t contact LDAP server (81)
```

Como se puede apreciar, no se ha podido conectar con el servidor LDAP. El siguiente ejemplo realizará la misma búsqueda, sólo que en este caso se activará el modo de depuración de la orden **ldapsearch** “-d -1” (se hará uso del nivel de depurado *-1*, que es el mayor nivel existente).

Ejemplo 2-9. Realización de una búsqueda simple con ldapsearch (modo depuración)

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

```
ldap_send_initial_request
ldap_new_connection
ldap_int_open_connection
ldap_connect_to_host: TCP gsr.pt:389 ❶
ldap_new_socket: 3
ldap_prepare_socket: 3
ldap_connect_to_host: Trying 192.168.2.1:389 ❷
ldap_connect_timeout: fd: 3 tm: -1 async: 0
ldap_ndelay_on: 3
ldap_is_sock_ready: 3
ldap_ndelay_off: 3
ldap_int_sasl_open: host=gsr.pt
ldap_open_defconn: successful ❸
ldap_send_server_request
ber_flush: 14 bytes to sd 3
  0000:  30 0c 02 01 01 60 07 02  01 03 04 00 80 00         0....‘........
ldap_write: want=14, written=14
  0000:  30 0c 02 01 01 60 07 02  01 03 04 00 80 00         0....‘........
ldap_result msgid 1
ldap_chkResponseList for msgid=1, all=1
ldap_chkResponseList returns NULL
wait4msg (infinite timeout), msgid 1
wait4msg continue, msgid 1, all 1
** Connections:
* host: gsr.pt  port: 389  (default)
  refcnt: 2  status: Connected
  last used: Tue Mar  9 16:18:26 2004

** Outstanding Requests:
 * msgid 1,  origid 1, status InProgress
   outstanding referrals 0, parent count 0
** Response Queue:
   Empty
ldap_chkResponseList for msgid=1, all=1
ldap_chkResponseList returns NULL
ldap_int_select
read1msg: msgid 1, all 1
ber_get_next
ldap_read: want=8, got=0

ber_get_next failed. ❹
ldap_perror ❺
ldap_bind: Can’t contact LDAP server (81) ❻
```

❶❷ Aquí se puede ver que el host con el que establece la conexión es el correcto.

❸ Una vez encontrado el host, se conecta satisfactoriamente al mismo.

❹❺❻En este momento comienzan los errores de conexión.

Como se puede observar en el Ejemplo 2-9, que no se obtiene la información suficiente para deducir cual ha sido el problema que ocasiona el error en la conexión. Por este motivo se ejecutará el demonio **slapd** en modo depuración y, aunque no sea necesario, se ejecutará con el nivel de depurado “-1”.

Antes proceder con este ejemplo, se mostrarán los posibles valores que puede tomar el modo de depuración de **slapd** y su significado[2]:

Tabla 2-1. Niveles de depurado de slapd

Nivel	Descripción
-1	Habilita todo el depurado
0	Sin depurado
1	Rastrea las llamadas a funciones
2	Depura el manejo de paquetes
4	Rastreo de depuración intensivo
8	Administración de la conexión
16	Muestra los paquetes enviados y recibidos
32	Procesado de búsqueda por filtro
64	Procesado del archivo de configuración
128	Procesado de la lista de control de acceso
256	stats log connections/operations/results
512	stats log entries sent
1024	Muestra las comunicaciones con los backends de la shell
2048	Muestra las entradas analizadas (parsing)

Ejemplo 2-10. Ejecución del servidor slapd en modo de depuración

```
    # /usr/sbin/slapd -d -1 -h ldap://gsr.pt:389/
    @(#) $OpenLDAP: slapd 2.1.30 (Jul 27 2004 08:02:08) $
        @euklid:/home/roland/debian/openldap/build/2.1.30/openldap2-2.1.30/debian/build/servers/sla
daemon_init: ldap://gsr.pt:389/
daemon_init: listen on ldap://gsr.pt:389/
daemon_init: 1 listeners to open...
ldap_url_parse_ext(ldap://gsr.pt:389/)
daemon: initialized ldap://gsr.pt:389/
daemon_init: 1 listeners opened
slapd init: initiated server.
slap_sasl_init: initialized!
reading config file /etc/ldap/slapd.conf
line 11 (include         /etc/ldap/schema/core.schema)
reading config file /etc/ldap/schema/core.schema/

(...)

slapd startup: initiated.
slapd starting
daemon: added 6r
daemon: select: listen=6 active_threads=0 tvp=NULL
```

En este momento ya tenemos el demonio **slapd** en modo depuración, por lo que si realizamos de nuevo la búsqueda del Ejemplo 2-8, se verá la información que muestra el servidor cuando esta se realiza:

Ejemplo 2-11. Ejecución del servidor slapd en modo de depuración (mensaje de rechazo de una conexión)

```
    daemon: activity on 1 descriptors
daemon: new connection on 9
fd=9 DENIED from unknown (192.168.2.1) ❶
daemon: closing 9
daemon: activity on:
daemon: select: listen=6 active_threads=0 tvp=NULL
```

❶ Esta línea muestra el motivo del rechazo de la conexión, no se permite la conexión desde la IP 192.168.2.1, que es desde la que se está tratando de realizar la consulta precisamente.

Si se añade la siguiente línea al archivo `/etc/hosts.allow` "slapd: 192.168.2.1" y se ejecuta de nuevo la búsqueda del Ejemplo 2-8, sucede lo siguiente:

- El servidor muestra la siguiente información:

  Ejemplo 2-12. Ejecución del servidor slapd en modo de depuración (mensaje de aceptación de una conexión)

```
    daemon: activity on 1 descriptors
daemon: new connection on 9
conn=2 fd=9 ACCEPT from IP=192.168.2.1:32852 (IP=192.168.2.1:389) ❶
daemon: added 9r
daemon: activity on:
daemon: select: listen=6 active_threads=0 tvp=NULL
daemon: activity on 1 descriptors
daemon: activity on: 9r
daemon: read activity on 9
connection_get(9)
connection_get(9): got connid=2
connection_read(9): checking for input on id=2
ber_get_next

(...)

conn=2 op=1 SRCH base="" scope=0 filter="(objectClass=*)"
conn=2 op=1 SRCH attr=namingContexts
=> test_filter
    PRESENT
=> access_allowed: search access to "" "objectClass" requested
=> acl_get: [1] check attr objectClass
=> dn: [2]
=> acl_get: [2] matched
=> acl_get: [2] check attr objectClass
<= acl_get: [2] acl  attr: objectClass
=> acl_mask: access to entry "", attr "objectClass" requested
=> acl_mask: to all values by "", (=n)
```

```
<= check a_dn_pat: *
<= acl_mask: [1] applying read(=rscx) (stop)
<= acl_mask: [1] mask: read(=rscx)
=> access_allowed: search access granted by read(=rscx)
<= test_filter 6
=> send_search_entry: dn=""
=> access_allowed: read access to "" "entry" requested
=> acl_get: [1] check attr entry
=> dn: [2]
=> acl_get: [2] matched
=> acl_get: [2] check attr entry
<= acl_get: [2] acl  attr: entry
=> acl_mask: access to entry "", attr "entry" requested
=> acl_mask: to all values by "", (=n)
<= check a_dn_pat: *
<= acl_mask: [1] applying read(=rscx) (stop)
<= acl_mask: [1] mask: read(=rscx)
=> access_allowed: read access granted by read(=rscx)
=> access_allowed: read access to "" "namingContexts" requested
=> acl_get: [1] check attr namingContexts
=> dn: [2]
=> acl_get: [2] matched
=> acl_get: [2] check attr namingContexts
<= acl_get: [2] acl  attr: namingContexts
access_allowed: no res from state (namingContexts)
=> acl_mask: access to entry "", attr "namingContexts" requested
=> acl_mask: to all values by "", (=n)
<= check a_dn_pat: *
<= acl_mask: [1] applying read(=rscx) (stop)
<= acl_mask: [1] mask: read(=rscx)
=> access_allowed: read access granted by read(=rscx)

(...)

ber_get_next on fd 9 failed errno=0 (Success)
connection_read(9): input error=-2 id=2, closing.
connection_closing: readying conn=2 sd=9 for close
connection_close: deferring conn=2 sd=9
do_unbind
conn=2 op=2 UNBIND
connection_resched: attempting closing conn=2 sd=9
connection_close: conn=2 sd=9
daemon: removing 9
conn=2 fd=9 closed
daemon: select: listen=6 active_threads=0 tvp=NULL
daemon: activity on 1 descriptors
daemon: select: listen=6 active_threads=0 tvp=NULL
```

❶ Finalmente se ha aceptado la conexión.

- Del lado del cliente se obtiene la misma información que en el Ejemplo 2-5.

Address family not supported by protocol

Un error derivado de la instalación por defecto, es el que se muestra en título de esta sección. Si no se especifica en que interfaces ha de escuchar el demonio **slapd**, dará el mentado error.

A continuación se verá la diferencia de ejecutar el servidor especificando o no la interfaz sobre la que tiene que escuchar. Para ello, una vez más se ejecutará en modo depuración.

Ejemplo 2-13. Ejecución del demonio slapd sin especificar la interfaz donde escuchar

```
    # /usr/sbin/slapd -d -1
    @(#) $OpenLDAP: slapd 2.1.30 (Jul 27 2004 08:02:08) $
        @euklid:/home/roland/debian/openldap/build/2.1.30/openldap2-2.1.30/\
                            debian/build/servers/slapd
                            openldap2-2.1.30/debian/build/servers/slapd
daemon_init: <null>
daemon_init: listen on ldap:///
daemon_init: 1 listeners to open...
ldap_url_parse_ext(ldap:///)
slap_open_listener: socket() failed for AF_INET6 errno=97 (Address family not supported by protoco
daemon: initialized ldap:///
daemon_init: 2 listeners opened
ldap_pvt_gethostbyname_a: host=todoscsi, r=0
slapd init: initiated server.
slap_sasl_init: initialized!
reading config file /etc/ldap/slapd.conf
line 11 (include         /etc/ldap/schema/core.schema)
reading config file /etc/ldap/schema/core.schema

(...)

slapd startup: initiated.
slapd starting
daemon: added 6r
daemon: select: listen=6 active_threads=0 tvp=NULL
```

❶ Aquí se muestra el error.

Ejemplo 2-14. Ejecución del demonio slapd especificando la interfaz donde escuchar

```
    # /usr/sbin/slapd -d -1 -h ldap://gsr.pt:389/
    @(#) $OpenLDAP: slapd 2.1.30 (Jul 27 2004 08:02:08) $
        @euklid:/home/roland/debian/openldap/build/2.1.30/openldap2-2.1.30/\
                            debian/build/servers/slapd
daemon_init: ldap://gsr.pt:389/
daemon_init: listen on ldap://gsr.pt:389/
daemon_init: 1 listeners to open...
ldap_url_parse_ext(ldap://gsr.pt:389/)
daemon: initialized ldap://gsr.pt:389/
daemon_init: 1 listeners opened
slapd init: initiated server.
slap_sasl_init: initialized!
```

```
reading config file /etc/ldap/slapd.conf
line 11 (include         /etc/ldap/schema/core.schema)
reading config file /etc/ldap/schema/core.schema

(...)

slapd startup: initiated.
slapd starting
daemon: added 6r
daemon: select: listen=6 active_threads=0 tvp=NULL
```

En el Ejemplo 2-14 se puede ver que ya no muestra ningún tipo de error al inicializar el servidor.

> **Nota:** En el Capítulo 3 se verá como configurar **slapd** para que arranque automáticamente con la especificación de la interfaces.

Notas

1. Puede ajustar más la búsqueda seleccionando sólo aquellas conexiones que quiera ver. Para ello puede hacer uso de **grep** y las cadenas “LISTEN” y “slapd”.
2. Si quiere obtener más información sobre los niveles de depurado, vea el archivo `ldap_log.h` que viene con el código fuente de OpenLDAP.

Capítulo 3. Retoques iniciales a la configuración por defecto de OpenLDAP

`/etc/default/slapd`

En este archivo se configuran los aspectos relativos a la ejecución del demonio **slapd**: parámetros pasados en el arranque, usuario y grupo de ejecución del demonio, etc. En las siguientes secciones se verán los cambios realizados.

> **Nota:** Un ejemplo completo de este archivo de configuración se encuentra en el Apéndice S

Cambio del usuario y grupo de ejecución de slapd

Por defecto, el demonio **slapd** se ejecuta como usuario *root* (vea el Ejemplo 2-3 para más detalles), comportamiento que no es recomendable por las implicaciones de seguridad que acarrea. En esta sección se describirán los pasos necesarios para ejecutar el demonio **slapd** con un usuario y un grupo específicos.

Creación del usuario y grupo para slapd

Antes de poder ejecutar el demonio **slapd** con un usuario y grupo específico, se ha de crear el usuario y grupo en el sistema, en caso de no existir.

El tipo de usuario y grupo que se crearán son los llamados “de sistema”, y se denominarán “slapd”. Para crearlos ejecute:

Ejemplo 3-1. Creación de un grupo y usuario de sistema para slapd

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

Como se puede apreciar en el Ejemplo 3-1, el home del usuario *slapd* es el directorio `/var/lib/ldap` (donde se almacena la base de datos de OpenLDAP, entre otras cosas), no posee shell asociada y está dentro del grupo *slapd* que se acaba de crear.

Cambio de propietario/grupo en los archivos de slapd

> **Aviso**
>
> Antes de continuar con este paso, ha de parar el demonio **slapd** para evitar comportamientos no esperados:
>
> **Ejemplo 3-2. Modo de parar el demonio slapd**
>
> ```
> # /etc/init.d/slapd stop
> Stopping OpenLDAP: slapd.
> ```

Antes de ejecutar el demonio **slapd** con el nuevo usuario y grupo creados, es necesario cambiar el propietario y el grupo de algunos archivos y directorios relacionados con **slapd**, para que este funcione con normalidad. Los cambios han de realizarse en los siguientes directorios, así como en los archivos que albergan:

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

Para ello se ha de ejecutar:

Ejemplo 3-3. Cambio del propietario/grupo en archivos relacionados con slapd

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

En estos momentos **slapd** ya casi está preparado para ejecutarse con el nuevo usuario.

Especificar el usuario/grupo con el que ejecutar slapd

El último paso consiste en indicar al demonio **slapd** con qué usuario y grupo se ha de ejecutar a partir de ahora. Esta característica se configura asignando los valores correspondientes a las variables *SLAPD_USER* y *SLAPD_GROUP* del archivo `/etc/default/slapd`.

Continuando con la configuración de ejemplo seguida en las secciones anteriores los valores que han de tener estas variables son:

Ejemplo 3-4. Asignación del usuario y grupo con que se ejecutará slapd

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

Arrancando el demonio slapd

Ahora sólo queda arrancar de nuevo el demonio **slapd** para que se ejecute con el nuevo usuario:

Ejemplo 3-5. Arrancando el demonio slapd

```
# /etc/init.d/slapd start
Starting OpenLDAP: slapd.
# /bin/ps auxf
USER       PID %CPU %MEM    VSZ  RSS TTY   STAT START TIME COMMAND
slapd ❶   12728  0.0  0.6 12216 3556 ?     S    15:02 0:00 /usr/sbin/slapd -g slapd -u slapd ❷
slapd ❸   12729  0.0  0.6 12216 3556 ?     S    15:02 0:00  \_ /usr/sbin/slapd -g slapd -u slapd ❹
slapd ❺   12730  0.0  0.6 12216 3556 ?     S    15:02 0:00      \_ /usr/sbin/slapd -g slapd -u sla
```

❶❸❺Usuario con el que se está ejecutando **slapd**.

❷❹❻Parámetros de ejecución de **slapd**, se puede apreciar que se ha indicado el usuario (-u slapd) y grupo (-g slapd) de ejecución del demonio.

Especificación de las interfaces donde escuchar

La configuración por defecto del demonio **slapd** hace que escuche en todas las interfaces de red presentes en el sistema. Esta característica no es deseable, por este motivo se verá la forma de modificarla.

La especificación de las interfaces de red, así como el protocolo utilizado en cada una de ellas (ldap, ldaps, ldai), se realiza en el archivo `/etc/default/slapd`. Dentro de este, la variable *SLAPD_SERVICES* poseerá las interfaces donde se desea que escuche **slapd**. El Ejemplo 3-6 muestra como hacerlo.

Ejemplo 3-6. Estableciendo las interfaces donde ha de escuchar slapd

```
SLAPD_SERVICES="ldap://gsr.pt:389/ ldaps://gsr.pt:636/"
```

> **Nota:** El protocolo “ldap” especifica las interfaces y los puertos donde escuchará **slapd** con la característica de que las conexiones que se establezcan a la misma no harán uso de cifrado.
>
> El protocolo “ldaps” especifica las interfaces y los puertos donde escuchará **slapd** con la característica de que las conexiones que se establezcan a la misma harán uso de cifrado.
>
> Adicionalmente se puede establecer un nuevo protocolo de comunicaciones, “ldapi”, destinado a las peticiones realizadas desde sockets Unix.

Una vez se han asignado las interfaces necesarias, se ha de reiniciar el demonio **slapd**:

Ejemplo 3-7. Reinicio del demonio slapd

```
# /bin/netstat -puta
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address     Foreign Address    State   PID/Program name
tcp        0      0 *:ldap ❶           *:*                LISTEN 12728/slapd
# /etc/init.d/slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: slapd.
```

```
# /bin/netstat -puta
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address    Foreign Address   State   PID/Program name
tcp        0      0 gsr.pt:ldap ❶     *:*               LISTEN 12817/slapd
tcp        0      0 gsr.pt:ldaps ❷     *:*              LISTEN 12817/slapd
# /bin/ps auxfw

USER  PID   %CPU %MEM  VSZ  RSS TTY STAT START TIME COMMAND
slapd 12817 0.0  0.6 12216 3552 ? S  15:19 0:00 /usr/sbin/slapd -h ldap://gsr.pt:389/ ❶
                                                |                  ldaps://gsr.pt:636/
                                                |               -g slapd -u slapd
slapd 12818 0.0  0.6 12216 3552 ? S  15:19 0:00  \_ /usr/sbin/slapd -h ldap://gsr.pt:389/ ❷
                                                   |                  ldaps://gsr.pt:636/
                                                   |                -g slapd -u slapd
slapd 12819 0.0  0.6 12216 3552 ? S  15:19 0:00     \_ /usr/sbin/slapd -h ldap://gsr.pt:389/ ❸
                                                                          ldaps://gsr.pt:636/
                                                                       -g slapd -u slapd
```

❶ Inicialmente el demonio **slapd** escucha en el puerto 389 en todas la interfaces.

❶❷ Una vez reiniciado con la nueva configuración, el demonio **slapd** escucha en las interfaces requeridas.

❶❷❸La lista de parámetros pasados al demonio **slapd** ha aumentado, ahora se especifica el host donde ha de escuchar y con qué protocolo.

Nota: La salida de la orden **/bin/ps** se ha retocado para mejorar la legibilidad.

/etc/ldap/ldap.conf

Este es el archivo de configuración global empleado por los clientes LDAP. En este momento estableceremos unas opciones iniciales, que pueden cambiar y ampliarse a lo largo del documento.

Nota: En el Apéndice R posee un ejemplo completo de configuración.

Ejemplo 3-8. Configuración inicial del archivo `/etc/ldap/ldap.conf`

```
#
# Configuración por defecto de LDAP
#

# Vea ldap.conf(5) para más detalles
# Este archivo ha de poderse leer por todo el mundo,
# pero no escribirse por todos.
```

```
   # Su servidor LDAP. Ha de ser resoluble sin utilizar LDAP.
10 HOST gsr.pt

   # El nombre distinguido para la base de las búsquedas.
   BASE dc=gsr, dc=pt

15 # El puerto.
   # Opcional: por defecto es el 389. El 636 es para ldaps
   port 389
```

Ha de asegurarse que los permisos de este archivo estén bien asignados (se ha de leer por todo el mundo):

Ejemplo 3-9. Estableciendo los permisos para `/etc/ldap/ldap.conf`

```
# /bin/chmod -v 644 /etc/ldap/ldap.conf
el modo de ‘/etc/ldap/ldap.conf’ cambia a 0644 (rw-r--r--)
```

/etc/ldap/slapd.conf

La única modificación que se ha de realizar en este archivo, de momento, es un cambio de permisos, de forma que sólo el propietario tenga permisos de lectura y escritura:

```
# /bin/chmod -v 600 /etc/ldap/slapd.conf
el modo de ‘/etc/ldap/slapd.conf’ cambia a 0600 (rw-------)
```

Capítulo 4. Preparando la conexión segura

Creación de certificados

Introducción

Este capítulo está dedicado a la creación de la entidad certificadora y los certificados necesarios para hacer uso de una conexión segura, característica que provee la versión 3 del protocolo LDAP por defecto, y por tanto, la versión de OpenLDAP que se está utilizando en este documento.

> **Aviso**
>
> Tal y como se distribuye el paquete de OpenLDAP en Debian GNU/Linux, no es posible, al menos a la hora de generar esta documentación, hacer uso de cifrado en las comunicaciones relacionadas con LDAP. En la la sección de nombre *Solución temporal a los problemas de OpenLDAP en Debian GNU/Linux* se detallará el problema y se dará una solución temporal, a la espera de que se solucionen los problemas con este paquete en Debian[1].

> **Atención**
>
> Se asume que ya posee una instalación de OpenSSL en su sistema, de no ser así, será necesario instalarla:
>
> ```
> # apt-get install openssl
> ```

Nota: La versión de OpenSSL empleada para generar esta documentación ha sido la *0.9.7d*.

Nota: Para la elaboración de este capítulo, se ha empleado, principalmente, la entrada bibliográfica Soper01 y el capítulo 6 de la entraba bibliográfica Tournier01.

Creación de un certificado

Para habilitar las conexiones SSL/TLS hacia el servidor LDAP, se necesita la presencia de un certificado en el servidor. Además, en el establecimiento de una conexión SSL/TLS, el certificado del servidor sólo proporciona una conexión segura y cifrada al servidor. Si se desea autentificar al cliente, se ha de presentar al servidor LDAP el certificado y el par de llaves del cliente.

Existen dos formas de crear e instalar un certificado en el servidor: la creación de un “certificado autofirmado” y la creación de un “certificado emitido por una CA”. Ambos métodos requieren la creación de un certificado para el servidor, enviárselo a los clientes OpenLDAP y realizar los cambios

apropiados en los archivos de configuración de OpenLDAP. Ambos métodos necesitan el uso de órdenes OpenSSL que solicitarán información para la creación del certificado.

> **Nota:** Para la elaboración de esta documentación se ha elegido la creación de un certificado a partir de una CA (la sección de nombre *Certificado emitido por una CA*) y sobre este método se basará el resto de la documentación. De todas formas, se ha incluido en la
> la sección de nombre *Certificado autofirmado* el otro método existente, a título informativo.

> **Aviso**
>
> Cuando se pregunte por el “Common Name”, ha de teclear el nombre del dominio de su servidor (FQDN), como por ejemplo: *miservidor.pt*, y no “su nombre” como sugiere OpenSSL. ¡Esta equivocación es la causa del 90% de los errores en el el certificado del servidor!

Certificado autofirmado

La primera forma para la creación del certificado del servidor emplea OpenSSL y genera un certificado autofirmado para el servidor. Para ello, desde la línea de comandos se ha de teclear (la letra en negrita son las opciones que ha de introducir el usuario):

> **Nota:** OpenLDAP sólo trabaja con llaves no cifradas, por lo que se ha de emplear el parámetro “-nodes” de OpenSSL para evitar el cifrado de la llave privada.

Ejemplo 4-1. Creación de un certificado autofirmado para el servidor

```
$ openssl req -newkey rsa:1024 -x509 -nodes -out server.pem -keyout server.pem -days 365
Generating a 1024 bit RSA private key
.........................++++++
.............................++++++
writing new private key to 'server.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PT
State or Province Name (full name) [Some-State]:Braganca
Locality Name (eg, city) []:Braganca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:gsr.pt
Organizational Unit Name (eg, section) []:gsr.pt
Common Name (eg, YOUR name) []:gsr.pt
Email Address []:sergio@gsr.pt
```

Esto creará un archivo `server.pem` en el directorio donde haya ejecutado la orden del Ejemplo 4-1. Puede ver una muestra de su resultado en el Apéndice O.

Ahora sólo falta indicar a OpenLDAP que utilice el certificado anteriormente creado. El siguiente ejemplo muestra las opciones de configuración que han de añadirse al archivo `/etc/ldap/slapd.conf` si se ha seguido el método de creación del certificado autofirmado.

Ejemplo 4-2. Opciones de configuración para `slapd.conf` que añaden un certificado autofirmado en el servidor.

```
TLSCACertificateFile server.pem
TLSCertificateFile server.pem
TLSCertificateKeyFile server.pem
```

> **Nota:** Puede observarse en el ejemplo anterior, que las tres opciones poseen el mismo valor: “server.pem”. Esto diferirá si se ha obtenido el certificado a partir de una CA, como puede verse en el Ejemplo 4-9.

Certificado emitido por una CA

Si ya posee una entidad certificadora (CA) de confianza, sáltese esta sección dedicada al proceso de obtención de un certificado firmado por una entidad certificadora y una llave privada para el servidor.

Sin embargo, si no posee de una entidad certificadora de confianza, OpenSSL realiza el proceso rápida y fácilmente. Para ello siga los siguientes pasos:

1. Creación de un directorio para crear y firmar los certificados, por ejemplo: `/var/tmp/mica`

   Ejemplo 4-3. Creación de un directorio para crear y firmar los certificados

   ```
   $ /bin/mkdir -v /var/tmp/mica
   /bin/mkdir: se ha creado el directorio ‘/var/tmp/mica’
   ```

2. Sitúese en el directorio `/var/tmp/mica` y ejecute el script `CA.sh` de OpenSSL.

   Ejemplo 4-4. Creación de una entidad certificadora

   ```
   $ cd /var/tmp/mica
   $ /usr/lib/ssl/misc/CA.sh -newca
   CA certificate filename (or enter to create)
   [Enter]
   Making CA certificate ...
   Generating a 1024 bit RSA private key
   ..................+++
   ................................+++
   writing new private key to ’./demoCA/private/./cakey.pem’
   Enter PEM pass phrase: [Clave ca] ❶
   ```

```
Verifying - Enter PEM pass phrase: [Clave ca]
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PT
State or Province Name (full name) [Some-State]:Braganca
Locality Name (eg, city) []:Braganca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Companhia GSR
Organizational Unit Name (eg, section) []:Unidade de certificados
Common Name (eg, YOUR name) []:gsr.pt
Email Address []:[Enter]
```

❶ La clave utilizada ha de tener un mínimo de 4 caracteres.

Esto creará la siguiente estructura de directorios bajo `/var/tmp/mica`:

```
$ /usr/bin/tree
.
'-- demoCA
    |-- cacert.pem
    |-- certs
    |-- crl
    |-- index.txt
    |-- newcerts
    |-- private
    |   '-- cakey.pem
    '-- serial

5 directories, 4 files
```

Pero los archivos realmente interesantes son `demoCA/cacert.pem` y `demoCA/private/cakey.pem` (El certificado de la entidad certificadora y la llave privada, respectivamente).

3. Creamos la petición para la firma del certificado perteneciente al servidor (CSR):

Ejemplo 4-5. Creación de la petición para la firma del certificado del servidor

```
$ /usr/bin/openssl req -newkey rsa:1024 -nodes -keyout newreq.pem -out newreq.pem
Generating a 1024 bit RSA private key
...++++++
...........++++++
writing new private key to 'newreq.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PT
State or Province Name (full name) [Some-State]:Braganca
Locality Name (eg, city) []:Braganca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SubGSR
Organizational Unit Name (eg, section) []:Controle de acesso
Common Name (eg, YOUR name) []:gsr.pt
Email Address []:sergio@gsr.pt


Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:[Clave] ❶
An optional company name []:.[Enter]
```

❶ La clave utilizada ha de tener un mínimo de 4 caracteres.

El resultado es el archivo `newreq.pem`.

4. Firma del CSR:

Ejemplo 4-6. Firma del CSR

```
$ /usr/lib/ssl/misc/CA.sh -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:[Clave ca]
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Sep 23 16:16:11 2004 GMT
            Not After : Sep 23 16:16:11 2005 GMT
        Subject:
            countryName               = PT
            stateOrProvinceName       = Braganca
            localityName              = Braganca
            organizationName          = SubGSR
            organizationalUnitName    = Controle de acesso
            commonName                = gsr.pt
            emailAddress              = sergio@gsr.pt
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                8C:66:2C:3E:0F:63:2F:53:29:FA:28:EA:7F:59:A4:16:4C:DF:7C:6C
            X509v3 Authority Key Identifier:
                keyid:F1:34:77:80:A4:34:4B:71:C8:BF:81:6C:DF:0C:98:D3:62:B7:10:BE
                DirName:/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de\
```

```
                                                        certificados/CN=gsr.pt
                serial:00

Certificate is to be certified until Sep 23 16:16:11 2005 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=PT, ST=Braganca, L=Braganca, O=Companhia GSR, OU=Unidade de certificados,\
                                                                                CN=gsr.pt
        Validity
            Not Before: Sep 23 16:16:11 2004 GMT
            Not After : Sep 23 16:16:11 2005 GMT
        Subject: C=PT, ST=Braganca, L=Braganca, O=SubGSR, OU=Controle de acesso, \
                                                    CN=gsr.pt/emailAddress=sergio@gsr.pt
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ab:bc:62:aa:75:ad:76:6d:05:e6:be:c2:b7:b7:
                    1f:28:3a:b9:ed:0b:b2:11:6a:9d:27:7b:06:69:89:
                    3a:13:3d:29:85:0d:02:87:b7:ac:cf:46:b0:01:3a:
                    30:c6:2e:25:13:af:6f:35:b6:d0:2c:ae:fb:42:24:
                    77:f3:c7:e1:a6:cb:00:35:ca:03:be:b1:d8:dd:22:
                    de:d6:bc:e2:94:d4:1a:ae:47:83:95:0c:a2:ae:1f:
                    c3:d3:f4:1d:7e:cd:cc:9c:48:28:63:35:5c:af:7b:
                    c9:bf:f8:f7:de:2b:09:61:c6:40:30:76:e3:9f:51:
                    28:d0:61:b2:18:9a:d9:8a:53
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                8C:66:2C:3E:0F:63:2F:53:29:FA:28:EA:7F:59:A4:16:4C:DF:7C:6C
            X509v3 Authority Key Identifier:
                keyid:F1:34:77:80:A4:34:4B:71:C8:BF:81:6C:DF:0C:98:D3:62:B7:10:BE
                DirName:/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de \
                                                                    certificados/CN=gsr.pt
                serial:00

    Signature Algorithm: md5WithRSAEncryption
        27:43:54:46:14:dd:f5:2d:64:40:b4:dd:62:b4:79:d6:93:32:
        d4:56:0d:a7:80:60:6a:93:1a:c2:02:e3:f8:33:d9:4d:32:c7:
        0b:34:29:01:72:98:1a:aa:c6:34:78:50:11:0d:92:ab:31:ba:
```

```
        9b:3f:27:39:1a:19:8b:a0:2c:d7:ca:56:04:69:c4:ae:cc:e5:
        dc:fa:ce:da:11:a9:25:0c:db:d6:8c:60:b1:86:9a:02:06:c5:
        c4:da:8f:8e:a6:4d:84:06:3d:e1:ce:3e:d9:fa:d4:5b:d5:44:
        36:4f:48:88:d0:ab:ec:03:e5:a7:4f:92:e8:8e:db:aa:89:7e:
        02:e4
-----BEGIN CERTIFICATE-----
MIIDkDCCAvmgAwIBAgIBATANBgkqhkiG9w0BAQQFADB+MQswCQYDVQQGEwJQVDER
MA8GA1UECBMIQnJhZ2FuY2ExETAPBgNVBAcTCEJyYWdhbmNhMRYwFAYDVQQKEw1D
b21wYW5oaWEgR1NSMSAwHgYDVQQLExdVbmlkYWRlIGRlIGNlcnRpZmljYWRvczEP
MA0GA1UEAxMGZ3NyLnB0MB4XDTA0MDkyMzE2MTYxMVoXDTA1MDkyMzE2MTYxMVow
gZAxCzAJBgNVBAYTAlBUMREwDwYDVQQIEwhCcmFnYW5jYTERMA8GA1UEBxMIQnJh
Z2FuY2ExDzANBgNVBAoTBlN1YkdTUjEbMBkGA1UECxMSQ29udHJvbGUgZGUgYWNl
c3NvMQ8wDQYDVQQDEwZnc3IucHQxHDAaBgkqhkiG9w0BCQEWDXNlcmdpb0Bnc3Iu
cHQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKu8Yqp1rXZtBea+wre3Hyg6
ue0LshFqnSd7BmmJOhM9KYUNAoe3rM9GsAE6MMYuJROvbzW20Cyu+0Ikd/PH4abL
ADXKA76x2N0i3ta84pTUGq5Hg5UMoq4fw9P0HX7NzJxIKGM1XK97yb/4994rCWHG
QDB2459RKNBhshia2YpTAgMBAAGjggEJMIIBBTAJBgNVHRMEAjAAMCwGCWCGSAGG
+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU
jGYsPg9jL1Mp+ijqf1mkFkzffGwwgaoGA1UdIwSBojCBn4AU8TR3gKQ0S3HIv4Fs
3wyY02K3EL6hgYOkgYAwfjELMAkGA1UEBhMCUFQxETAPBgNVBAgTCEJyYWdhbmNh
MREwDwYDVQQHEwhCcmFnYW5jYTEWMBQGA1UEChMNQ29tcGFuaGlhIEdTUjEgMB4G
A1UECxMXVW5pZGFkZSBkZSBjZXJ0aWZpY2Fkb3MxDzANBgNVBAMTBmdzci5wdIIB
ADANBgkqhkiG9w0BAQQFAAOBgQAnQ1RGFN31LWRAtN1itHnWkzLUVg2ngGBqkxrC
AuP4M9lNMscLNCkBcpgaqsY0eFARDZKrMbqbPyc5GhmLoCzXylYEacSuzOXc+s7a
EaklDNvWjGCxhpoCBsXE2o+Opk2EBj3hzj7Z+tRb1UQ2T0iI0KvsA+WnT5Lojtuq
iX4C5A==
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
```

Esto crea el archivo `newcert.pem` (el certificado del servidor firmado por la entidad certificadora) con la clave privada, `newreq.pem`.

> **Nota:** Para verificar que el certificado está correctamente firmado se puede utilizar la siguiente orden:
>
> **Ejemplo 4-7. Verificación de la firma creada en un certificado por una CA**
>
> ```
> $ /usr/bin/openssl verify -CAfile demoCA/cacert.pem newcert.pem
> newcert.pem: OK
> ```

5. Ahora se puede renombrar y mover los certificados al sitio deseado. En este caso se moverá al directorio `/etc/ldap/ssl`, quedando la estructura final como sigue:

Ejemplo 4-8. Estructura de directorios final para los certificados

```
# /usr/bin/tree /etc/ldap/ssl
/etc/ldap/ssl
|-- cacert.pem
|-- certs
|   ‘-- servidorcert.pem ❶
|-- crl
|-- index.txt
|-- newcerts
|   ‘-- 01.pem
|-- private
|   |-- cakey.pem
|   ‘-- servidorkey.pem ❷
‘-- serial

4 directories, 7 files
```

❶ Este archivo se corresponde con el archivo `newcert.pem` generado tras el Ejemplo 4-6

❷ Este archivo se corresponde con el archivo `newreq.pem` generado tras el Ejemplo 4-6

> **Importante:** Sería recomendable hacer la llave privada del servidor sólo legible por el usuario con el que se ejecuta **slapd**, para ello teclee:
>
> ```
> # /bin/chmod -v 400 /etc/ldap/ssl/private/servidorkey.pem
> el modo de ‘/etc/ldap/ssl/private/servidorkey.pem’ cambia a 0400 (r--------)
> ```
>
> Los demás certificados tendría que poderse leer por todo el mundo.

6. Hacer que el certificado de la entidad certificadora esté disponible para los clientes de LDAP.

   Si los clientes están en la misma máquina, se ha de copiar el archivo `cacert.pem` a un lugar accesible por los clientes. Si los clientes están en otros equipos, se ha de copiar el archivo `cacert.pem` a esas máquinas y hacerlo accesible.

Como se ha podido apreciar, este proceso requieres algunos pasos más que la creación un certificado autofirmado, pero los beneficios obtenidos sobrepasan cualquier gasto de tiempo empleado en crear la entidad certificadora.

El certificado de los clientes

Los certificados para los clientes se crean de forma similar a los certificados para el servidor. Si se siguen los pasos detallados en la sección de nombre *Certificado emitido por una CA*, los únicos cambios son los siguientes:

1 y 2: No se hace nada... no se necesita crear de nuevo la entidad certificadora. El objetivo es utilizar la misma entidad certificadora para firmar el certificado del cliente.

3: Se ejecuta todo lo que allí se muestra, lo único que se ha de cambiar es el nombre del servidor por el del cliente cuando se pregunte el “Common Name”. Se da por supuesto que todas las demás respuestas se han de ajustar a los datos del cliente.

4: Las mismas órdenes, obteniéndose los mismos archivos para el certificado y la llave privada. ¡Gracias que se renombró el certificado en el 5!.

5: Ahora se puede renombrar y mover el certificado y la llave privada del cliente al lugar indicado (por ejemplo, `/home/usuario/ssl/`[2]). También sería recomendable que cambiase los permisos de la llave privada, para que sólo pueda ser leída por el usuario al que pertenece.

6: No se ha de hacer nada en este paso.

Ahora que ya están creados los certificados, sólo queda configurar OpenLDAP.

Configuración de OpenLDAP

Hay tres áreas a considerar para la configuración de OpenLDAP: el servidor (`slapd.conf`), el cliente (`ldap.conf`) y el directorio (*schema*). Esta sección configurará los requerimientos de un servidor SSL así como la autentificación de un cliente.

> **Nota:** Un ejemplo completo del archivo de configuración del demonio **slapd** se encuentra en el Apéndice Q

Servidor

Se ha de añadir las siguientes líneas al archivo de configuración de **slapd**, `slapd.conf`.

Ejemplo 4-9. Líneas de configuración para un servidor SSL/TLS

```
# Certificado firmado de una entidad certificadora y
# el certificado del servidor

TLSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCACertificateFile /etc/ldap/ssl/cacert.pem
TLSCertificateFile /etc/ldap/ssl/certs/servidorcert.pem
TLSCertificateKeyFile /etc/ldap/ssl/private/servidorkey.pem

# Si desea que el cliente necesite autentificación,
# descomente la siguiente línea
TLSVerifyClient demand
# ... si no, descomente esta otra
# TLSVerifyClient never
```

Cliente

El archivo de configuración `/etc/ldap/ldap.conf` configura las opciones por defecto para los clientes LDAP.

Si se necesitan valores específicos para los usuarios, se puede crear el archivo `ldaprc` o `.ldaprc` en el home del usuario o en el directorio actual, lo que sobreescribirá la configuración global de LDAP.

> **Atención**
>
> Si se requiere la autentificación de los clientes, se necesita añadir el certificado y la llave privada del cliente al archivo `ldaprc` o `.ldaprc`.

Directivas de configuración del cliente LDAP

La siguiente tabla refleja las directivas referentes a la parte de configuración del cliente LDAP. Las ocurrencias de las palabras **específicas para usuarios** quieren decir que las directivas a las que afectan sólo son aplicadas en la configuración del archivo `ldaprc` o `.ldaprc`, no son directivas globales de LDAP.

Tabla 4-1. Directivas de configuración de clientes LDAP

Directiva	Valor	Descripción
BASE	dn	Base por defecto (Default Base - DN) a utilizar cuando se realizan operaciones ldap
BINDDN	dn	Base por defecto a la que cambiar cuando se realizan operaciones ldap *específicas para usuarios*
HOST	nombre[:puerto]	Nombre de los servidores LDAP a los que conectarse (separados por espacios)
PORT	número	Puerto por defecto utilizado en las conexiones a un servidor LDAP. 636 = SSL
SIZELIMIT	número	Límite de resultados devueltos en una búsqueda (0 = sin límite)
TIMELIMIT	número	Límite en el tiempo de búsqueda (0 = sin límite)
TLS	nivel	Si el usuario ha de utilizar TLS por defecto (never | hard), el uso de esta directiva está desaconsejado; es incompatible con la petición StartTLS de LDAPv3

Directiva	Valor	Descripción
TLS_CACERT	nombre de un archivo	Especifica el archivo que contiene todos los certificados pertenecientes a entidades certificadoras que el cliente reconoce
TLS_CACERTDIR	directorio	Usado si falla TLS_CACERT
TLS_REQCERT	nivel	Especifica que tipo de comprobación se ha de realizar a un certificado de servidor (never | allow | try | demand,hard)
TLS_CERT	nombre de un archivo	**Autentificación de clientes**: especifica el certificado del cliente **específico del usuario**
TLS_KEY	nombre de un archivo	**Autentificación de clientes**: especifica la llave privada, para la entrada TLS_CERT, **específico del usuario**

Ejemplo de un archivo `ldap.conf`

A continuación se muestra un ejemplo de configuración de un archivo `ldap.conf`:

> **Nota:** En el Apéndice R se encuentra un ejemplo de configuración más extenso de este archivo.

Ejemplo 4-10. Ejemplo de configuración de un archivo `ldap.conf`

```
#
# Configuración global de LDAP
#

# Lea ldap.conf(5) para más detalles
# Este archivo se ha de poder leer por todo el mundo, pero no escribir.
HOST gsr.pt
BASE dc=gsr, dc=pt
PORT 636

TLS_CACERT /etc/ldap/ssl/certs/cacert.pem
TLS_REQCERT demand
```

Esta configuración hará que los clientes se conecten a ldaps://gsr.pt:636 sin necesidad de especificar el host ni el puerto en las órdenes del cliente.

Ejemplo de un archivo `.ldaprc`

El archivo `.ldaprc` se utiliza para sobreescribir las opciones globales de LDAP y para establecer el el certificado y la llave privada utilizados para la autentificación del cliente.

Ejemplo 4-11. Ejemplo de configuración de un archivo `.ldaprc` (en el home del usuario o en el directorio actual)

```
#
# Configuraciones de usuario específicas para LDAP
#

# Sobreescribe la directiva global (si se ha establecido)
TLS_REQCERT demand

# Autentificación del cliente
TLS_CERT /home/ldap-user/ssl/certs/client.cert.pem
TLS_KEY /home/ldap-user/ssl/certs/keys/client.key.pem
```

Esta configuración mínima es todo lo que se necesita para la autentificación de un cliente.

Schema

En el archivo `slapd.conf`, los esquemas (schema) aparecen cerca de la parte superior del archivo. A continuación se muestra un ejemplo de algunos de los esquemas que se pueden establecer.

> **Nota:** En el directorio `/etc/ldap/schema` se encuentran varias definiciones de esquemas para LDAP.

Ejemplo 4-12. Esquemas en un archivo de configuración `slapd.conf`

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/misc.schema
include         /etc/ldap/schema/openldap.schema
include         /etc/ldap/schema/inetorgperson.schema
```

Resumen de configuración

Existen varios grados de configuración SSL que se pueden establecer. La Tabla 4-2 resume las directivas y los valores que estas han de tomar para realizar desde una configuración básica (“Básica”) a una muy estricta (“La mejor”) en el servidor, en cuanto a conexiones SSL se refiere.

Tabla 4-2. Resumen de configuración SSL en LDAP

Archivo	Directiva	Básica	OK	Buena	Mejor	La mejor
`slapd.conf`	TLSCACertificateFile o TLSCACertificatePath	x	x	x	x	x
	TLSCertificateFile	x	x	x	x	x
	TLSCertificateKeyFile	x	x	x	x	x
	TLSCipherSuite	-	x	x	x	x
	TLSVerifyClient	never	never	allow	try	demand
`ldap.conf`	TLS_CACERT	-	x	x	x	x
	TLS_CACERTDIR (opcional)	-	x	x	x	x
	TLS_REQCERT	never	never	allow	try	demand
`ldaprc` o `.ldaprc`	TLS_CERT	-	-	-	x	x
	TLS_KEY	-	-	-	x	x

LEYENDA:

-: no se usa

x: se usa y se ha de asignar un nombre de archivo o un directorio

Note: El valor por defecto de TLSVerifyClient es “never” y el valor por defecto de TLS_REQCERT es “demand”

Solución temporal a los problemas de OpenLDAP en Debian GNU/Linux

Descripción del problema

Debido a un problema de licencias con OpenSSL, los desarrolladores de Debian han decidido incorporar GNU TLS (http://www.gnu.org/software/gnutls/) al paquete de OpenLDAP de esta distribución.

Este soporte no se ha incorporado oficialmente al proyecto OpenLDAP, y la implementación que se distribuye desde Debian no funciona correctamente. El principal problema que se ha presentado en la

realización de esta documentación, relacionado con el soporte de gnutls por parte de OpenLDAP, ha sido que no reconoce el certificado generado en la la sección de nombre *Creación de un certificado*, por lo que no puede verificar su autenticidad, y por lo tanto no se puede establecer una conexión segura.

Posible solución: uso de OpenSSL

La primera solución que se planteó, para poder llevar a cabo la parte de cifrado de esta documentación, fue el empleo de OpenSSL en detrimento de GNU TLS[3].

La solución pasaba por especificar, en las opciones de compilación de OpenLDAP, el empleo de OpenSSL para el cifrado (en Debian se utiliza GNU TLS por defecto). Para ello, y teniendo en cuenta el reporte 214753 (http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=214753) [4] del sistema de seguimiento de errores de Debian, se recompiló el paquete OpenLDAP con esta nueva opción y se probó el funcionamiento del sistema.

Con el uso de OpenSSL, en lugar de GNU TLS, el certificado ya era reconocido y permitía realizar conexiones cifradas con el servidor LDAP. Pero ahora se presentaba un nuevo problema[5]: tras finalizar la ejecución de cualquier orden que implicara la conexión cifrada con el servidor LDAP, se obtenía una *violación de segmento* (*segmentation fault*). Este problema impedía, por ejemplo, hacer uso de las cuentas almacenadas en el directorio LDAP para acceder al sistema.

Después de un período de pruebas y análisis del problema, se consiguió solucionarlo, presentando la solución en la siguiente sección.

Solución temporal propuesta

Después del planteamiento del problema (la sección de nombre *Descripción del problema*), la solución que se ha llevado a cabo ha sido la de eliminar los parches aplicados por los desarrolladores de Debian, para dar soporte GNU TLS a OpenLDAP, entre otros.

> **Atención**
>
> De todas formas, ha de tomarse esta solución como algo temporal (a la espera de que se solucionen los problemas con el paquete de Debian). Si se desea hacer uso de cifrado junto con OpenLDAP en un entorno de producción, sería recomendable utilizar la versión oficial estable de OpenLDAP (en estos momentos es la versión 2.2.*), que todavía no tiene paquetes para Debian.

En las siguientes secciones se muestran los pasos seguidos para aplicar la solución planteada.

Obtención del código fuente de OpenLDAP

Puede obtener el código fuente de la versión 2.1.30 de OpenLDAP de dos formas: a partir del proyecto OpenLDAP o de los distintos mirrors de Debian. Si opta por la segunda opción, tendrá que teclear la siguiente orden en un directorio en el que tenga permisos de escritura:

Ejemplo 4-13. Obtención del código fuente de OpenLDAP

```
$ /usr/bin/apt-get source openldap2
```

> **Nota:** Asegúrese de tener una entrada *deb-src* en el archivo `/etc/apt/sources.list` que apunte a uno de los mirrors de Debian, para poder bajarse el código fuente de OpenLDAP.

Aplicación del parche

La solución planteada se muestra en forma de parche a las fuentes de OpenLDAP. Dependiendo de donde haya obtenido el código fuente, tendrá que aplicar uno u otro parche (ambos darán el mismo resultado):

- Si ha obtenido el código fuente de OpenLDAP del proyecto oficial, ha de aplicar el siguiente parche: openldap-2.1.30-debianized.patch.bz2 (http://guepardo.dyndns.org:8080/sergio-gonzalez/doc/10-ldap-samba-cups-pykota/recursos/openldap-2.1.30-debianized.patch.bz2).
- Si ha preferido obtener el código fuente desde Debian, ha de aplicar el siguiente parche: openldap-2.1.30-without-gnutls.patch.bz2 (http://guepardo.dyndns.org:8080/sergio-gonzalez/doc/10-ldap-samba-cups-pykota/recursos/openldap-2.1.30-without-gnutls.patch.bz2).

El proceso para aplicar los parches es similar en ambas situaciones, por lo que aquí sólo se mostrará el proceso para una de ellas. Se aplicará el parche al código fuente obtenido desde Debian.

Ejemplo 4-14. Aplicando el parche a las fuentes de OpenLDAP

```
$ cd openldap2-2.1.30/
/usr/bin/bzcat ../openldap-2.1.30-without-gnutls.patch.bz2 | /usr/bin/patch -p1
patching file configure
patching file configure.in
patching file contrib/ldapc++/config.guess
patching file contrib/ldapc++/config.sub
patching file debian/changelog
patching file debian/control
patching file include/ldap_pvt_gnutls.h
patching file include/portable.h.in
patching file libraries/libldap/getdn.c
patching file libraries/libldap/gnutls.c
patching file libraries/libldap/Makefile.in
patching file libraries/libldap/tls.c
patching file libraries/libldap_r/Makefile.in
patching file servers/slapd/schema_init.c
```

Resolviendo las dependencias de compilación

El último paso, antes de proceder a recompilar el código, es la resolución de las dependencias de compilación de OpenLDAP. Para ello, ha de ejecutar:

Ejemplo 4-15. Resolviendo las dependencias de compilación para OpenLDAP

```
# /usr/bin/apt-get build-dep openldap2
```

La orden anterior instalará dos paquetes, *libgnutls11-dev* y *libgcrypt11-dev*, que no son necesarios tras aplicar el parche, por lo que puede desinstalarlos si lo considera oportuno.

Compilación del paquete

Ahora ya está todo listo para proceder a recompilar el paquete, para ello teclee:

Ejemplo 4-16. Compilando OpenLDAP

```
$ /usr/bin/dpkg-buildpackage -us -uc -b -rfakeroot
```

Tras la compilación, se habrán generado los siguientes paquetes:

Ejemplo 4-17. Listado de paquetes de OpenLDAP

```
$ /bin/ls -l ../*deb
-rw-r--r--  1 sergio src 112810 2004-09-21 22:12 ldap-utils_2.1.30-3.1_i386.deb
-rw-r--r--  1 sergio src 284366 2004-09-21 22:12 libldap2_2.1.30-3.1_i386.deb
-rw-r--r--  1 sergio src 321336 2004-09-21 22:12 libldap2-dev_2.1.30-3.1_i386.deb
-rw-r--r--  1 sergio src  71864 2004-09-21 22:12 libslapd2-dev_2.1.30-3.1_all.deb
-rw-r--r--  1 sergio src 945220 2004-09-21 22:12 slapd_2.1.30-3.1_i386.deb
```

Instalación de los nuevos paquetes

La única acción que nos queda por hacer es la instalación de los nuevos paquetes que se han generado. Para ello teclee:

Ejemplo 4-18. Instalación de los nuevos paquetes de OpenLDAP

```
# /usr/bin/dpkg -i ../slapd_2.1.30-3.1_i386.deb \
                   ../ldap-utils_2.1.30-3.1_i386.deb \
                   ../libldap2_2.1.30-3.1_i386.deb
(Leyendo la base de datos ...
132792 ficheros y directorios instalados actualmente.)
Preparando para reemplazar slapd 2.1.30-3 (usando slapd_2.1.30-3.1_i386.deb) ...
Stopping OpenLDAP: slapd.
Stopping OpenLDAP: slapd.
Desempaquetando el reemplazo de slapd ...
Preparando para reemplazar ldap-utils 2.1.30-3 (usando ldap-utils_2.1.30-3.1_i386.deb) ...
Desempaquetando el reemplazo de ldap-utils ...
Preparando para reemplazar libldap2 2.1.30-3 (usando libldap2_2.1.30-3.1_i386.deb) ...
Desempaquetando el reemplazo de libldap2 ...
Configurando libldap2 (2.1.30-3.1) ...

Configurando slapd (2.1.30-3.1) ...
Starting OpenLDAP: slapd.
```

```
Configurando ldap-utils (2.1.30-3.1) ...
```

Con esto se finalizaría la instalación del servidor OpenLDAP modificado.

Probando el servidor en modo seguro

En este punto ya se puede re/iniciar el demonio **slapd** con la nueva configuración de seguridad. Para ello emplee la orden **/etc/init.d/slapd restart** (en el Ejemplo 3-7 se muestra como hacerlo).

En las siguientes secciones se verá la forma de comprobar que OpenLDAP se comporta como debe. Para cumplir este objetivo, se hará uso de las herramientas que vienen con OpenSSL para verificar las conexiones SSL y se realizarán búsquedas en el directorio LDAP.

Comprobando la conexión SSL

> **Nota:** Antes de ejecutar la siguiente orden, ha de asegurarse que valor tiene la variable *TLSVerifyClient*. Si su valor es *demand*, la orden no se ejecutará correctamente, ya que el cliente no se ha autentificado, como se requiere en la configuración de OpenLDAP.

Nótese que a la orden del Ejemplo 4-19 se le pasa como argumento[6] el certificado de la entidad certificadora del cliente. ¿Por qué se ha de especificar el certificado, si ya se ha configurado en el archivo `ldap.conf`? la razón es porque la orden que estamos ejecutando, es una orden dependiente de OpenSSL y no de OpenLDAP.

Ejemplo 4-19. Comprobando la conexión SSL sin autentificación del cliente

```
$ /usr/bin/openssl s_client -connect gsr.pt:636 -showcerts -state \
                            -CAfile /etc/ldap/ssl/cacert.pem
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv2/v3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=1 /C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
verify return:1
depth=0 /C=PT/ST=Braganca/L=Braganca/O=SubGSR/OU=Controle de \
                                              acesso/CN=gsr.pt/emailAddress=sergio@gsr.pt
verify return:1
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
```

```
---
Certificate chain
 0 s:/C=PT/ST=Braganca/L=Braganca/O=SubGSR/OU=Controle de \
                                              acesso/CN=gsr.pt/emailAddress=sergio@gsr.pt
   i:/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
-----BEGIN CERTIFICATE-----
MIIDkDCCAvmgAwIBAgIBATANBgkqhkiG9w0BAQQFADB+MQswCQYDVQQGEwJQVDER
MA8GA1UECBMIQnJhZ2FuY2ExETAPBgNVBAcTCEJyYWdhbmNhMRYwFAYDVQQKEw1D
b21wYW5oaWEgR1NSMSAwHgYDVQQLExdVbmlkYWRlIGRlIGNlcnRpZmljYWRvczEP
MA0GA1UEAxMGZ3NyLnB0MB4XDTA0MDkyMzE2MTYxMVoXDTA1MDkyMzE2MTYxMVow
gZAxCzAJBgNVBAYTAlBUMREwDwYDVQQIEwhCcmFnYW5jYTERMA8GA1UEBxMIQnJh
Z2FuY2ExDzANBgNVBAoTBlN1YkdTUjEbMBkGA1UECxMSQ29udHJvbGUgZGUgYWNl
c3NvMQ8wDQYDVQQDEwZnc3IucHQxHDAaBgkqhkiG9w0BCQEWDXNlcmdpb0Bnc3Iu
cHQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKu8Yqp1rXZtBea+wre3Hyg6
ue0LshFqnSd7BmmJOhM9KYUNAoe3rM9GsAE6MMYuJROvbzW20Cyu+0Ikd/PH4abL
ADXKA76x2N0i3ta84pTUGq5Hg5UMoq4fw9P0HX7NzJxIKGM1XK97yb/4994rCWHG
QDB2459RKNBhshia2YpTAgMBAAGjggEJMIIBBTAJBgNVHRMEAjAAMCwGCWCGSAGG
+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU
jGYsPg9jL1Mp+ijqf1mkFkzffGwwgaoGA1UdIwSBojCBn4AU8TR3gKQ0S3HIv4Fs
3wyY02K3EL6hgYOkgYAwfjELMAkGA1UEBhMCUFQxETAPBgNVBAgTCEJyYWdhbmNh
MREwDwYDVQQHEwhCcmFnYW5jYTEWMBQGA1UEChMNQ29tcGFuaGlhIEdTUjEgMB4G
A1UECxMXVW5pZGFkZSBkZSBjZXJ0aWZpY2Fkb3MxDzANBgNVBAMTBmdzci5wdIIB
ADANBgkqhkiG9w0BAQQFAAOBgQAnQ1RGFN31LWRAtN1itHnWkzLUVg2ngGBqkxrC
AuP4M9lNMscLNCkBcpgaqsY0eFARDZKrMbqbPyc5GhmLoCzXylYEacSuzOXc+s7a
EaklDNvWjGCxhpoCBsXE2o+Opk2EBj3hzj7Z+tRb1UQ2T0iI0KvsA+WnT5Lojtuq
iX4C5A==
-----END CERTIFICATE-----
 1 s:/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
   i:/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
-----BEGIN CERTIFICATE-----
MIIDUDCCArmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB+MQswCQYDVQQGEwJQVDER
MA8GA1UECBMIQnJhZ2FuY2ExETAPBgNVBAcTCEJyYWdhbmNhMRYwFAYDVQQKEw1D
b21wYW5oaWEgR1NSMSAwHgYDVQQLExdVbmlkYWRlIGRlIGNlcnRpZmljYWRvczEP
MA0GA1UEAxMGZ3NyLnB0MB4XDTA0MDkyMzE2MDY1NFoXDTA1MDkyMzE2MDY1NFow
fjELMAkGA1UEBhMCUFQxETAPBgNVBAgTCEJyYWdhbmNhMREwDwYDVQQHEwhCcmFn
YW5jYTEWMBQGA1UEChMNQ29tcGFuaGlhIEdTUjEgMB4GA1UECxMXVW5pZGFkZSBk
ZSBjZXJ0aWZpY2Fkb3MxDzANBgNVBAMTBmdzci5wdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA15+Ciw1MUiRiY88v0rsAZDr+W/w4uQ3bx20v3ddE9Ok0mwv0
vE+DDJjKVUL4FK0rUe8ReDka4D3kB9j2vshWJjf2pA5nWtsoBgm5Dft0RIHM82GM
KCqeG5Lb7/21UaKloJNXTDPfh/HVydQzt2Uivbss3iUdGaDuKCt7IKynA/kCAwEA
AaOB3TCB2jAdBgNVHQ4EFgQU8TR3gKQ0S3HIv4Fs3wyY02K3EL4wgaoGA1UdIwSB
ojCBn4AU8TR3gKQ0S3HIv4Fs3wyY02K3EL6hgYOkgYAwfjELMAkGA1UEBhMCUFQx
ETAPBgNVBAgTCEJyYWdhbmNhMREwDwYDVQQHEwhCcmFnYW5jYTEWMBQGA1UEChMN
Q29tcGFuaGlhIEdTUjEgMB4GA1UECxMXVW5pZGFkZSBkZSBjZXJ0aWZpY2Fkb3Mx
DzANBgNVBAMTBmdzci5wdIIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUA
A4GBAEyudW3FLXIFNbWQ7qJqEE6KhrsiSgR1+VjavJZJP0j2A5sf0vsp083mWJd5
yCWvgxb/Bcx2kbi9KjeP/dtYJM0drAQzFAW4CQQBNxsk3lNkEMot0/8epybirKVG
nThgAkySYQDPXfNEc5qSm2eAgLI7aElBLHQk2R6YVn26i0Gu
-----END CERTIFICATE-----
---
Server certificate
subject=/C=PT/ST=Braganca/L=Braganca/O=SubGSR/OU=Controle de \
                                            acesso/CN=gsr.pt/emailAddress=sergio@gsr.pt
```

```
issuer=/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
---
No client certificate CA names sent ❶
---
SSL handshake has read 1933 bytes and written 340 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES256-SHA
    Session-ID: C5101CF18CB3C821E1AD7C6CCD74693773C1AF75D2A209C6E12075B300A29CF2
    Session-ID-ctx:
    Master-Key: DB2972AF0D2AFF52B57861BBFE8164F5DE2347D3B5248C8D193C26F9B2DA93C6FFB16\
                                                          A705BAD5447716F7BAB2DA958D6
    Key-Arg   : None
    Start Time: 1095969142
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
```

❶ Esta línea indica que el cliente no se ha autentificado ante el servidor.

> **Nota:** Normalmente, para finalizar la ejecución de la orden anterior, se ha de pulsar **Ctrl**+**c**. No se preocupe por ello.

Ahora se verá un ejemplo donde el cliente se autentifica ante el servidor:

Ejemplo 4-20. Comprobando la conexión SSL con autentificación del cliente

```
$ /usr/bin/openssl s_client -connect gsr.pt:636 -state \
                            -CAfile /etc/ldap/ssl/cacert.pem \
                            -cert /home/certs/ldap.cliente.cert.pem \
                            -key /home/certs/ldap.cliente.key.pem
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv2/v3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=1 /C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
verify return:1
depth=0 /C=PT/ST=Braganca/L=Braganca/O=SubGSR/OU=Controle de \
                                              acesso/CN=gsr.pt/emailAddress=sergio@gsr.pt
verify return:1
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server certificate request A ❶
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A ❷
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write certificate verify A ❸
SSL_connect:SSLv3 write change cipher spec A
```

```
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
---
Certificate chain
 0 s:/C=PT/ST=Braganca/L=Braganca/O=SubGSR/OU=Controle de \
                                                acesso/CN=gsr.pt/emailAddress=sergio@gsr.pt
   i:/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
-----BEGIN CERTIFICATE-----
MIIDkDCCAvmgAwIBAgIBATANBgkqhkiG9w0BAQQFADB+MQswCQYDVQQGEwJQVDER
MA8GA1UECBMIQnJhZ2FuY2ExETAPBgNVBAcTCEJyYWdhbmNhMRYwFAYDVQQKEw1D
b21wYW5oaWEgR1NSMSAwHgYDVQQLExdVbmlkYWRlIGRlIGNlcnRpZmljYWRvczEP
MA0GA1UEAxMGZ3NyLnB0MB4XDTA0MDkyMzE2MTYxMVoXDTA1MDkyMzE2MTYxMVow
gZAxCzAJBgNVBAYTAlBUMREwDwYDVQQIEwhCcmFnYW5jYTERMA8GA1UEBxMIQnJh
Z2FuY2ExDzANBgNVBAoTBlN1YkdTUjEbMBkGA1UECxMSQ29udHJvbGUgZGUgYWNl
c3NvMQ8wDQYDVQQDEwZnc3IucHQxHDAaBgkqhkiG9w0BCQEWDXNlcmdpb0Bnc3Iu
cHQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKu8Yqp1rXZtBea+wre3Hyg6
ue0LshFqnSd7BmmJOhM9KYUNAoe3rM9GsAE6MMYuJROvbzW20Cyu+0Ikd/PH4abL
ADXKA76x2N0i3ta84pTUGq5Hg5UMoq4fw9P0HX7NzJxIKGM1XK97yb/4994rCWHG
QDB2459RKNBhshia2YpTAgMBAAGjggEJMIIBBTAJBgNVHRMEAjAAMCwGCWCGSAGG
+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU
jGYsPg9jL1Mp+ijqf1mkFkzffGwwgaoGA1UdIwSBojCBn4AU8TR3gKQ0S3HIv4Fs
3wyY02K3EL6hgYOkgYAwfjELMAkGA1UEBhMCUFQxETAPBgNVBAgTCEJyYWdhbmNh
MREwDwYDVQQHEwhCcmFnYW5jYTEWMBQGA1UEChMNQ29tcGFuaGlhIEdTUjEgMB4G
A1UECxMXVW5pZGFkZSBkZSBjZXJ0aWZpY2Fkb3MxDzANBgNVBAMTBmdzci5wdIIB
ADANBgkqhkiG9w0BAQQFAAOBgQAnQ1RGFN31LWRAtN1itHnWkzLUVg2ngGBqkxrC
AuP4M9lNMscLNCkBcpgaqsY0eFARDZKrMbqbPyc5GhmLoCzXylYEacSuzOXc+s7a
EaklDNvWjGCxhpoCBsXE2o+Opk2EBj3hzj7Z+tRb1UQ2T0iI0KvsA+WnT5Lojtuq
iX4C5A==
-----END CERTIFICATE-----
 1 s:/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
   i:/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
-----BEGIN CERTIFICATE-----
MIIDUDCCArmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB+MQswCQYDVQQGEwJQVDER
MA8GA1UECBMIQnJhZ2FuY2ExETAPBgNVBAcTCEJyYWdhbmNhMRYwFAYDVQQKEw1D
b21wYW5oaWEgR1NSMSAwHgYDVQQLExdVbmlkYWRlIGRlIGNlcnRpZmljYWRvczEP
MA0GA1UEAxMGZ3NyLnB0MB4XDTA0MDkyMzE2MDY1NFoXDTA1MDkyMzE2MDY1NFow
fjELMAkGA1UEBhMCUFQxETAPBgNVBAgTCEJyYWdhbmNhMREwDwYDVQQHEwhCcmFn
YW5jYTEWMBQGA1UEChMNQ29tcGFuaGlhIEdTUjEgMB4GA1UECxMXVW5pZGFkZSBk
ZSBjZXJ0aWZpY2Fkb3MxDzANBgNVBAMTBmdzci5wdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA15+Ciw1MUiRiY88v0rsAZDr+W/w4uQ3bx20v3ddE9Ok0mwv0
vE+DDjjKVUL4FK0rUe8ReDka4D3kB9j2vshWJjf2pA5nWtsoBgm5Dft0RIHM82GM
KCqeG5Lb7/21UaKloJNXTDPfh/HVydQzt2Uivbss3iUdGaDuKCt7IKynA/kCAwEA
AaOB3TCB2jAdBgNVHQ4EFgQU8TR3gKQ0S3HIv4Fs3wyY02K3EL4wgaoGA1UdIwSB
ojCBn4AU8TR3gKQ0S3HIv4Fs3wyY02K3EL6hgYOkgYAwfjELMAkGA1UEBhMCUFQx
ETAPBgNVBAgTCEJyYWdhbmNhMREwDwYDVQQHEwhCcmFnYW5jYTEWMBQGA1UEChMN
Q29tcGFuaGlhIEdTUjEgMB4GA1UECxMXVW5pZGFkZSBkZSBjZXJ0aWZpY2Fkb3Mx
DzANBgNVBAMTBmdzci5wdIIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUA
A4GBAEyudW3FLXIFNbWQ7qJqEE6KhrsiSgR1+VjavJZJP0j2A5sf0vsp083mWJd5
yCWvgxb/Bcx2kbi9KjeP/dtYJM0drAQzFAW4CQQBNxsk3lNkEMot0/8epybirKVG
nThgAkySYQDPXfNEc5qSm2eAgLI7aElBLHQk2R6YVn26i0Gu
-----END CERTIFICATE-----
---
```

```
Server certificate
subject=/C=PT/ST=Braganca/L=Braganca/O=SubGSR/OU=Controle de \
                                              acesso/CN=gsr.pt/emailAddress=sergio@gsr.pt
issuer=/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
---
Acceptable client certificate CA names ❹
/C=PT/ST=Braganca/L=Braganca/O=Companhia GSR/OU=Unidade de certificados/CN=gsr.pt
---
SSL handshake has read 2072 bytes and written 2274 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES256-SHA
    Session-ID: CE4D0BFD367AF2F4B2E51ECB8C48A1D1A3F5EC0F00346EF13551534C1F1CE8E1
    Session-ID-ctx:
    Master-Key: 4D9089B2602C0376B92079BA539D8D3F244B5CBF31A68FD3A51DDC801251AA16\
                                                  5C194DA63B1BFB7025D818F2480E6450
    Key-Arg   : None
    Start Time: 1095970126
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
```

❶❷❸❹Negociado extra relacionado con la comunicación SSL.

Uso de cifrado con las herramientas de OpenLDAP

OpenLDAP tiene varias herramientas, como son: ldapsearch, ldapadd, ldapmodify y ldapdelete. A continuación se verán algunos ejemplos de su uso, para ilustrar la comunicación mediante SSL y TLS.

Los ejemplos se centrarán en las búsquedas de varias entradas, previamente incorporadas al directorio.

Añadir datos al directorio

Lo primero que se va a hacer es añadir una serie de datos al directorio LDAP, sobre los cuales, posteriormente, se realizarán las búsquedas. Para ello, puede copiar el siguiente texto a un archivo denominado `datos-iniciales.ldif`, por ejemplo.

Tenga en cuenta que ha de eliminar cualquier espacio al inicio o al final de las líneas del ejemplo. Tampoco olvide adaptar el ejemplo que aquí se presenta a su configuración.

```
#datos-iniciales.ldif
dn: cn=sergio,dc=gsr,dc=pt
objectclass: organizationalRole
cn: sergio

dn: ou=unidade de contas,dc=gsr,dc=pt
objectclass: organizationalUnit
ou: unidade de contas
```

```
description: Organizacao de provas que contera ao administrador

dn: cn=senhor administrador,ou=unidade de contas,dc=gsr,dc=pt
objectclass: person
userPassword: chaveprova
description: Usuario de exemplo como administrador
cn: senhor administrador
sn: admin
```

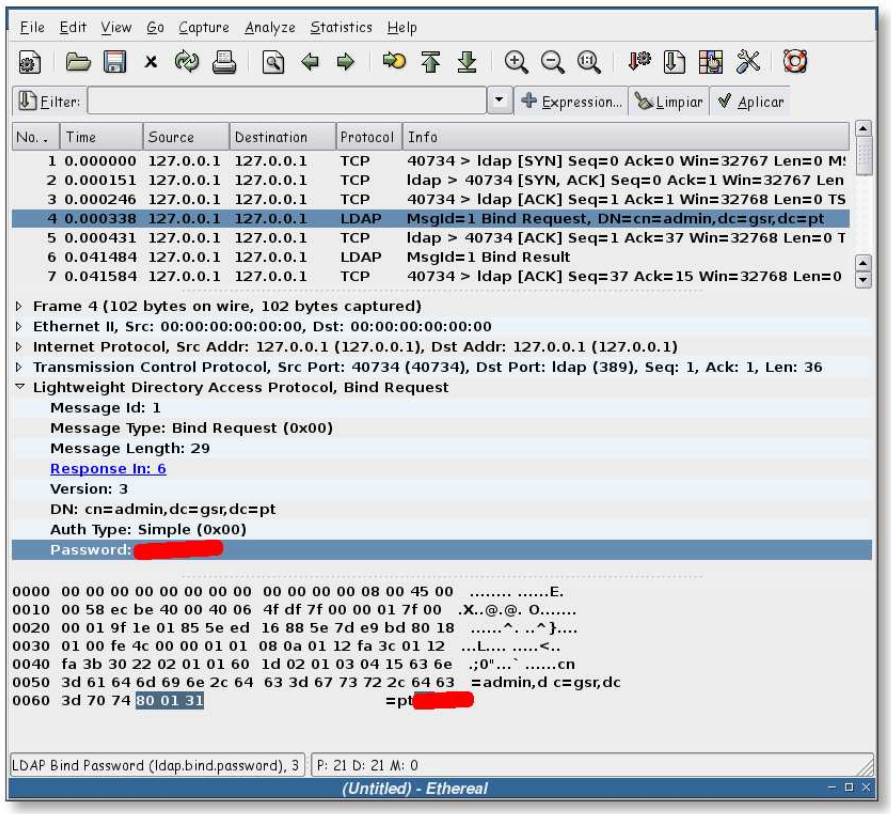
Ahora se procederá a añadir estas entradas a la base de datos de LDAP, para ello haga uso del usuario administrador de su directorio LDAP.

Ejemplo 4-21. Incorporación de datos al directorio LDAP por medio de un archivo LDIF

```
$ /usr/bin/ldapadd -x -D "cn=admin,dc=gsr,dc=pt" -W -f datos-iniciales.ldif
Enter LDAP Password:[Clave]
adding new entry "cn=sergio,dc=gsr,dc=pt"

adding new entry "ou=unidade de contas,dc=gsr,dc=pt"

adding new entry "cn=senhor administrador,ou=unidade de contas,dc=gsr,dc=pt"
```

La orden anterior se ha realizado en texto plano, por lo que la transmisión de la clave del administrador del directorio LDAP se ha hecho sin ningún tipo de cifrado, como se puede apreciar en la siguiente captura de pantalla (debajo del color rojo aparece la clave del administrador):

Figura 4-1. Captura de la clave del administrador del directorio LDAP con ethereal



Al comunicarse con el servidor LDAP sin hacer uso de cifrado, las claves de los usuarios viajan en texto plano, como puede apreciarse en esta captura de pantalla. Las líneas en rojo ocultan la clave del administrador del directorio LDAP capturada por el programa ethereal.

Para evitar esta situación, se puede hacer uso de SSL o TLS en las comunicaciones con el servidor LDAP. Las siguientes secciones explican como hacerlo:

Cómo activar el cifrado SSL en las comunicaciones con el servidor LDAP

Para asegurarse de que sus comunicaciones con el servidor LDAP utilizan SSL al hacer uso de las herramientas que incorpora OpenLDAP, ha de añadir el siguiente parámetro a sus órdenes: “-H ldaps://gsr.pt/”.

Cómo activar el cifrado TLS en las comunicaciones con el servidor LDAP

La principal diferencia entre una conexión SSL y una TLS, es que la primera siempre utilizará el cifrado en la conexión mientras que la segunda provee al cliente la opción de hacer uso de cifrado cuando lo desee.

Tenga en cuenta que por el simple hecho de acceder al servidor mediante *ldap://:389* no asegura que la conexión haga uso de cifrado TLS, pero tampoco si accede mediante *ldaps://*. Para activar una conexión TLS tendrá que hace uso del parámetro "-Z" o "-ZZ".

El parámetro "-ZZ" fuerza que la negociación TLS tenga éxito, mientras que el parámetro "-Z", intenta habilitar el cifrado TLS, pero si no lo consigue, continua con la conexión sin TLS.

Búsquedas en el directorio

En esta sección se realizarán una serie de búsquedas en el directorio. El uso del parámetro *-D "cn=admin,dc=gsr,dc=pt"* es necesario, debido a la restricción de acceso que se ha impuesto en el archivo `slapd.conf`:

```
access to *
        by dn="cn=admin,dc=gsr,dc=pt" write
        by dn="cn=readadmin,dc=gsr,dc=pt" read ❶
        by self write
        by users read
        by anonymous auth
```

❶ Para más datos sobre este usuario, ver el Apéndice A.

Ejemplo 4-22. Devuelve todas las entradas del directorio

Si el cliente se encuentra en la misma máquina que el servidor:

```
$ /usr/bin/ldapsearch -x -b 'dc=gsr,dc=pt' -D "cn=admin,dc=gsr,dc=pt" -W \
                      '(objectclass=*)'
```

Si el cliente se encuentra en una máquina distinta al servidor y se quiere hacer uso de SSL :

```
$ /usr/bin/ldapsearch -x -b 'dc=gsr,dc=pt' -D "cn=admin,dc=gsr,dc=pt" -W \
                      '(objectclass=*)' -H ldaps://gsr.pt/
```

Si el cliente se encuentra en una máquina distinta al servidor y se quiere hacer uso de TLS :

```
$ /usr/bin/ldapsearch -x -b 'dc=gsr,dc=pt' -D "cn=admin,dc=gsr,dc=pt" -W \
                      '(objectclass=*)' -H ldap://gsr.pt/ -ZZ
```

Después de ejecutar las órdenes anteriores, la salida debería ser similar a:

```
Enter LDAP Password:[Clave]
# extended LDIF
#
# LDAPv3
# base <dc=gsr,dc=pt> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# gsr.pt
dn: dc=gsr,dc=pt
objectClass: top
objectClass: dcObject
```

```
objectClass: organization
o: gsr.pt
dc: gsr

# admin, gsr.pt
dn: cn=admin,dc=gsr,dc=pt
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fXkxcFlKZVpQQzQ5Qlk=

# sergio, gsr.pt
dn: cn=sergio,dc=gsr,dc=pt
objectClass: organizationalRole
cn: sergio

# unidade de contas, gsr.pt
dn: ou=unidade de contas,dc=gsr,dc=pt
objectClass: organizationalUnit
ou: unidade de contas
description: Organizacao de provas que contera ao administrador

# senhor administrador, unidade de contas, gsr.pt
dn: cn=senhor administrador,ou=unidade de contas,dc=gsr,dc=pt
objectClass: person
userPassword:: Y2hhdmVwcm92YQ==
description: Usuario de exemplo como administrador
cn: senhor administrador
sn: admin

# search result
search: 3
result: 0 Success

# numResponses: 6
# numEntries: 5
```

Ejemplo 4-23. Devuelve algunas entradas del directorio

```
$ /usr/bin/ldapsearch -x -b 'cn=sergio,dc=gsr,dc=pt' -D "cn=admin,dc=gsr,dc=pt" \
                      '(objectclass=*)' -H ldaps://gsr.pt/ -w clave
# extended LDIF
#
# LDAPv3
# base <cn=sergio,dc=gsr,dc=pt> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# sergio, gsr.pt
dn: cn=sergio,dc=gsr,dc=pt
```

```
objectClass: organizationalRole
cn: sergio

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
$
$ /usr/bin/ldapsearch -x -b 'ou=unidade de contas„dc=gsr,dc=pt' \
                      -D "cn=admin,dc=gsr,dc=pt" '(objectclass=*)' -H ldaps://gsr.pt/ -w clave
# extended LDIF
#
# LDAPv3
# base <ou=unidade de contas,dc=gsr,dc=pt> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# unidade de contas, gsr.pt
dn: ou=unidade de contas,dc=gsr,dc=pt
objectClass: organizationalUnit
ou: unidade de contas
description: Organizacao de provas que contera ao administrador

# senhor administrador, unidade de contas, gsr.pt
dn: cn=senhor administrador,ou=unidade de contas,dc=gsr,dc=pt
objectClass: person
userPassword:: Y2hhdmVwcm92YQ==
description: Usuario de exemplo como administrador
cn: senhor administrador
sn: admin

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Como ha podido comprobar, la comunicación con el servidor LDAP se realiza satisfactoriamente, bien sea utilizando cifrado bien sin el.

Notas

1. La versión de OpenLDAP utilizada para la realización de esta documentación es la 2.1.30-3.
2. Tenga en cuenta que el directorio donde almacene el certificado del usuario ha de ser accesible por todo el mundo.

3. Esta decisión se tomó, debido a que si se empleaba el paquete oficial de OpenLDAP, tal cual, no se presentaban los problemas aquí detallados. Ha de recordarse que la distribución oficial de OpenLDAP hace uso de OpenSSL.
4. OpenLDAP source package does not compile correctly with '--with-tls=openssl' flag
5. Inexistente si se hacía uso de la distribución oficial de OpenLDAP.
6. -CAfile

Capítulo 5. Autentificación de usuarios a través de OpenLDAP

Introducción

En este capítulo se verá como configurar una máquina para que sus usuarios se autentifiquen a través de un servidor LDAP. Para ello se han de modificar dos aspectos del comportamiento del sistema:

- El mapeado entre los números de identificación de los usuarios y sus nombres (utilizados, por ejemplo, por **/bin/ls -l**) o la localización del directorio *home*. La búsqueda de este tipo de información es responsabilidad del servicio de nombres, cuyo archivo de configuración es: `/etc/nsswitch.conf`.
- La autentificación (comprobación de claves), que es responsabilidad del subsistema PAM, cuya configuración se hace a través del directorio `/etc/pam.d/`

Ambos subsistemas se han de configurar separadamente, pero en este caso, ambos se van a configurar de tal forma que hagan uso de LDAP.

En este capítulo sólo se trata la instalación y configuración de los dos aspectos arriba expuestos, de todas formas, hay un tercer punto que, en sistemas en producción, sería interesante abordar: la caché del servicio de nombres. Para ver en qué consiste y como se instala y configura, vea el Apéndice B.

Nota: Este capítulo se ha basado en la entrada bibliográfica metaconsultancy01, entre otras.

Instalación del software necesario

Antes de poder autentificar a los usuarios a través de un servidor LDAP, es necesario instalar algunas utilidades en el cliente, como pam_ldap y nss_ldap. Esta sección mostrará la forma de instalación de estas utilidades.

Instalación de *nss-ldap*

nss-ldap permite a un servidor LDAP actuar como un servidor de nombres. Esto significa que provee la información de las cuentas de usuario, los IDs de los grupos, la información de la máquina, los alias, los grupos de red y básicamente cualquier cosa que normalmente se obtiene desde los archivos almacenados bajo `/etc` o desde un servidor NIS.

En Debian GNU/Linux el paquete *libnss-ldap* provee esta funcionalidad, por lo que será instalado en la máquina, como muestra el Ejemplo 5-2

Antes de proceder a su instalación, eche un vistazo a la descripción del paquete:

Ejemplo 5-1. Instalación de *libnss-ldap*

```
$ /usr/bin/apt-cache show libnss-ldap
Package: libnss-ldap
Priority: extra
Section: net
Installed-Size: 220
Maintainer: Stephen Frost <sfrost@debian.org>
Architecture: i386
Version: 220-1 ❶
Depends: libc6 (>= 2.3.2.ds1-4), libdb4.2, libkrb53 (>= 1.3.2), libldap2 (>= 2.1.17-1), debconf
Recommends: nscd, libpam-ldap
Filename: pool/main/libn/libnss-ldap/libnss-ldap_220-1_i386.deb
Size: 73688
MD5sum: 1d2667fd13efc134e5baaa1d63f45372
Description: NSS module for using LDAP as a naming service
 This package provides a Name Service Switch that allows your LDAP server
 act as a name service. This means providing user account information,
 group id’s, host information, aliases, netgroups, and basically anything
 else that you would normally get from /etc flat files or NIS.
 .
 If used with glibc 2.1’s nscd (Name Service Cache Daemon) it will help
 reduce your network traffic and speed up lookups for entries.
```

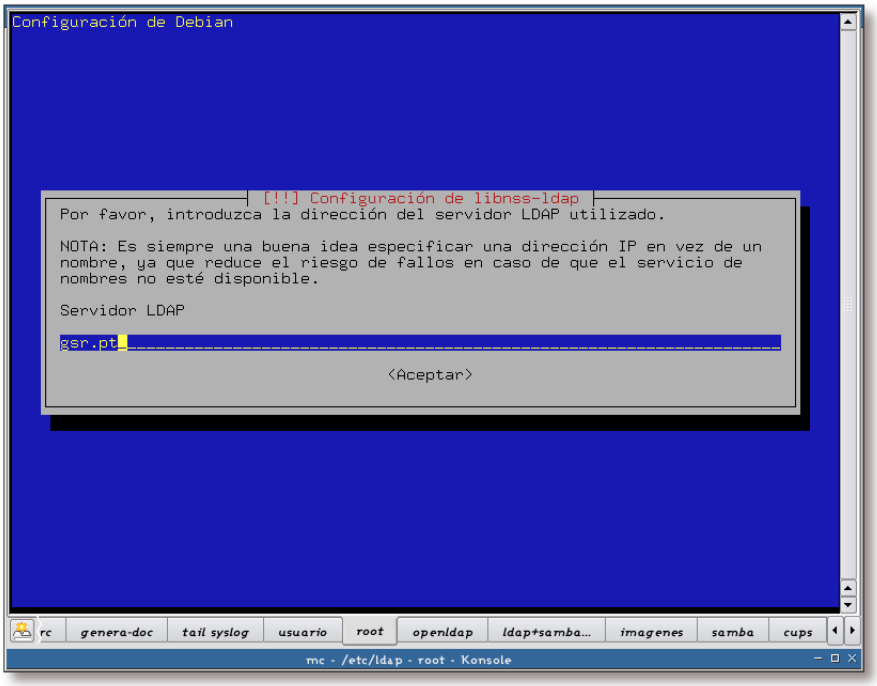
❶ Versión de *libnss-ldap* que se va a instalar

Ejemplo 5-2. Instalación de *libnss-ldap* (primera parte)

```
# /usr/bin/apt-get install libnss-ldap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Paquetes recomendados
  nscd libpam-ldap
Se instalarán los siguientes paquetes NUEVOS:
  libnss-ldap
0 actualizados, 1 se instalarán, 0 para eliminar y 27 no actualizados.
Se necesita descargar 0B/73,7kB de archivos.
Se utilizarán 225kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...
```

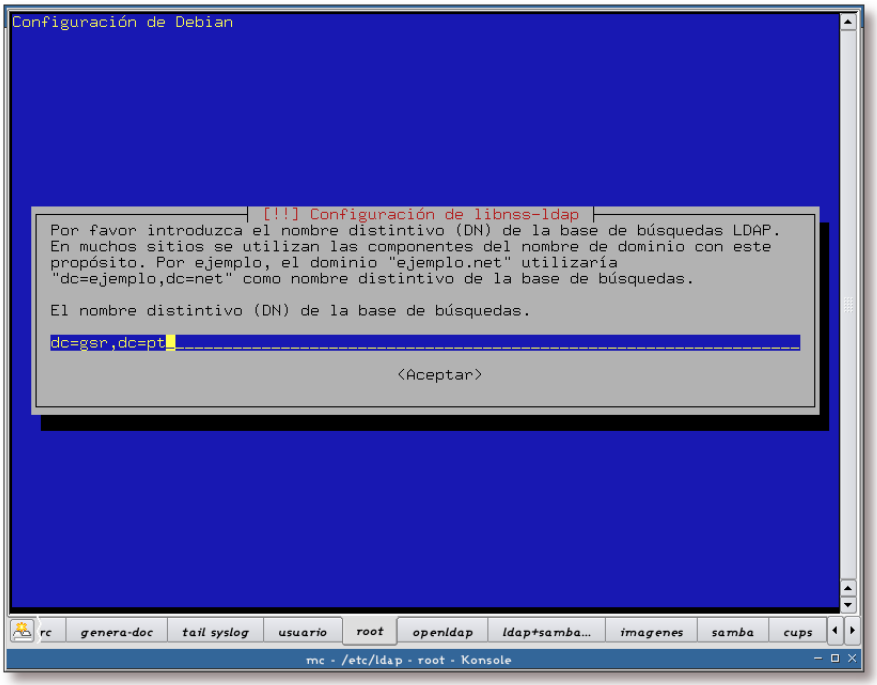
> **Nota:** Si ha instalado previamente este paquete, es posible que no se muestren todas las pantallas listadas seguidamente. Para forzar una configuración completa, teclee la siguiente orden:
>
> ```
> # /usr/sbin/dpkg-reconfigure --priority=low libnss-ldap
> ```

Figura 5-1. Dirección del servidor LDAP



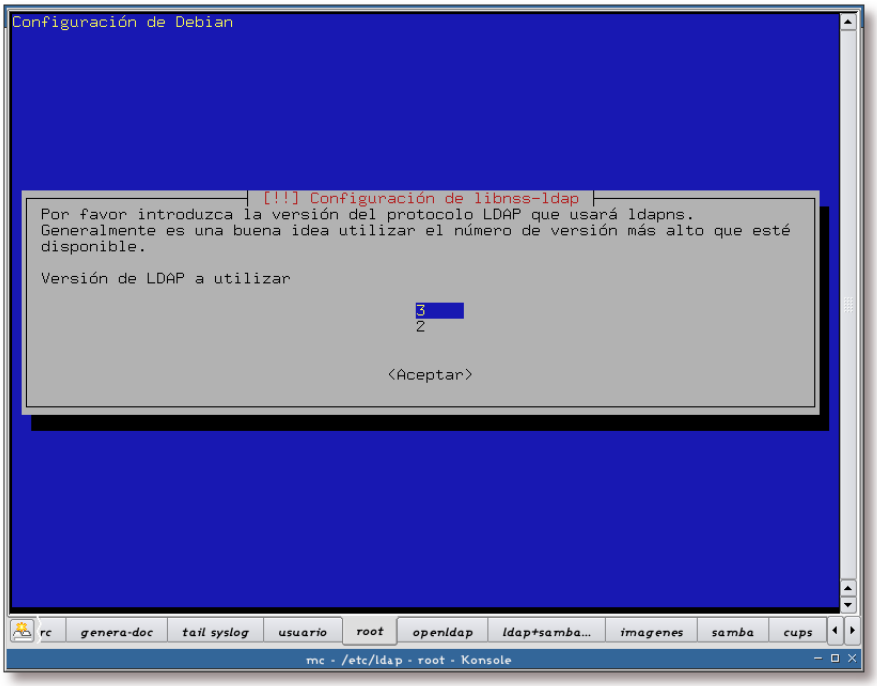
Dirección del servidor LDAP que se va a utilizar para la autentificación de usuarios.

Figura 5-2. Nombre distintivo de la base de búsquedas



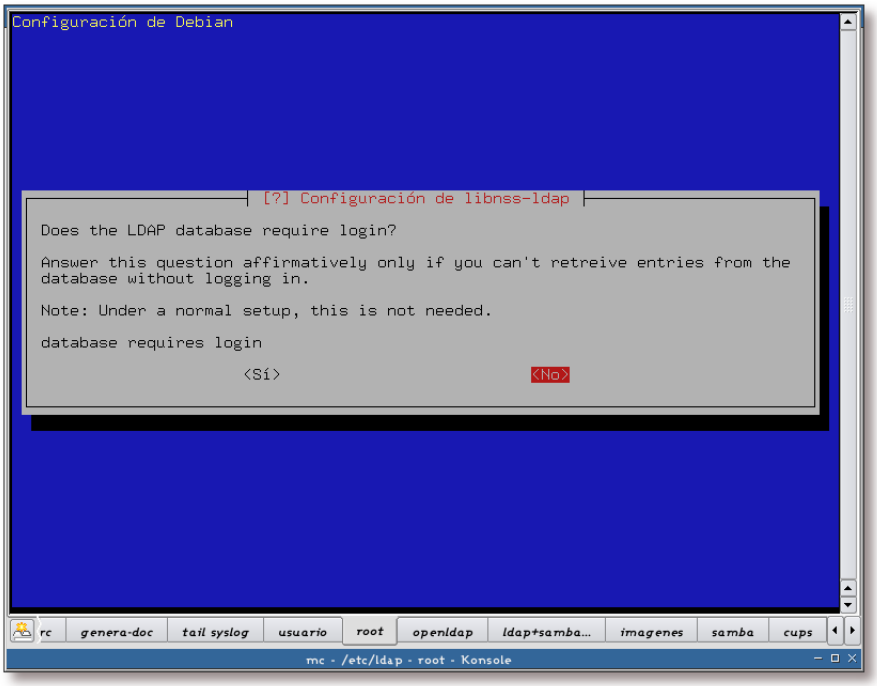
Nombre distintivo de la base de búsquedas.

Figura 5-3. Versión del protocolo LDAP



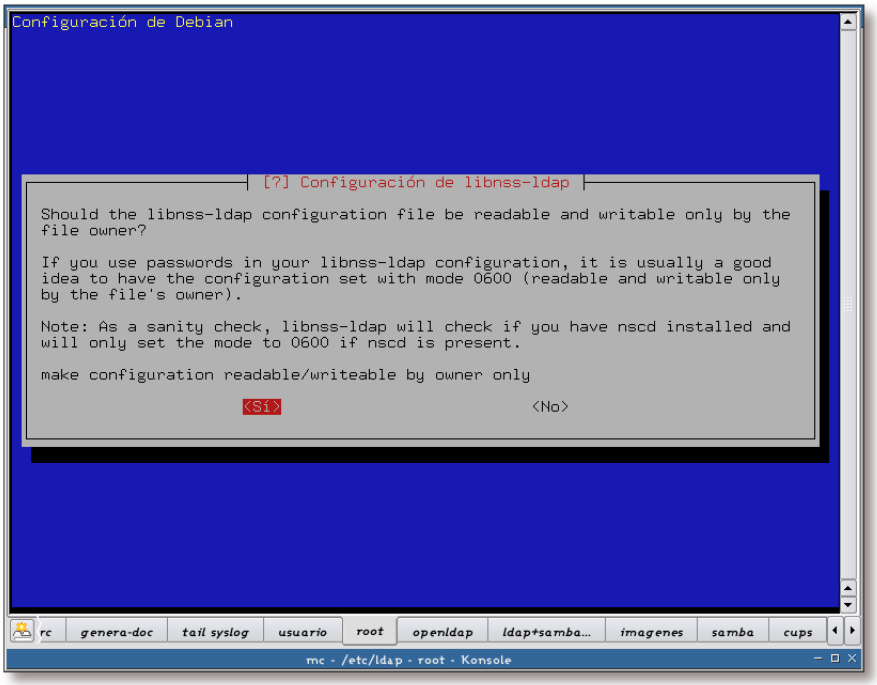
Versión del protocolo LDAP a utilizar, es recomendable hacer uso de la versión 3.

Figura 5-4. Método de acceso a la base de datos



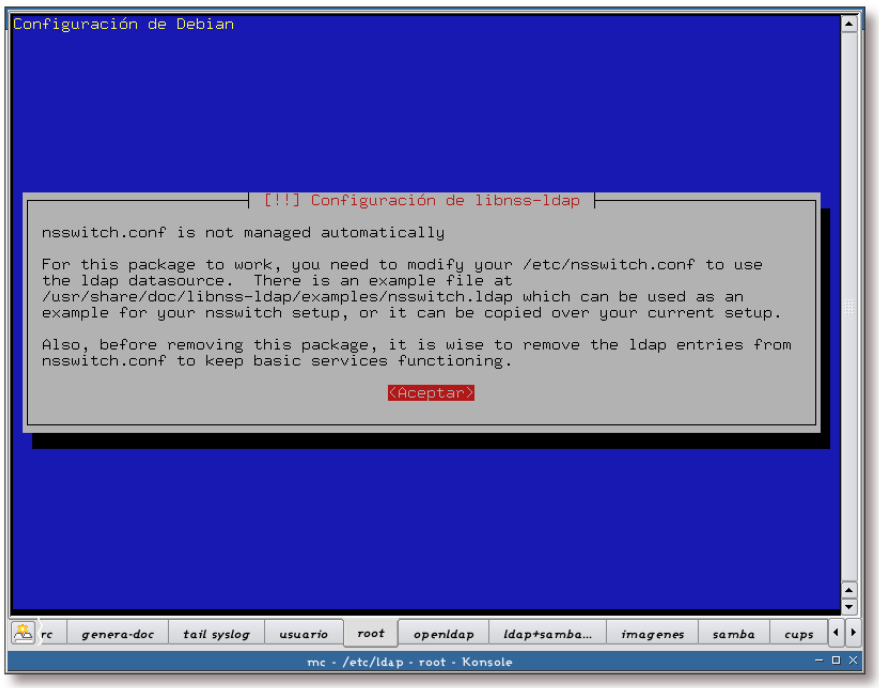
En este ejemplo no se necesita autentificarse para acceder a la base de datos LDAP, por lo que se responde: *NO*.

Figura 5-5. Permisos del archivo de configuración



Es buena idea que sólo el propietario del archivo pueda leer su información, máxime cuando este puede tener claves. Por este motivo se responde que *Sí* a esta pregunta.

Figura 5-6. Información sobre *libnss-ldap*



La configuración del paquete nos muestra información adicional sobre el mismo. Si se quiere ver el ejemplo del archivo `/etc/nsswitch.conf` que provee *libnss-ldap*, acceda a: `/usr/share/doc/libnss-ldap/examples/nsswitch.ldap`. De todas formas, en el Apéndice T se dispone de un ejemplo.

Ejemplo 5-3. Instalación de *libnss-ldap* (segunda parte)

```
Seleccionando el paquete libnss-ldap previamente no seleccionado.
(Leyendo la base de datos ...
132069 ficheros y directorios instalados actualmente.)
Desempaquetando libnss-ldap (de .../libnss-ldap_220-1_i386.deb) ...
Configurando libnss-ldap (220-1) ...

localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

La configuración de *nss-ldap* se almacena en el archivo `/etc/libnss-ldap.conf`, cuyo contenido se encuentra en el Apéndice V.

> **Aviso**
>
> El archivo `/etc/libnss-ldap.conf` se ha de poder leer por todos los usuarios del sistema, para asegurarse de que es legible por todo el mundo, puede ejecutar: **/bin/chmod 644 /etc/libnss-ldap.conf**.

Instalación de *pam_ldap*

pam_ldap permite hacer uso de un servidor LDAP para la autentificación de usuarios (comprobación de claves) a aquellas aplicaciones que utilicen PAM.

En Debian GNU/Linux el paquete *libpam-ldap* provee esta funcionalidad, por lo que será instalado en la máquina, como muestra el Ejemplo 5-5

Antes de proceder con su instalación, eche un vistazo a la descripción del paquete:

Ejemplo 5-4. Información sobre el paquete *libpam-ldap*

```
$ /usr/bin/apt-cache show libpam-ldap
Package: libpam-ldap
Priority: extra
Section: admin
Installed-Size: 288
Maintainer: Stephen Frost <sfrost@debian.org>
Architecture: i386
Version: 169-1 ❶
Depends: libc6 (>= 2.3.2.ds1-4), libldap2 (>= 2.1.17-1), libpam0g (>= 0.76), debconf (>= 0.5)
Suggests: libnss-ldap
Filename: pool/main/libp/libpam-ldap/libpam-ldap_169-1_i386.deb
Size: 52158
MD5sum: 5d1d450ac94b5e86a313a8277f5f84a3
Description: Pluggable Authentication Module allowing LDAP interfaces
 This module let's you use you LDAP server to authenticate users with
 programs that utilize PAM. If used along with libnss-ldap, you can
 replace your entire flat file (/etc/*) structure or NIS with LDAP.
```

❶ Versión de *libpam-ldap* que acompaña a Debian GNU/Linux en su versión "en desarrollo", que va a ser instalada

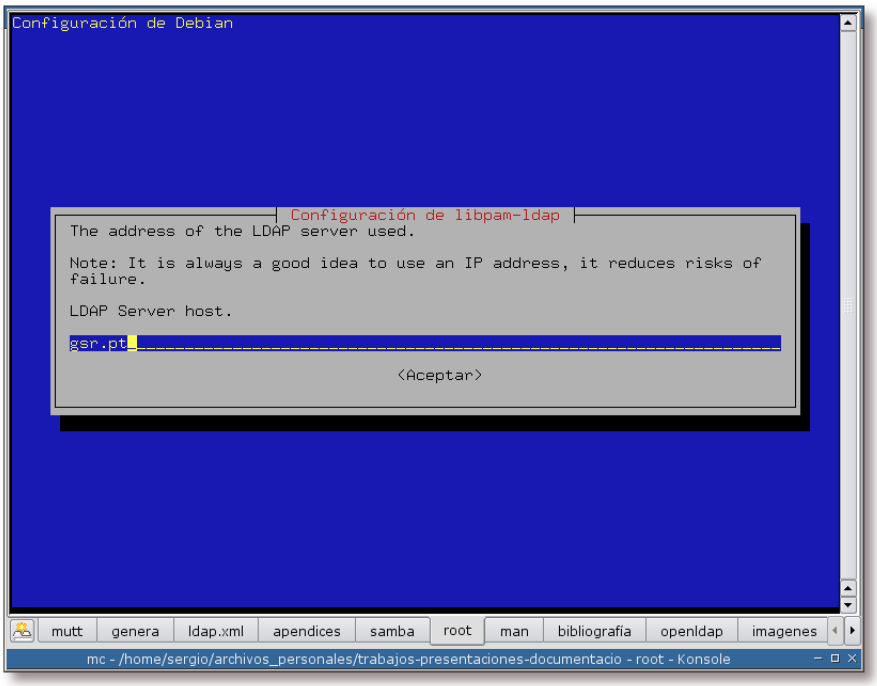
Ejemplo 5-5. Instalación de *libpam-ldap* (primera parte)

```
# /usr/bin/apt-get install libpam-ldap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Paquetes sugeridos:
  libnss-ldap
Se instalarán los siguientes paquetes NUEVOS:
  libpam-ldap
0 actualizados, 1 se instalarán, 0 para eliminar y 27 no actualizados.
```

```
Se necesita descargar 0B/52,2kB de archivos.
Se utilizarán 295kB de espacio de disco adicional después de desempaquetar.

Preconfiguring packages ...
```

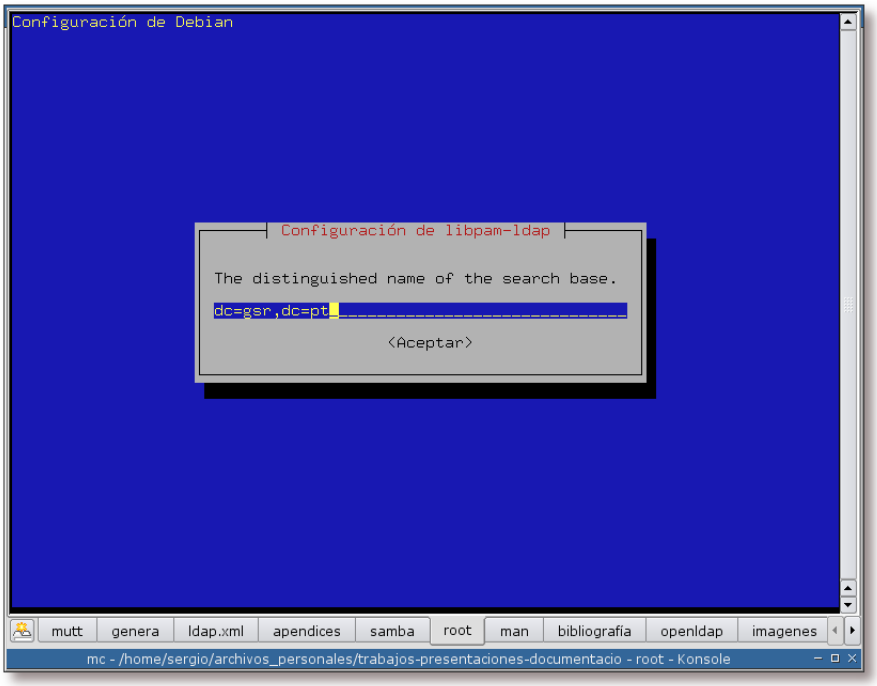
> **Nota:** Si ha instalado previamente este paquete, es posible que no se muestren todas las pantallas listadas seguidamente. Para forzar una configuración completa, teclee la siguiente orden:
>
> ```
> # /usr/sbin/dpkg-reconfigure --priority=low libpam-ldap
> ```

Figura 5-7. URL del servidor LDAP



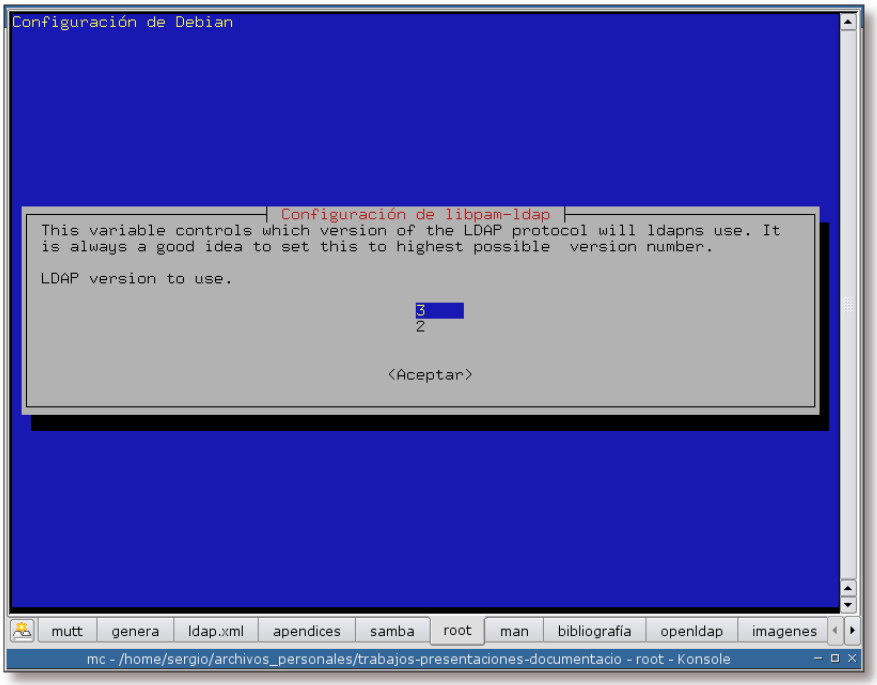
Dirección del servidor LDAP que se va a utilizar para la autentificación de usuarios.

Figura 5-8. Nombre distintivo de la base de búsquedas



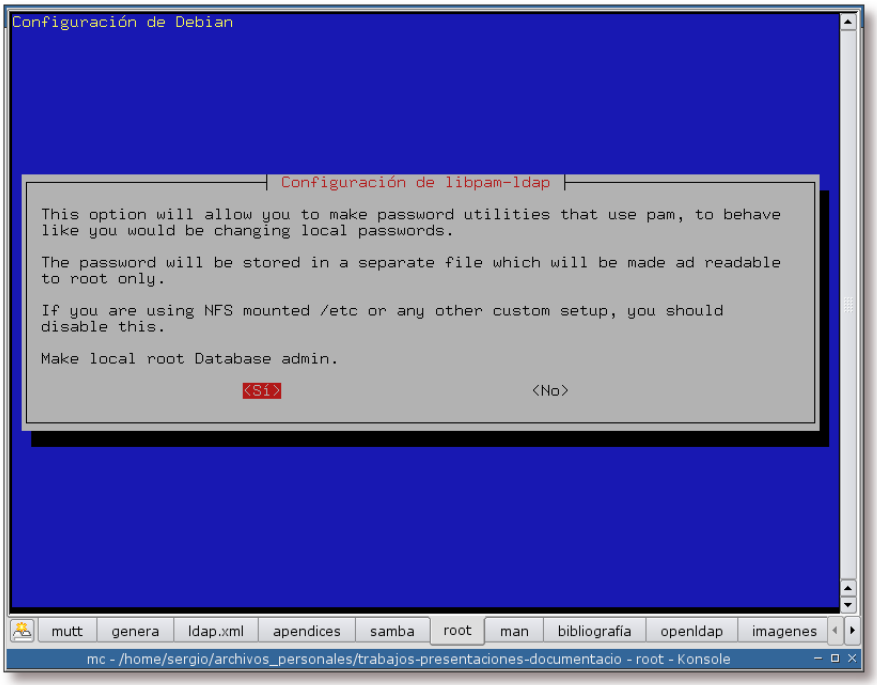
Nombre distintivo de la base de búsquedas.

Figura 5-9. Versión del protocolo LDAP



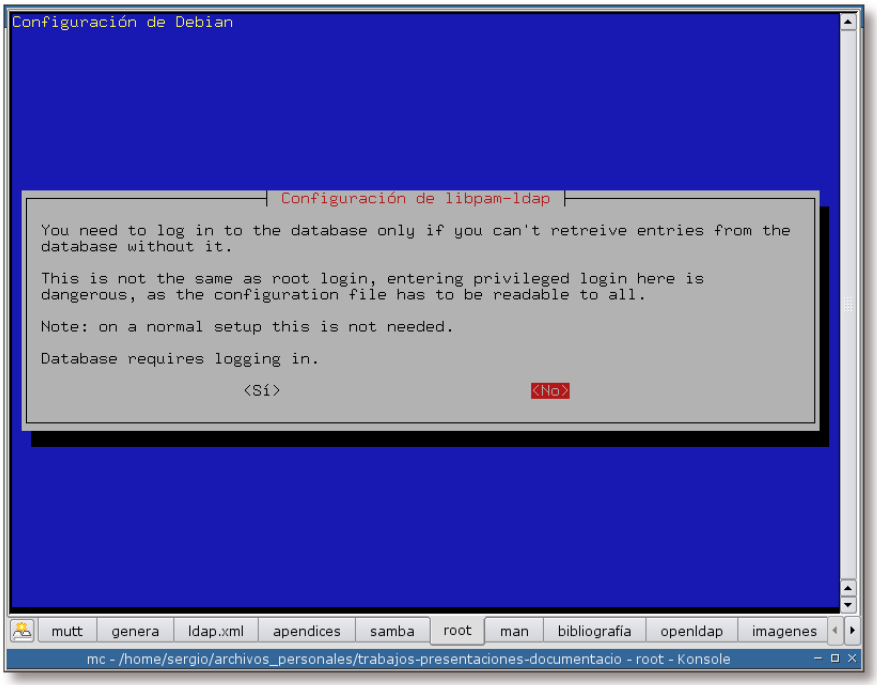
Versión del protocolo LDAP a utilizar, es recomendable hacer uso de la versión 3.

Figura 5-10. Comportamiento a la hora del cambio de claves



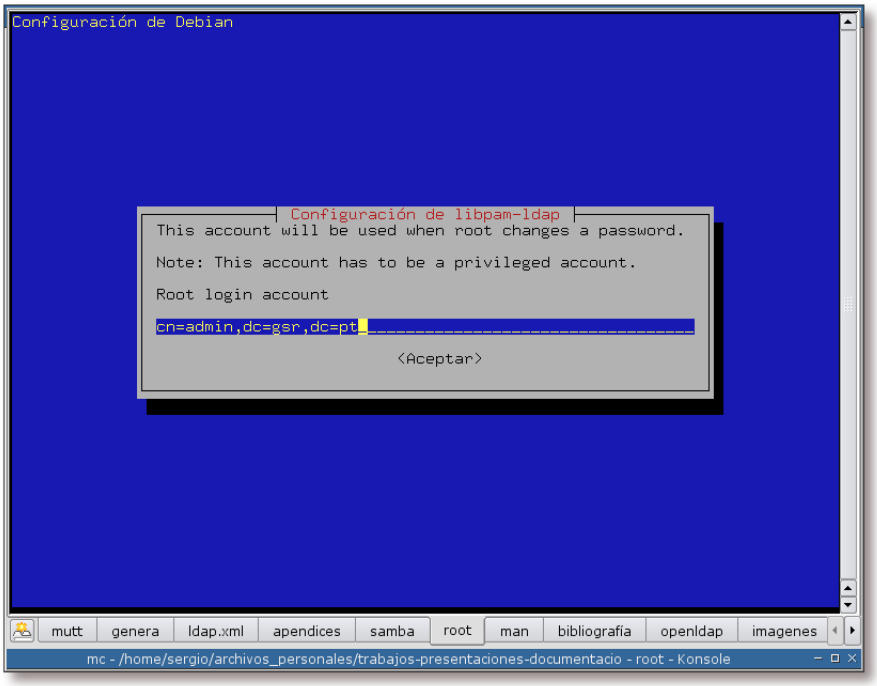
Contestamos afirmativamente a esta pregunta, de esta forma, aquellas aplicaciones que cambien claves por medio de PAM, se comportarán como si lo hiciesen de forma local.

Figura 5-11. ¿Necesita autentificación la conexión con la base de datos?



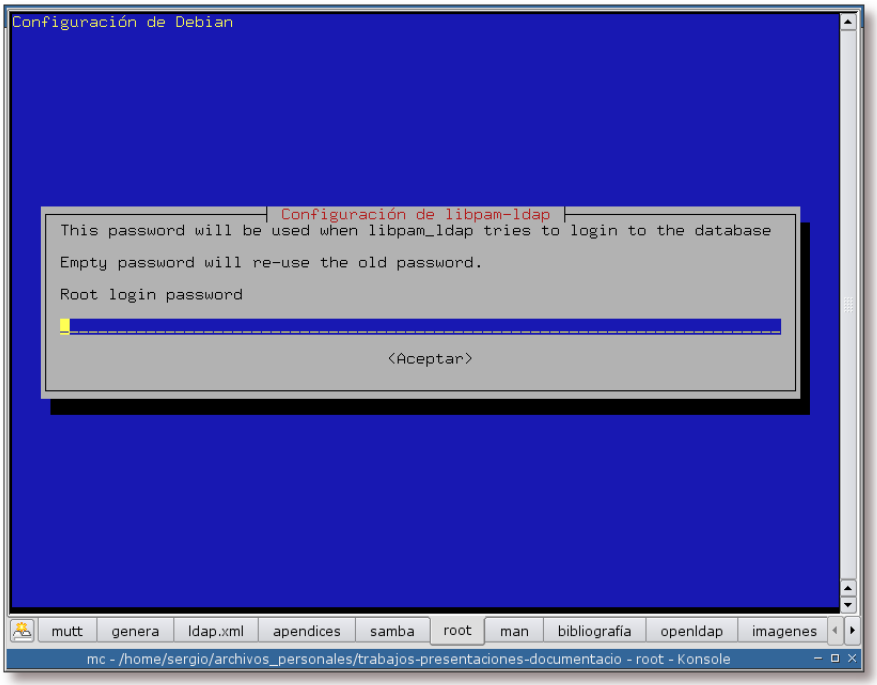
En este ejemplo no se necesita autentificarse para acceder a la base de datos LDAP, por lo que se responde que NO.

Figura 5-12. Administrador de LDAP



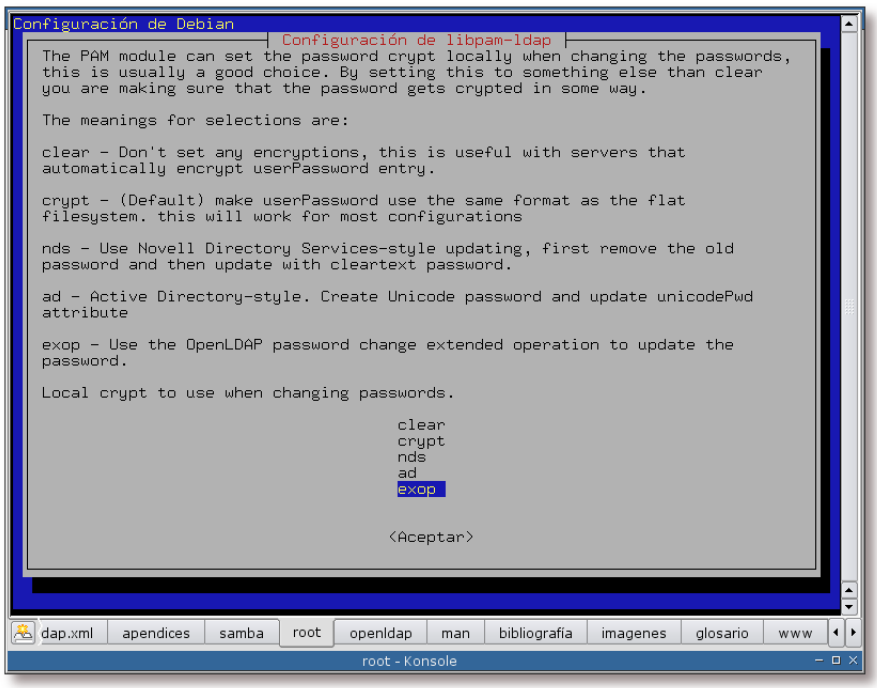
Cuenta del administrador de LDAP, en este caso “admin”.

Figura 5-13. Clave del administrador de LDAP



Se introduce la clave del administrador de LDAP.

Figura 5-14. Elección el método de cifrado para las claves



El método de cifrado elegido para almacenar las claves ha sido “exop”, de esta forma *pam-ldap* utilizará el algoritmo de hash especificado en el archivo `/etc/ldap/slapd.conf`, en lugar de realizar la operación hash localmente y escribir el resultado en la base de datos directamente.

Ejemplo 5-6. Instalación de *libpam-ldap* (segunda parte)

```
Seleccionando el paquete libpam-ldap previamente no seleccionado.
(Leyendo la base de datos ...
132024 ficheros y directorios instalados actualmente.)
Desempaquetando libpam-ldap (de .../libpam-ldap_169-1_i386.deb) ...
Configurando libpam-ldap (169-1) ...

localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

La configuración del módulo *pam_ldap.so* se almacena en el archivo `/etc/pam_ldap.conf`, cuyo contenido se encuentra en el Apéndice U.

Aviso

El archivo `/etc/pam_ldap.conf` se ha de poder leer por todos los usuarios del sistema, para asegurarse de que es legible por todo el mundo, puede ejecutar: **/bin/chmod 644 /etc/pam_ldap.conf**.

En estos momentos el sistema ya está listo para la configuración de los distintos servicios que utilizan PAM, de forma que estos utilicen LDAP para la comprobación de la clave. Cada servicio que hace uso de PAM para la autentificación, posee su propio archivo bajo el directorio `/etc/pam.d/`. Para que dicho servicio utilice LDAP en la comprobación de claves, se ha de modificar su archivo de configuración. Esto se verá en la la sección de nombre *Configuración de PAM*.

Configuración de los archivos necesarios

> **Aviso**
>
> Tenga en cuenta que va a modificar archivos de configuración utilizados para el ingreso al sistema. Sería recomendable que tuviese en todo momento una consola de root abierta, por si deja de funcionar la autentificación.

`/etc/libnss-ldap.conf` y `/etc/pam_ldap.conf`

Como en ambos archivos se van a modificar las mismas variables, se ha utilizado una única sección para ambos. Las modificaciones que se van a realizar a continuación son, principalmente, necesarias para activar el cifrado en las conexiones con el servidor LDAP. Esto es necesario si no se quiere que las claves de los usuarios, por ejemplo, viajen por la red en texto plano.

> **Nota:** En los apéndices Apéndice V y Apéndice U verá un ejemplo completo de estos archivos de configuración.

Usuario con el que conectar al directorio LDAP

Debido a que durante el proceso de configuración de OpenLDAP se va a prohibir a los usuarios anónimos acceder a la información almacenada en el directorio, se hace necesario especificar un usuario válido con el cual autentificarse para realizar las operaciones llevadas a cabo por *libnss-ldap* y *libpam-ldap*, entre otras. Este usuario y su clave estarán especificados por las variables *binddn* y *bindpw*, respectivamente.

```
binddn cn=readadmin,dc=gsr,dc=pt ❶
bindpw ********** ❷
```

❶ En el Apéndice A tiene un ejemplo sobre como crear y configurar un usuario que sólo tenga permisos de lectura en el directorio LDAP.

❷ Clave del usuario en texto plano.

Asegúrese de que está descomentada la variable “rootbinddn” y su valor es el usuario administrador del directorio LDAP, en este caso: “cn=admin,dc=gsr,dc=pt”.

```
rootbinddn cn=admin,dc=gsr,dc=pt
```

Una vez hecho esto, tendrá que almacenar la clave del administrador en el archivo `/etc/ldap.secret`, para ello teclee:

Ejemplo 5-7. Creación del directorio `/etc/ldap.secret`

```
# /bin/echo "clave-del-administrdor" > /etc/ldap.secret
# /bin/chmod 600 /etc/ldap.secret
```

> **Nota:** La clave se almacena en texto plano, por lo que el archivo `/etc/ldap.secret` ha de pertenecer al usuario *root* y sus permisos han de ser 600.

Protocolo de cifrado empleado en las comunicaciones

La primera opción que se activará será el soporte para TLS, para ello ha de descomentar la línea siguiente en ambos archivos de configuración:

```
ssl start_tls
```

> **Nota:** Si desea que las conexiones utilicen SSL, tendrá que sustituir la línea anterior por la siguiente:
>
> `ssl on`
>
> En esta documentación se ha preferido utilizar TLS en las comunicaciones, por lo que se ha empleado la opción “ssl start_tls”.

Opciones para el cifrado (certificados)

Para las conexiones cifradas se requiere un certificado en el servidor y este ha de ser válido. Para ello ha de descomentar la siguiente línea:

```
tls_checkpeer yes
```

Para poder verificar la validez del certificado del servidor, se ha de proporcionar la CA que lo generó, esto se indica con la siguiente línea:

```
tls_cacertfile /etc/ldap/ssl/cacert.pem
```

Algoritmo de cifrado

Algoritmos de cifrado que se desean utilizar:

```
tls_ciphers TLSv1
```

Certificados y llaves de los clientes

Como en la configuración de OpenLDAP se ha requerido la autentificación del cliente antes de conectarse al servidor (vea el Ejemplo 4-9), se hace necesario descomentar las siguientes líneas:

```
tls_cert
tls_key
```

`/etc/nsswitch.conf`

`nsswitch.conf` es el fichero de configuración de las Bases de Datos del Sistema y del sistema de Conmutación de los Servicios de Nombres (Name Service Switch).

En otras palabras, es un archivo que indica el orden y el procedimiento a seguir para la búsqueda de la información requerida, por ejemplo, para hacer búsquedas de hosts o usuarios.

La forma de configurar este archivo es muy simple: primero se especifica la base de datos sujeta a la búsqueda (primera columna) seguida del procedimiento que se va a emplear para realizar una búsqueda sobre la misma (columnas siguientes).

De esta forma, basta con configurar el procedimiento de búsqueda para que haga uso de LDAP en algún momento. El Ejemplo 5-8 muestra como hacerlo:

Ejemplo 5-8. Modificaciones en el de configuración `/etc/nsswitch.conf`

```
passwd: ❶         files ldap ❷
group: ❸          files ldap ❹
shadow: ❺         files ldap ❻
hosts: ❼          files ldap dns ❽
```

❶❸❺❼Bases de datos de búsqueda

❷❹❻Procedimiento de búsqueda: primero se mira en los archivos locales y luego en el directorio LDAP.

❽ Procedimiento de búsqueda: primero se mira en los archivos locales, luego en el directorio LDAP y finalmente se realiza una consulta al servidor DNS.

> **Nota:** En el Apéndice T se encuentra disponible un ejemplo completo de configuración de `nsswitch.conf`.

> **Sugerencia:** Fíjese que no se ha eliminado el uso de los ficheros locales, “files”, ya que algunos usuarios y grupos de usuarios (como por ejemplo root) permanecerán de forma local. Si su sistema no utiliza la entrada “files”, y el servidor LDAP se cae, nadie, ni siquiera root, podrá entrar al sistema.

nss-ldap espera que las cuentas sean objetos con los siguientes atributos: *uid*, *uidNumber*, *gidNumber*, *homeDirectory* y *loginShell*. Estos atributos están permitidos por la clase objeto (objectClass) *posixAccount*.

Una vez realizada la configuración, se puede comprobar que todo funciona bien con la orden **getent** seguido de la base de datos de búsqueda deseada (por ejemplo: **/usr/bin/getent hosts**). Como resultado se mostrará la base de datos consultada por pantalla.

Configuración de PAM

PAM permite configurar el método de autentificación que van a utilizar las aplicaciones que hagan uso de él. Gracias a esto, se pueden añadir fácilmente distintas opciones de autentificación, como el uso de una base de datos LDAP.

En las siguientes secciones se mostrarán los archivos que se han de modificar para lograr la autentificación a través de LDAP.

> **Importante:** Hace relativamente poco tiempo que la versión en desarrollo de Debian (Sid) ha cambiado la forma de configuración de PAM. Actualmente posee secciones comunes a todos los archivos, estas secciones comunes son aquellos archivos localizados en el directorio `/etc/pam.d/` que comiencen por "common-".
>
> Se ha de tener en cuenta la forma en la que se ha ido actualizando Debian Sid en la última temporada, para determinar si su sistema está utilizando o no dichos archivos comunes para la configuración de PAM.
>
> Un buen punto de partida, sería ojear los archivos almacenados bajo `/etc/pam.d/` y comprobar las diferencias entre los archivos con extensión *.dpkg-dist* y los que no la tienen.

pam-ldap asume que las cuentas del sistema son objetos con los siguientes atributos: *uid* y *userPassword*. Los atributos están permitidos por la clase objeto (objectClass) *posixAccount*.

`/etc/pam.d/common-account`

Este archivo ha de tener únicamente estas entradas:

Ejemplo 5-9. Opciones de configuración para `/etc/pam.d/common-account`

```
account required          pam_unix.so
account sufficient        pam_ldap.so
```

> **Nota:** En el Apéndice W tiene un ejemplo completo de este archivo de configuración.

`/etc/pam.d/common-auth`

Este archivo ha de tener únicamente estas entradas:

Ejemplo 5-10. Opciones de configuración para `/etc/pam.d/common-auth`

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

> **Nota:** En el Apéndice X tiene un ejemplo completo de este archivo de configuración.

`/etc/pam.d/common-session`

Este archivo ha de tener únicamente estas entradas:

Ejemplo 5-11. Opciones de configuración para `/etc/pam.d/common-session`

```
session required        pam_limits.so
session required        pam_unix.so
session optional        pam_ldap.so
```

Si desea que el sistema sea capaz de crear directorios home "al vuelo" (piense en el siguiente caso: acaba de añadir un usuario en la base de datos LDAP, pero no ha creado un directorio home para este usuario en el sistema), puede utilizar el módulo *pam_mkhomedir* para este propósito. Para ello añada la siguiente línea al principio del archivo `common-session`:

Ejemplo 5-12. Opción para crear directorios home al vuelo

```
session required        pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

> **Importante:** El módulo *pam_mkhomedir* sólo crea directorios de un nivel. Es importante tener esto en cuenta para planificar la estructura del home de los usuarios.

> **Nota:** En el Apéndice Z tiene un ejemplo completo de este archivo de configuración.

`/etc/pam.d/common-passwd`

Este archivo ha de tener únicamente estas entradas:

Ejemplo 5-13. Opciones de configuración para `/etc/pam.d/common-password`

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

❶ Se supone que tiene instalado en su sistema la librería *libpam-cracklib*, si no es así, instálela o comente esta línea.

Nota: En el Apéndice Y tiene un ejemplo completo de este archivo de configuración.

Comprobando que todo funciona

Ahora que ya está el sistema preparado para hacer uso de LDAP en la autentificación de los usuarios, sería recomendable hacer algunas pruebas con la nueva configuración para ver si todo funciona correctamente.

La orden **pamtest** puede ayudar a realizar estas pruebas. **pamtest** acepta dos parámetros: el primero es el nombre del servicio al cual se va a conectar para realizar la autentificación, el segundo es el nombre del usuario que se va a autentificar sobre dicho servicio. Veamos unos ejemplos:

Nota: La orden **pamtest** se encuentra en el paquete *libpam-dotfile*, por lo que si no está disponible en su sistema, ha de ejecutar:

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

Ejemplo 5-14. Comprobando la configuración del sistema con pamtest

```
$ /usr/bin/pamtest passwd sergio
Trying to authenticate <sergio> for service <passwd>.
Password:[Clave del usuario]
Authentication successful.
$ /usr/bin/pamtest ssh sergio
Trying to authenticate <sergio> for service <ssh>.
Password:[Clave fallida del usuario]
Failed to authenticate: Authentication service cannot retrieve authentication info.
$ /usr/bin/pamtest ssh sergio
Trying to authenticate <sergio> for service <ssh>.
Password:[Clave del usuario]
Authentication successful.
```

Una vez se ha llegado a este punto, el sistema ya está preparado para autentificar a los usuarios a través de LDAP. En el apartado dedicado a Samba

(Parte II en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*) veremos, entre otras cosas, como añadir usuarios a la base de datos LDAP.

II. Samba

Capítulo 6. Conceptos teóricos

Introducción

> **Nota:** Este capítulo se ha basado en las introducciones de las entradas bibliográficas EcksteinCollier-BrownKelly01, TsEcksteinCollier-Brown01 y Sharpe01. También se ha de notar que las imágenes y los ejemplos utilizados en este apartado han sido obtenidos o basados en dichos documentos.

Samba es una herramienta de red extremadamente útil para cualquier persona que posea en su red sistemas Unix y Windows. Samba se ejecuta en un sistema Unix, permitiendo a los sistemas Windows compartir archivos e impresoras en la máquina Unix, a la vez que los usuarios de Unix tienen acceso a los recursos compartidos en los sistemas Windows.

Aunque parece natural hacer uso de servidores Windows para servir archivos e impresoras en una red donde haya clientes Windows, hay buenas razones para elegir un servidor Samba para estos servicios. Samba es un software confiable que corre en un sistema operativo confiable como Unix, dando como resultado la obtención de menos problemas y bajo coste de mantenimiento. A parte de esto, Samba ofrece mejor rendimiento ante cargas de trabajo extremadamente duras, sobrepasando a un servidor Windows 2000 en un factor de 2 a 1 en un PC con la misma configuración de hardware, de acuerdo con unos *benchmarks* publicados por terceros. Cuando un PC ya no pueda acometer las peticiones de los clientes, debido a la alta carga, el servidor Samba se puede trasladar fácilmente a un mainframe Unix propietario, el cual puede sobrepasar en mucho a un PC corriendo Windows. Si todo esto no fuese suficiente, Samba posee una ventaja muy buena en relación al coste: es libre. No sólo el software está a su disposición libremente, sino que no necesita ningún tipo de licencia para los clientes, ejecutándose en sistemas operativos de gran calidad y libres, como GNU/Linux y FreeBSD.

¿Qué es Samba?

Samba es una suite de aplicaciones Unix que habla el protocolo SMB (Server Message Block). Los sistemas operativos Microsoft Windows y OS/2 utilizan SMB para compartir por red archivos e impresoras y para realizar tareas asociadas. Gracias al soporte de este protocolo, Samba permite a las máquinas Unix *entrar en el juego*, comunicándose con el mismo protocolo de red que Microsoft Windows y aparecer como otro sistema Windows en la red (desde la perspectiva de un cliente Windows). El servidor Samba ofrece los siguientes servicios:

- Compartir uno o varios sistemas de archivos
- Compartir uno o varios sistemas de archivos distribuidos
- Compartir impresoras instaladas en el servidor entre los clientes Windows de la red
- Ayudar a los clientes permitiéndoles navegar por la red
- Autentificar a los clientes que ingresan en un dominio Windows

- Proveer o ayudar con un servidor de resolución de nombres Windows (WINS) [1].

La suite Samba también incluye herramientas para los clientes, que permiten a los usuarios de un sistema Unix acceder a los directorios e impresoras que los sistemas Windows y servidores Samba comparten en la red.

Samba es la idea de Andrew Tridgell, quien actualmente lidera el equipo de desarrollo de Samba. El proyecto nació en 1991 mientras Andrew trabajaba con la suite de *Digital Equipment Corporation* (DEC) llamada Pathworks, creada para conectar ordenadores VAX DEC con los de otras compañías. Sin conocer la transcendencia de lo que estaba haciendo, Andrew creó un programa servidor de archivos para un extraño protocolo que formaba parte de la suite Pathworks. Este protocolo pasó a llamarse más tarde SMB. Unos años más tarde, lo liberó como su servidor SMB particular y lo comenzó a distribuir por Internet bajo el nombre de “SMB Server”. Sin embargo, Andrew no pudo mantener ese nombre -este pertenecía a un producto de otra compañía-, así que intentó lo siguiente para buscarle un nuevo nombre desde Unix:

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

Obteniendo como respuesta:

```
salmonberry
samba
sawtimber
scramble
```

De ésta manera nació el nombre de Samba.

Hoy en día, la suite Samba gira alrededor de un par de demonios Unix que permiten la compartición de recursos entre los clientes SMB de una red. Estos demonios son:

smbd

Demonio que permite la compartición de archivos e impresoras sobre una red SMB y proporciona autentificación y autorización de acceso para clientes SMB.

nmbd

Demonio que soporta el servicio de nombres NetBIOS y WINS, que es una implementación de Microsoft del servicio de nombres NetBIOS (NBNS). Este demonio también ayuda añadiendo la posibilidad de navegar por la red.

Samba actualmente está mantenido y es ampliado por un grupo de voluntarios bajo la supervisión activa de Andrew Tridgell. Al igual que el núcleo Linux, los autores de Samba lo distribuyen como software *open source (http://opensource.org)*, bajo los términos de la licencia GPL (GNU General Public License). Desde su concepción, el desarrollo de Samba ha sido patrocinado en parte por la *Australian National University*, donde Andrew Tridgell hizo su doctorado. A partir de entonces, muchas otras organizaciones han patrocinado a los desarrolladores de Samba, incluyendo LinuxCare, VA Linux Systems, Hewlett-Packard e IBM. Es algo verdaderamente testimonial el que entidades tanto comerciales como no comerciales estén dispuestas a gastar dinero para dar soporte a un esfuerzo Open Source.

Microsoft también ha contribuido ofreciendo la definición de su protocolo SBM al grupo IETF (Internet Engineering Task Force) en 1996, cuyo nombre es *Common Internet File System* (CIFS).

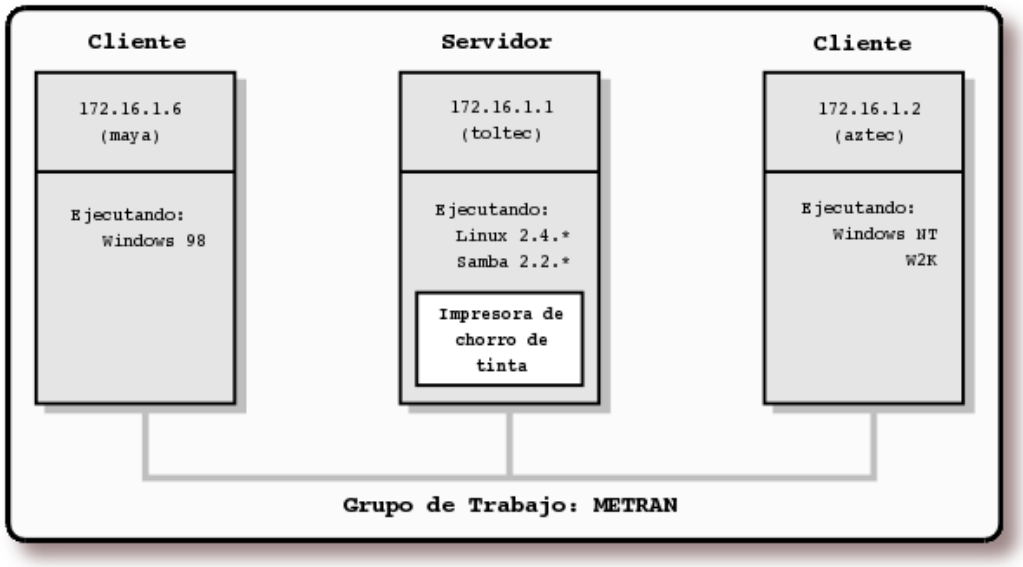
¿Qué puede hacer Samba por mí?

Como se explicó anteriormente, Samba puede ayudar la coexistencia de máquinas Windows y Unix en la misma red. Sin embargo, existen algunas razones por las cuales podría desear instalar un servidor Samba en su red:

- No quiere pagar -o no puede disponer- de un servidor Windows completo, pero todavía necesita la funcionalidad que provee
- Qué las licencias de acceso a los clientes[2] que Microsoft solicita para que cada cliente Windows pueda acceder al servidor Windows sean incosteables
- Tal vez quiera proporcionar un área común para datos o directorios de usuarios en orden a realizar una transición desde un servidor Windows hacia uno Unix, o viceversa
- Desea compartir impresoras entre clientes Windows y Unix
- Tenga que dar soporte a un grupo de usuarios cuyos ordenadores posean una mezcla de sistemas operativos, Windows y Unix
- Quiera integrar la autentificación de Unix y Windows, manteniendo una única base de datos para las cuentas de los usuarios que funcione en ambos sistemas
- Quiera establecer una red entre sistemas Unix, Windows, Macintosh (OS X) y otros, utilizando un único protocolo

A continuación se verá a Samba en acción. Se asume la siguiente configuración de red: un servidor Samba sobre una máquina Unix, cuyo *hostname* es *toltec*, y un par de clientes Windows, denominados *maya* y *aztec*, todos los equipos están conectados gracias a una red de área local (LAN). Se asume también que *toltec* tiene una impresora de inyección de tinta conectada, *lp*, y un disco compartido *spirit* -ambos recursos están disponibles para las otras dos máquinas-. Un gráfico de esta red se muestra en la Figura 6-1.

Figura 6-1. Configuración de red simple con un servidor Samba[3]

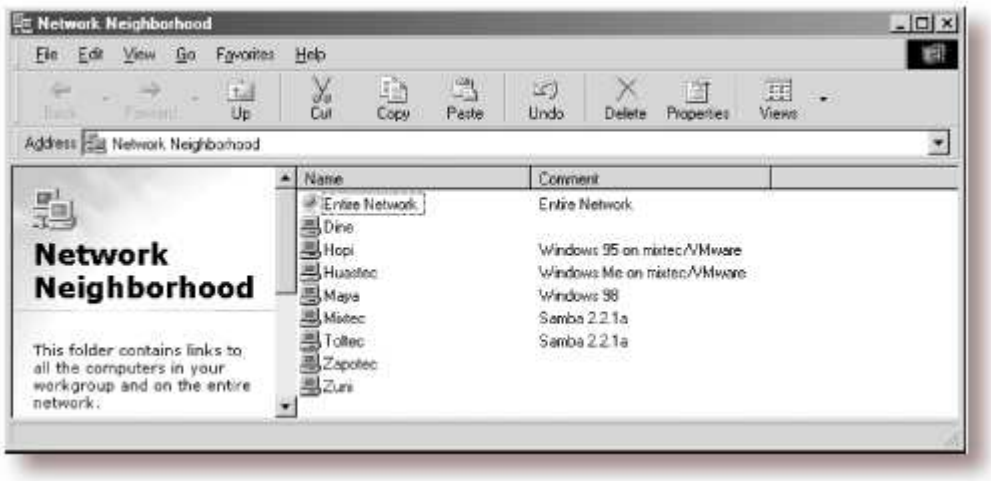


En esta red, cada ordenador comparte el mismo grupo de trabajo (*workgroup*). Un grupo de trabajo no es más que una etiqueta que identifica a un determinado grupo de ordenadores y sus recursos en una red SBM. Pueden existir varios grupos de trabajo sobre la red al mismo tiempo, pero para el ejemplo sólo se tiene uno: el grupo de trabajo *METRAN*.

Compartiendo un disco

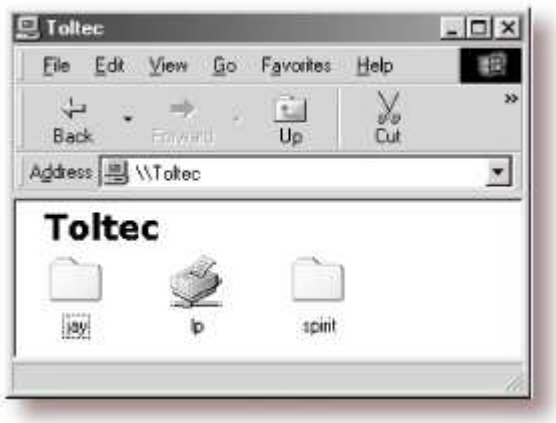
Si todo está bien configurado, se debería ver el servidor Samba, *toltec*, a través del entorno de red de la máquina Windows denominada *maya*. De hecho, la Figura 6-2 muestra el entorno de red de la *maya*, incluyendo a *toltec* y a cada una de las máquinas que residen en el grupo de trabajo *METRAN*. Dese cuenta del icono “Entire Network” al principio de la lista. Como se mencionó anteriormente, pueden existir más grupos de trabajo sobre una red SBM al mismo tiempo. Si un usuario hace *click* sobre ese icono, verá la lista de todos los grupos de trabajo que actualmente existen en la red.

Figura 6-2. Entorno de red



Se puede ver con más detalle los recursos compartidos por *toltec* haciendo doble *click* sobre su icono. Esta acción provoca un contacto con *toltec*, solicitándole la lista de sus recursos compartidos -la impresora y el disco- que proporciona. En este caso, existe una impresora denominada *lp*, un directorio personal denominado *jay* y el disco compartido llamado *spirit* en el servidor, como se muestra en la Figura 6-3. Tenga en cuenta que Windows muestra los *hostnames* con letras mayúsculas/minúsculas (*Toltec*). La distinción entre mayúsculas y minúsculas es irrelevantes en los nombres de las máquinas (*hostname*), por lo que puede ver *toltec*, *Toltec* y *TOLTEC* como resultado de algunas órdenes o en distintas pantallas, pero todos se refieren al mismo sistema. Gracias a Samba, Windows 98 ve al servidor Unix como a un servidor SBM válido, y puede acceder al directorio *spirit* como si fuese un directorio más del sistema.

Figura 6-3. Recursos compartidos por *toltec* vistos desde *maya*



Una característica interesante de Windows es la capacidad de mapear una letra de unidad (como E:, F: o Z:) hacia un directorio compartido usando la opción “Conectar a Unidad de Red” (*Map Network Drive*) desde el explorador de Windows [4]. Una vez hecho esto, las aplicaciones podrán acceder a la carpeta compartida utilizando la letra de la unidad de disco asignada. Se pueden almacenar datos en ella, instalar y ejecutar programas desde ella e incluso protegerla con una contraseña para evitar accesos no deseados. La Figura 6-4 muestra un ejemplo de mapeado de un directorio compartido hacia una letra de una unidad.

Figura 6-4. Mapeo de una unidad de red en una letra de unidad Windows

Eche un vistazo a la línea que aparece al lado de la ruta (*Path*) en la imagen Figura 6-4. Una forma equivalente de representar un directorio en una máquina de la red es utilizando dos barras invertidas (\\), seguidas del nombre de la máquina de red, otra barra invertida (\), y el directorio de red de la máquina, como se muestra en el Ejemplo 6-1:

Ejemplo 6-1. Representación de un directorio en una máquina de red

```
\\maquina-de-red\directorio
```

Esto se conoce como notación UNC (*Universal Naming Convention*) en el mundo Windows. Por ejemplo, la caja de diálogo de la Figura 6-4 representa el directorio de red del servidor *toltec* como en el Ejemplo 6-2:

Ejemplo 6-2. Notación UNC (*Universal Naming Convention*)

```
\\toltec\spirit
```

Si esto le resulta familiar, probablemente esté pensando en *uniform resource locator* (URL), que es la notación que utilizan los navegadores web como Mozilla (http://www.mozilla.org/) o Konqueror (http://konqueror.kde.org/) para acceder a las máquinas a través de Internet. Asegúrese de no confundir ambas notaciones, las URLs utilizan barras inclinadas hacia la derecha en vez de barras invertidas, y están precedidas por el nombre del protocolo de transferencia de datos (por ejemplo: ftp, http) y dos puntos (:). En realidad, URL y UNC son dos cosas completamente distintas, aunque algunas veces se

pueda especificar un recurso SBM haciendo uso de la notación URL en vez de la notación UNC. Para especificar la siguiente dirección, *\\toltec\spirit*, en notación URL, se ha de escribir: *smb://toltec/spirit*.

Una vez que la unidad de red está configurada, Windows y sus programas la verán como una unidad de disco más. Si tiene alguna aplicación multiusuario, puede instalarla sobre una unidad de red[5]. La Figura 6-5 muestra la unidad de red resultante, como si fuese una unidad más en el cliente Windows 98. Advierta la tubería de enlace en el icono de la unidad "J:"; esto indica que es una unidad de red, en lugar de una unidad física.

Figura 6-5. Un directorio de red mapeado como la unidad J en el cliente

Dependiendo del sistema operativo Widows que utilice (Windows Me, Windows 2000 o Windows XP), el entorno de red funcionará de una forma distinta. Es necesario pulsar sobre algunos iconos más, pero se puede ver el servidor *toltec* como se muestra en la Figura 6-6. Esta captura está realizada desde un sistema Windows 2000. Haciendo uso de la opción "Conectar a unidad de red" (*Map Network Drive*), obtendríamos el mismo resultado en otras versiones de Windows.

Figura 6-6. Recursos compartidos en *toltec* (vistos desde *aztec*)

Compartiendo una impresora

Probablemente se haya fijado en la impresora *lp* que aparece en la lista de recursos de *toltec* en la Figura 6-3. Esto indica que el servidor Unix posee una impresora que puede ser compartida con los clientes SBM del grupo de trabajo. Los datos enviados a la impresora desde cualquier cliente será colocado en la cola de impresión del servidor Unix, para seguidamente ser impresos en el orden de llegada.

Configurar una impresora para que sea accesible a través de Samba a los clientes Windows es, si cabe más sencillo que configurar una unidad de disco. Haciendo doble *click* sobre la impresora e identificando el fabricante y modelo de la misma, puede instalar el controlador para esa impresora en el cliente Windows. Desde ese momento, Windows podrá formatear cualquier información enviada a la impresora de red y acceder a ella como si fuese una impresora local. En Windows 98, al hacer doble *click* sobre el icono de impresoras que aparece en el *Panel de Control*, abre la ventana de impresoras que se muestra en la Figura 6-7. Una vez más, note la tubería colocada bajo la impresora, lo que indica que se trata de una impresora en red.

Figura 6-7. Impresora en red disponible en *toltec*

Viendo las cosas desde Unix

Como se mencionó anteriormente, Samba no es más que un conjunto de demonios. Puede verlos haciendo uso de la orden **ps**; puede ver cualquier mensaje que generen a través de archivos de depuración personalizados o a través del syslog (dependiendo de como se haya configurado Samba); y puede configurarlos desde un único archivo de configuración: `smb.conf`. A parte de esto, si quiere saber que están haciendo los demonios en un determinado momento, Samba posee un programa denominado **smbstatus** que muestra la información requerida. El Ejemplo 6-3 muestra su salida:

Ejemplo 6-3. Muestra de la salida de la orden smbstatus

```
# /usr/bin/smbstatus
Processing section "[homes]"
Processing section "[printers]"
Processing section "[spirit]"

Samba version 2.2.6
Service      uid    gid    pid     machine
----------------------------------------
spirit       jay    jay    7735    maya     (172.16.1.6) Sun Aug 12 12:17:14 2002
spirit       jay    jay    7779    aztec    (172.16.1.2) Sun Aug 12 12:49:11 2002
jay          jay    jay    7735    maya     (172.16.1.6) Sun Aug 12 12:56:19 2002

Locked files:
Pid    DenyMode   R/W        Oplock     Name
--------------------------------------------------
7735   DENY_WRITE RDONLY     NONE       /u/RegClean.exe   Sun Aug 12 13:01:22 2002

Share mode memory usage (bytes):
```

```
1048368(99%) free + 136(0%) used + 72(0%) overhead = 1048576(100%) total
```

El informe de estado de Samba proporciona tres grupos de datos, cada uno de ellos dividido en secciones separadas. La primera sección identifica los sistemas que han conectado con el servidor Samba, identificando a cada cliente por su nombre de máquina (*maza* y *aztec*) y su dirección IP. La segunda sección informa del nombre y estado de los ficheros compartidos por el servidor que están actualmente en uso, incluyendo el estado de lectura/escritura o cualquier bloqueo que estos posean. Finalmente, Samba informa sobre la memoria en uso por los recursos que administra, incluyendo la cantidad de memoria que se está utilizando por los recursos compartidos más el gasto fijo de memoria. (Tenga en cuenta que esta no es la misma cantidad de memoria que el total de memoria utilizada por los procesos **smbd** y **nmbd**.)

Familiarizándose con una red SMB

Ahora que ya posee una breve visión sobre Samba, tómese algún tiempo para familiarizarse con el entorno que ha adoptado Samba: una red SBM. Trabajar con redes SBM es significativamente diferente a trabajar con protocolos comunes de TCP/IP, como FTP o SSH, debido a que hay bastantes conceptos nuevos que aprender y mucha información a cubrir. Primero, se discutirán los conceptos básicos existentes tras una red SBM, seguido de algunas implementaciones de Microsoft sobre SBM, para finalmente mostrar donde puede encajar un servidor Samba y dónde no.

Comprendiendo NetBIOS

Para comenzar, echemos la vista atrás. En 1984, IBM diseñó una API (*Application Programming Interface*) simple para conectar en red sus ordenadores, llamada *Network Basic Input/Output System* (NetBIOS). La API NetBIOS proporcionaba un diseño rudimentario para que una aplicación se conectase y compartiese datos con otros ordenadores.

Es útil pensar en la API NetBIOS como una extensión de red para las llamadas de la API BIOS estándar. La BIOS contiene código de bajo nivel para realizar operaciones en el sistema de archivos de un ordenador local. Originalmente, NetBIOS tenía que intercambiar instrucciones con los ordenadores a través de redes *IBM PC* o *Token Ring*. Esto exigió un protocolo de transporte de bajo nivel para transportar las peticiones de un ordenador al siguiente.

A finales de 1985, IBM liberó dicho protocolo, combinándolo con la API NetBIOS para convertirse en *NetBIOS Extended User Interface* (NetBEUI). NetBEUI fue diseñado para pequeñas redes de área local (LANs), permitiendo a cada ordenador usar un nombre (de hasta 15 caracteres) que no estuviese siendo utilizado en la red. Se entiende por una “LAN pequeña”, una red de menos de 255 nodos -¡Esto se consideraba un número generoso en 1985!-.

El protocolo NetBEUI se volvió muy popular en las aplicaciones de red, incluyendo aquellas que corrían bajo *Windows for Workgroups*. Más tarde, aparecieron implementaciones de NetBIOS sobre los protocolos IPX de Novell, los cuales competían con NetBEUI. Sin embargo, los protocolos de red escogidos por la floreciente comunidad de Internet fueron TCP/IP y UDP/IP, así como las implementaciones de las APIs NetBIOS sobre dichos protocolos, que pronto se convirtieron en una necesidad.

Recuerde que TCP/IP hace uso de números para representar las direcciones de los ordenadores (192.168.220.100, por ejemplo), mientras que NetBIOS usa sólo nombres. Este fue el mayor problema encontrado a la hora de juntar los dos protocolos. En 1987, el grupo IETF (*Internet Engineering Task Force*) publicó una serie de documentos de estandarización, titulados RFC 1001 y 1002, que perfilaban cómo NetBIOS podría trabajar sobre una red TCP/UDP. Este conjunto de documentos todavía lidera las implementaciones que existen hoy en día, incluyendo aquellas proporcionadas por Microsoft para sus sistemas operativos Windows, así como a la suite Samba.

Desde entonces, el estándar que estos documentos lideran se ha convertido en NetBIOS sobre TCP/IP, o NBT[6] para abreviar.

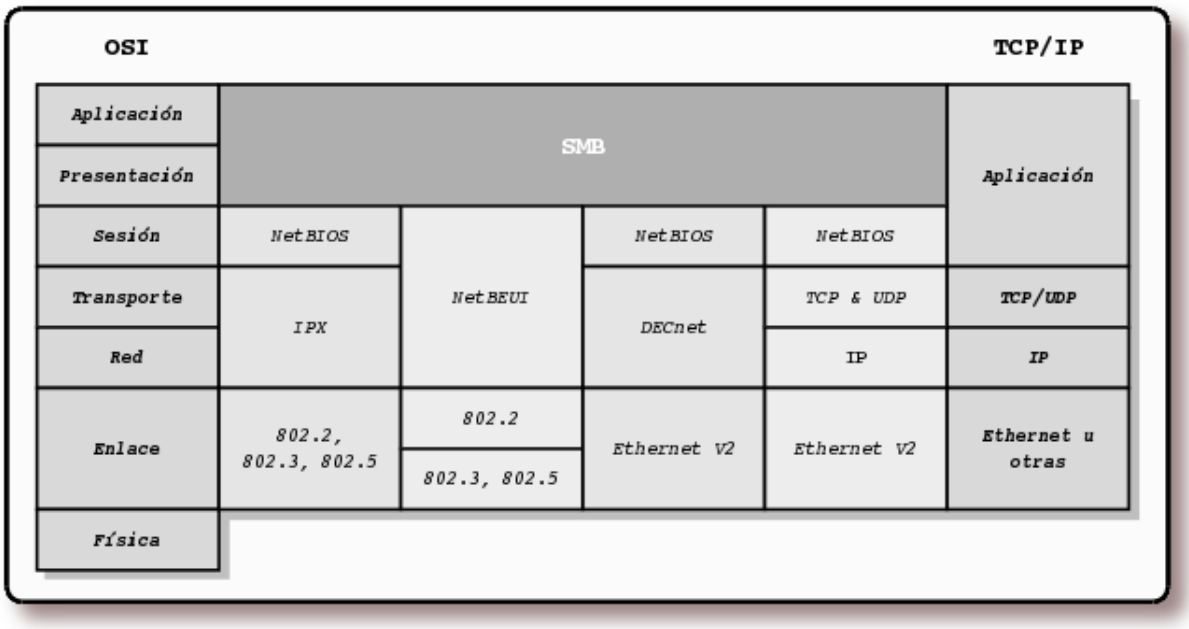
El estándar NBT (RFC 1001/1002) actualmente establece un trio de servicios sobre una red:

- Un Servicio de Nombres
- Dos Servicios de Comunicación:
  - Datagramas
  - Sesiones

El servicio de nombres resuelve el problema del paso de un nombre a una dirección anteriormente comentado; permite a cada ordenador proclamar un nombre específico en la red que puede se puede convertir en una dirección IP legible, como hacen hoy en día los DNS en Internet. Los servicios de datagramas y sesiones son protocolos secundarios de comunicación, usados para transmitir datos desde y hacia máquinas NetBIOS a través de la red.

Como se ha visto hasta este momento, SMB puede correr sobre múltiples protocolos. El siguiente diagrama muestra este hecho[7]:

Figura 6-8. Protocolos sobre los que corre SMB[8]



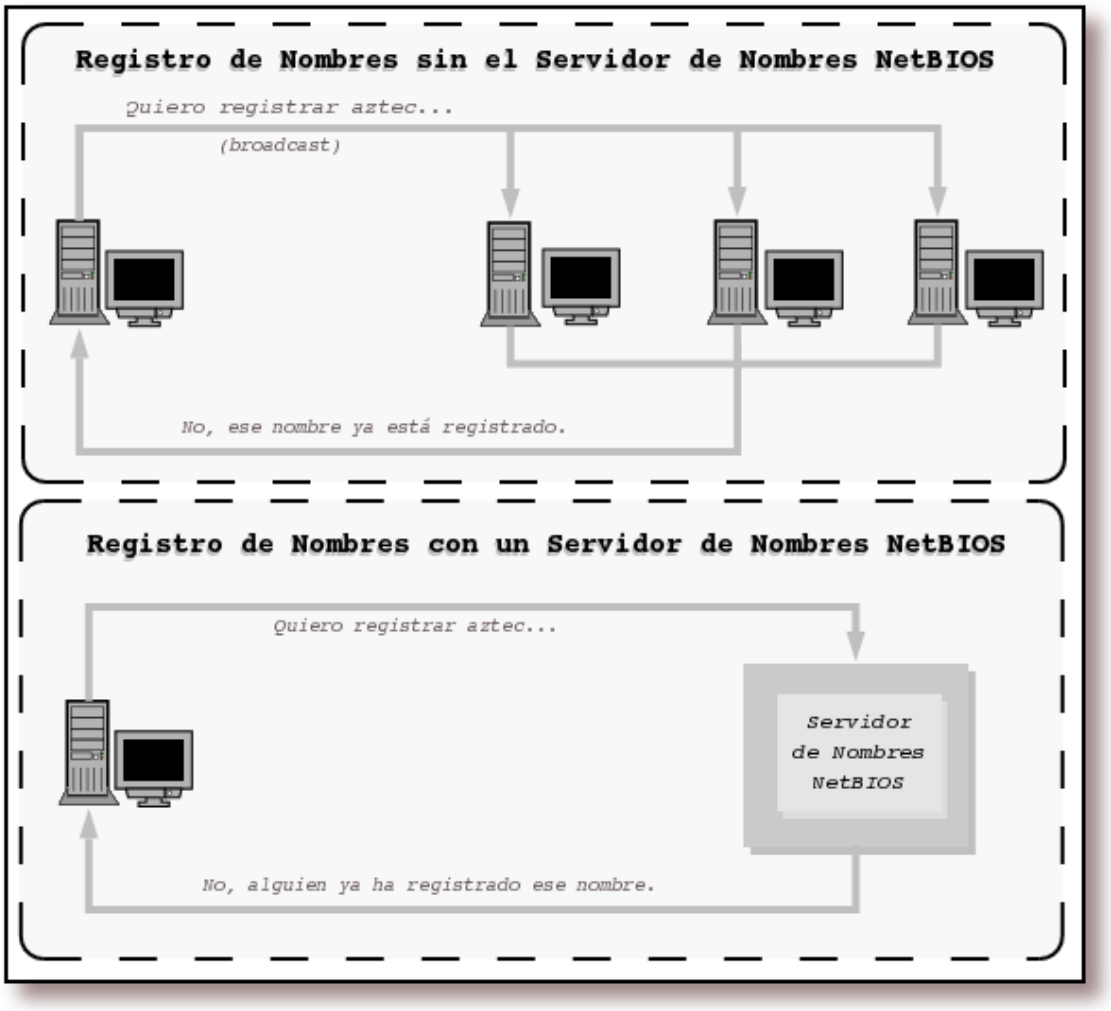
Obteniendo un nombre

En el mundo NetBIOS, cuando cada ordenador se activa, quiere reclamar un nombre para sí; esto se denomina registro de nombre. Sin embargo, dos máquinas en el mismo grupo de trabajo no podrían solicitar el mismo nombre; ya que esto confundiría a una máquina que quisiese comunicarse con cualquiera de esas dos. Existen dos métodos diferentes para asegurarse de que esto no ocurrirá:

- Hacer uso de NBNS para controlar el registro de nombres NetBIOS por parte de las máquinas
- Permitir la defensa de su nombre a cada máquina de la red, en el caso de que otra máquina intente usarlo

La Figura 6-9 ilustra un registro de nombre (fallido), con y sin NBNS.

Figura 6-9. Registro de nombres Broadcast versus NBNS[9]

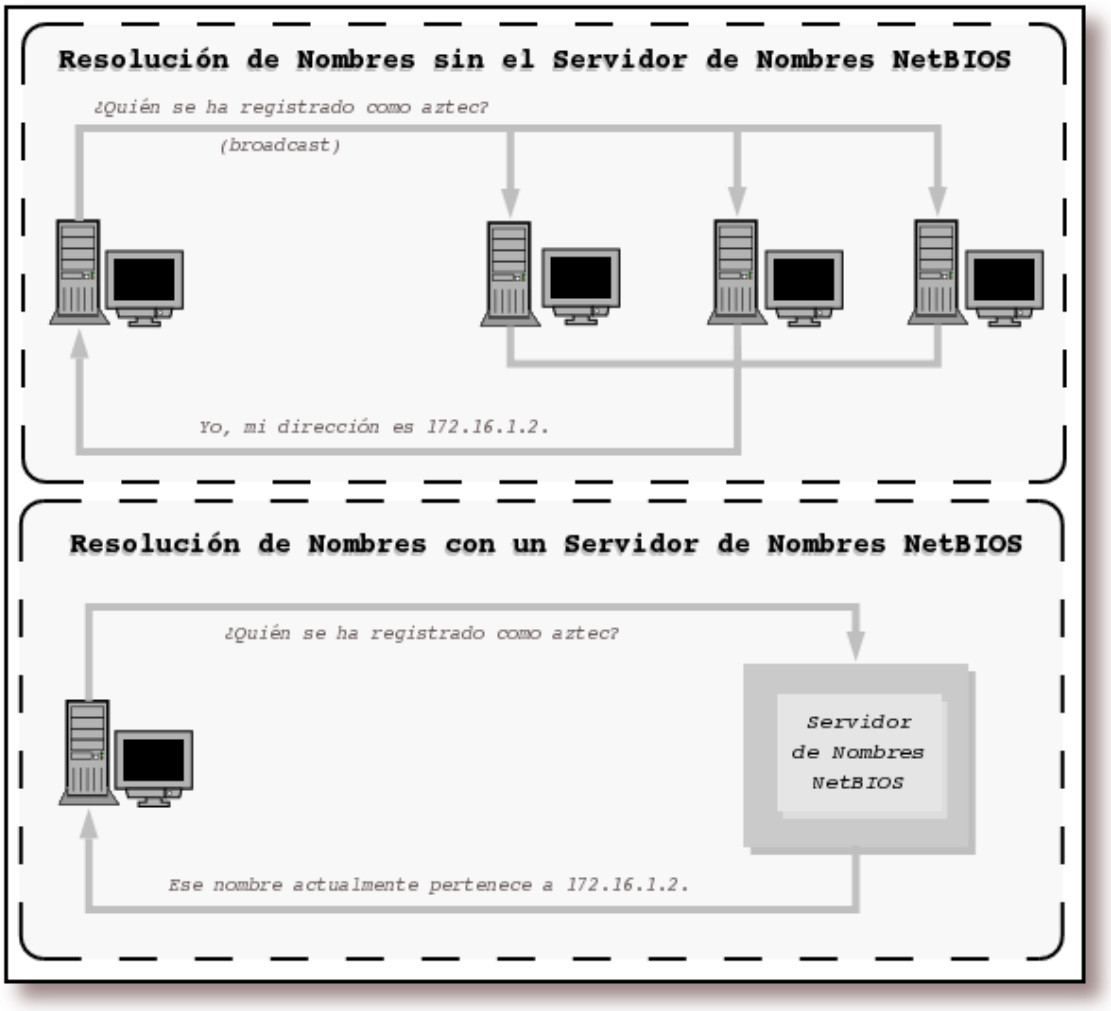


Como se mencionó anteriormente, debería existir alguna forma de resolver nombres NetBIOS a la dirección IP correspondiente; a esto se le conoce como *resolución de nombres*. Existen dos estrategias diferentes con NBT aquí también:

- Que cada ordenador comunique su dirección IP cuando “escuche” una petición broadcast para su nombre NetBIOS
- Usar el NBNS para ayudar a resolver los nombres NetBIOS a direcciones IP

La Figura 6-10 ilustra los dos tipos de resolución de nombres.

Figura 6-10. Resolución de nombres Broadcast versus NBNS[10]



Como se podría esperar, tener un NBNS en su red puede ayudar enormemente. Para ver exactamente por qué, eche un vistazo al método broadcast.

Aquí, cuando un cliente arranca, envía un mensaje broadcast manifestando su deseo de registrar un nombre NetBIOS específico para el. Si nadie pone objeción al uso del nombre, el obtiene el nombre. Por otro lado, si otra máquina en la subred local está actualmente usando ese nombre, enviará un mensaje de respuesta al cliente solicitante indicando que ese nombre ya está siendo usado. Esto es conocido como *defender el nombre del host*. Este tipo de sistema es útil cuando un cliente se ha caído inesperadamente de la red -otro puede tomar su nombre-, pero se incurre en un importante aumento del tráfico de la red para algo tan simple como el registro de un nombre.

Con un NBNS, ocurre lo mismo, pero con la diferencia de que la comunicación está confinada a la máquina solicitante y al servidor de nombres NBNS. No se produce un broadcast cuando una máquina desea registrar su nombre; el mensaje de registro es simplemente enviado desde el cliente hacia el servidor NBNS, y el servidor NBNS responde si el nombre está o no libre. A esto se le denomina como

comunicación punto-a-punto, y es beneficioso en redes con más de una subred. Esto se debe a que los routers suelen estar preconfigurados para bloquear los paquetes broadcast entrantes.

Los mismos principios se aplican a la resolución de nombres. Sin un servidor NBNS, la resolución de nombres NetBIOS se podría realizar mediante broadcast. Todos los paquetes se enviarían a cada ordenador de la red, con la esperanza de que el ordenador afectado por la petición responda directamente a la máquina solicitante. El uso de un servidor NBNS y la comunicación punto-a-punto para este propósito carga mucho menos la red que inundar la red con peticiones broadcast para cada petición de resolución de nombres que se produzca.

Se puede discutir que los paquetes broadcast no causan problemas significativos en las redes modernas y de gran ancho de banda compuestas por máquinas con CPUs muy rápidas, si sólo un grupo reducido de ordenadores están presentes en la red, o la demanda de ancho de banda es pequeña. Hay muchos casos en los que la anterior suposición es cierta; sin embargo, se aconseja no confiar en el broadcast tanto como se pueda. Esta es una regla a seguir en redes grandes y saturadas, y si se sigue este consejo a la hora de configurar redes pequeñas, estas podrán crecer sin problemas en el futuro.

Tipos de nodos

¿Cómo informo a los clientes sobre la estrategia a seguir para realizar el registro y la resolución de nombres? Cada máquina en una red NBT gana una de las siguientes designaciones, dependiendo de cómo se maneje el registro y la resolución de nombres: b-node, p-node, m-node y h-node. El comportamiento de cada tipo de nodo se resumen en la Tabla 6-1.

Tabla 6-1. Tipos de nodo NetBIOS

Rol	Valor
b-node	Hace uso de registro y resolución broadcast únicamente
p-node	Hace uso de registro y resolución punto-a-punto únicamente
m-node (mixto)	Hace uso de broadcast para el registro. Si lo consigue, notifica al servidor NBNS el resultado. Hace uso de broadcast para la resolución; utiliza NBNS si el broadcast no ha tenido éxito
h-node (híbrido)	Hace uso del servidor NBNS para el registro y la resolución; utiliza broadcast si el servidor NBNS no responde o no está operativo

Los clientes Windows suelen encontrarse como *h-nodes* o nodos híbridos. Los tres primeros tipos de nodos aparecen el los RFCs 1001/1002, y los *h-nodes* fueron inventados más tarde por Microsoft, como un método más tolerable a fallos.

Puede encontrar el tipo de nodo de un ordenador Windows 95/98/Me ejecutando la orden **winipcfg** y pulsando sobre el botón de *Más información*. En Windows NT/2000/XP, puede hacer uso de la orden **ipconfig /all** en el prompt de una ventana de comandos. En cualquier caso, busque la línea que diga *Node Type*.

¿Qué hay en un nombre?

Los nombres utilizados en NetBIOS son ligeramente diferentes de los nombres empleados en los DNS, con los que estará familiarizado. En primer lugar, los nombres NetBIOS existen en un espacio de nombres único. En otras palabras, no existen niveles jerárquicos como en samba.org (dos niveles) o en ftp.samba.org (tres niveles). Los nombres NetBIOS están formados por una única cadena como *toltec* o *maya*, cada uno de ellos pertenecientes a un grupo de trabajo o un dominio. En segundo lugar, los nombres NetBIOS sólo pueden contener 15 caracteres y están compuestos únicamente por los caracteres alfanuméricos estándar (a-z, A-Z, 0-9) y los siguientes:

```
!  @  #  $  %  ^  &  (  )  -  ’  {  }  .  ~
```

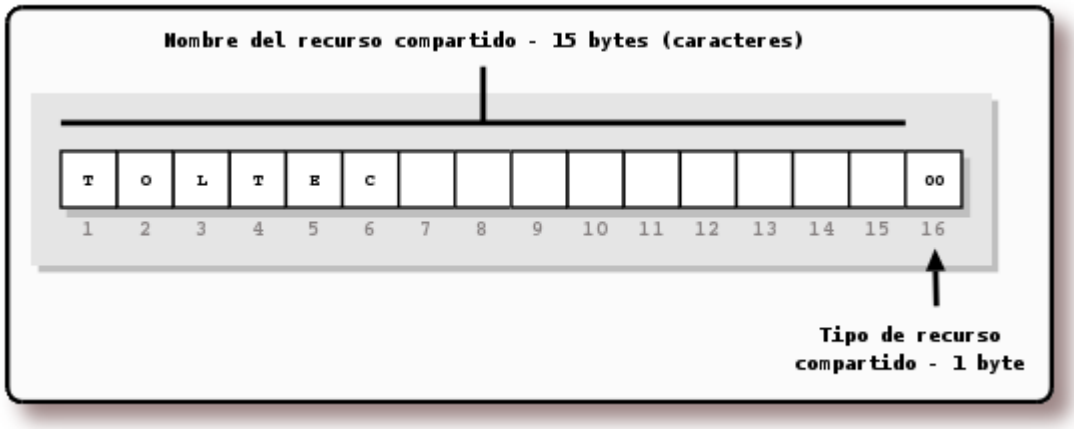
Aunque se puede hacer uso del punto (.) en un nombre NetBIOS, no es recomendable, debido a que esos nombres puede que no funcionen en futuras versiones de NBT.

No es una coincidencia que todos los nombres DNS válidos también sean válidos en NetBIOS. De hecho, el nombre DNS para un servidor Samba es frecuentemente usado como su nombre NetBIOS. Por ejemplo, si tiene un sistema con el siguiente nombre: *toltec.ora.com*, su nombre NetBIOS podría ser TOLTEC (seguido de 9 espacios en blanco).

Nombres de recursos y tipos

Con NetBIOS, un ordenador no sólo anuncia su presencia, sino que también comunica a las otras máquinas que tipo de servicios ofrece. Por ejemplo, *toltec* puede indicar que no es únicamente una estación de trabajo, sino que también es un servidor de ficheros y puede recibir mensajes Windows Messenger. Esto se consigue añadiendo el byte décimosexto al final del nombre de la máquina (recurso), denominado tipo de recurso, y registrando el nombre más de una vez, una vez por cada servicio que ofrece. Observe la Figura 6-11.

Figura 6-11. Estructura de nombres NetBIOS[11]



El tipo de recurso de 1 byte indica el único servicio que el ordenador ofrece. La notación empleada a partir de este momento para mostrar el tipo de servicio ofrecido por un determinado ordenador estará

enmarcada entre los símbolos de mayor y menor que (<>) después del nombre NetBIOS, como se muestra en el Ejemplo 6-4:

Ejemplo 6-4. Notación empleada para mostrar el tipo de servicio NetBIOS ofrecido por un ordenador

```
TOLTEC<00>
```

Puede saber qué nombres están registrados para una máquina NBT determinada usando la orden de Windows **nbtstat**. Debido a que estos servicios son únicos (no puede haber más de uno registrado), aparecerán listados como tipo ÚNICO (UNIQUE) en la salida. Por ejemplo, el Ejemplo 6-5 describe al servidor *toltec*:

Ejemplo 6-5. Ejecución de la orden nbtstat

```
D:\> nbtstat -a toltec
       NetBIOS Remote Machine Name Table
   Name               Type         Status
---------------------------------------------
TOLTEC          <00>  UNIQUE      Registered
TOLTEC          <03>  UNIQUE      Registered
TOLTEC          <20>  UNIQUE      Registered
...
```

Esto indica que el servidor ha registrado el nombre NetBIOS *toltec* como nombre de máquina, como un receptor de mensajes desde el servicio Messenger de Windows y como un servidor de archivos. Algunos de los posibles atributos que un nombre puede tener se listan en la Tabla 6-2.

Tabla 6-2. Tipos de recursos únicos NetBIOS

Nombre del Recurso	Valor en hexadecimal del byte
Standard Workstation Service	00
Messenger Service	03
RAS Server Service	06
Domain Master Browser Service (associated with primary domain controller)	1B
Master Browser name	1D
NetDDE Service	1F
Fileserver (including printer server)	20
RAS Client Service	21
Network Monitor Agent	BE
Network Monitor Utility	BF

Nombres de grupos y tipos

SMB también usa el concepto de grupos, con los cuales los ordenadores se pueden registras ellos

mismos. Anteriormente se mencionó que los ordenadores del ejemplo pertenecían a un grupo de trabajo, el cual es una partición de ordenadores en la misma red. Por ejemplo, una empresa podría tener fácilmente un grupo de trabajo ADMINISTRACIÓN y otro VENTAS, cada uno con diferentes servidores e impresoras. En el mundo Windows, un grupo de trabajo y un grupo SMB son la misma cosa.

Continuando con el ejemplo sobre **nbtstat**, el servidor Samba *toltec* es también un miembro del grupo de trabajo *METRAN* (el atributo GROUP hex 00), y participará en la elección del buscador (browser) maestro (atributo GROUP 1E). Observe el Ejemplo 6-6>:

Ejemplo 6-6. Muestra de los grupos a los que pertenece un servidor con nbtstat

```
       NetBIOS Remote Machine Name Table
   Name               Type         Status
---------------------------------------------
METRAN          <00>   GROUP       Registered
METRAN          <1E>   GROUP       Registered
..__MSBROWSE__.<01>   GROUP       Registered
```

Los posibles atributos de grupo que puede tener una máquina se ilustran en la Tabla 6-3. Existe más información disponible en el libro “Windows NT in a Nutshell” de Eric Pearce, publicado por O’Reilly.

Tabla 6-3. Tipos de Recursos de Grupo NetBIOS

Nombre del Recurso	Valor en hexadecimal del byte
Standard Workstation group	00
Logon server	1C
Master Browser name	1D
Normal Group name (used in browser elections)	1E
Internet Group name (administrative)	20
<01><02>_ _MSBROWSE_ _<02>	01

La entrada final, _ _ MSBROWSE _ _, es utilizada para anunciar un grupo a otros buscadores maestros. Los caracteres no imprimibles en el nombre se muestran como guiones bajos en una salida de **nbtstat**. No se preocupe si no comprende todos los recursos o tipos de grupos. Algunos de ellos no los necesitará con Samba, y sobre los otros se verá más en el resto del capítulo. Lo importante aquí es recordar la lógica del mecanismo de nombres.

Scope ID

En los años oscuros del funcionamiento en red de SMB, antes de la introducción de los grupos NetBIOS, se debía utilizar una estrategia muy primitiva para aislar grupos de ordenadores del resto de la red. Cada paquete SMB contenía un campo denominado *scope ID*, la idea era que los sistemas de la red se pudiesen configurar de forma que sólo aceptasen los paquetes con el *scope ID* que coincidiese con su configuración. Esta característica fue apenas utilizada y desgraciadamente aun pervive en las implementaciones modernas. Algunas de las utilidades incluidas en la distribución de Samba permite establecer el *scope ID*. El establecimiento del *scope ID* en una red es sinónimo de problemas, sólo se ha

mencionado para evitar confusiones cuando aparezca el término más adelante.

Datagramas y sesiones

En este punto, se hará un paréntesis para abordar la responsabilidad de NBT: proporcionar servicios de conexión entre dos máquinas NetBIOS. NBT ofrece dos servicios: el servicio de sesión y el servicio de datagramas. Comprender cómo funcionan estos servicios no es vital para usar Samba, pero le dará una idea sobre cómo trabaja NBT y cómo arreglar problemas cuando Samba no funcione.

El servicio de datagramas no proporciona una conexión estable entre ordenadores. Los paquetes de datos se envían o difunden (broadcast) de una máquina a otra, sin tener en cuenta el orden en que estos llegan al destino, o incluso si han llegado todos. El uso de datagramas requiere menos procesamiento que las sesiones, aunque la confiabilidad de la conexión puede sufrir. Los datagramas, por tanto, son empleados para enviar rápidamente bloques no vitales de datos a una o más máquinas. El servicio de datagramas se comunica usando las primitivas que se muestran en la Tabla 6-4.

Tabla 6-4. Primitivas de datagrama

Primitiva	Descripción
Send Datagram	Envía un paquete datagrama a un ordenador o grupo de ordenadores
Send Broadcast Datagram	Difunde (broadcast) datagramas a cualquier ordenador, esperando por un *Receive Broadcast datagram* (datagrama de acuse de recibo)
Receive Datagram	Recibe un datagrama desde un ordenador
Receive Broadcast Datagram	Espera por un datagrama de difusión (broadcast)

El servicio de sesiones es más complejo. Las sesiones son un método de comunicación que, en teoría, ofrece la capacidad de detectar conexiones problemáticas o inoperativas entre dos aplicaciones NetBIOS. Esto lleva a pensar en una sesión NBT en términos de una llamada telefónica, analogía que obviamente influyó en el diseño del estándar CIFS.

Una vez que se establece la conexión, permanece abierta durante toda la *conversación*, cada lado conoce quien es el ordenador emisor y receptor, y cada uno se puede comunicar haciendo uso de las primitivas mostradas en la Tabla 6-5.

Tabla 6-5. Primitivas de sesión

Primitiva	Descripción
Call	Inicia una sesión con un ordenador que está escuchando bajo un nombre determinado
Listen	Espera por una llamada desde un emisor conocido o cualquier emisor
Hang-up	Finaliza una conversación
Send	Envía datos al otro ordenador
Receive	Recibe datos del otro ordenador

Primitiva	Descripción
Session Status	Obtiene información de las sesiones solicitadas

Las sesiones son el *backbone* de la compartición de recursos en una red NBT. Se utilizan normalmente para establecer conexiones estables desde los clientes a unidades de disco o impresoras compartidas en un servidor. El cliente "llama" al servidor y comienza a negociar la información, como los archivos que desea abrir, los datos que desea intercambiar, etc. Estas llamadas pueden durar mucho tiempo -horas, incluso días- y todo esto ocurre dentro del contexto de una única conexión. Si se produce un error, el software de sesión (TCP) retransmitirá los datos hasta que se reciban correctamente, a diferencia del método "envía-y-reza" del servicio de datagramas (UDP).

En realidad, mientras que las sesiones se supone que están para manejar comunicaciones problemáticas, algunas veces no lo hacen. Si la conexión es interrumpida, la información de sesión que está abierta entre dos ordenadores puede volverse inválida. Si esto ocurre, la única forma de restablecer la sesión entre los dos ordenadores es llamar de nuevo y comenzar desde cero.

Si desea más información sobre estos servicios, eche un vistazo al RFC 1001. Sin embargo, hay dos cosas importantes a recordar aquí:

- Las sesiones siempre ocurren entre dos máquinas NetBIOS. Si una sesión se interrumpe, se supone que el cliente ha almacenado suficiente información de estado para restablecerla. Sin embargo, en la práctica, normalmente esto no ocurre.
- Los datagramas pueden ser difundidos (broadcast) hacia múltiples ordenadores, pero no son confiables. En otras palabras, no hay manera de que el emisor sepa si los datagramas que ha enviado han llegado correctamente a sus destinos.

Grupos de trabajo y dominios Windows

Hasta ahora se ha cubierto la tecnología básica SMB, que sería todo lo que necesitaría saber si su red estuviese compuesta únicamente de clientes MS-DOS. Se asumirá que posee clientes Windows, especialmente las versiones más recientes, por lo que en las siguientes secciones se describirán las mejoras que Microsoft ha introducido en en las redes SMB -denominadas: *Windows para grupos de trabajo* y *Dominios Windows*.

Grupos de trabajo Windows

Los grupos de trabajo de Windows son muy similares a los grupos SMB ya descritos. Pero necesita saber algunas cosas adicionales.

Navegando

La navegación es el proceso de buscar otros ordenadores o recursos compartidos en la red Windows. Tenga en cuenta que no tiene ningún parecido con un navegador web, a parte de la idea general de

"descubrir que hay". Por otro lado, navegar por la red de Windows es parecido a hacerlo por la web, en el sentido de que todo lo que existe pude cambiar sin previo aviso.

Antes de la existencia del navegador, los usuarios debían conocer el nombre del ordenador al que se querían conectar, luego tenían que teclear manualmente una dirección UNC en el gestor de archivos o la aplicación implicada para poder acceder al recurso. La dirección UNC era algo parecido a lo que se muestra en el Ejemplo 6-7:

Ejemplo 6-7. Notación UNC

```
\\toltec\spirit\
```

La navegación es mucho más conveniente, ya que permite examinar los contenidos de la red haciendo uso de una interfaz "apunta-y-pulsa" del entorno de red de los clientes Windows.

Encontrará dos tipos de navegación en una red SMB:

- Navegar por una lista de ordenadores y sus recursos compartidos
- Navegar por los recursos compartidos de un determinado ordenador

A continuación se profundizará un poco en el primer tipo. En cada LAN (o subred) con un grupo de trabajo o dominio Windows, un ordenador tiene la responsabilidad de mantener la lista de ordenadores que están en un momento dado accesibles a través de la red. Este ordenador se denomina buscador (browser) maestro local, y la lista que mantiene se denomina lista de búsqueda. Los ordenadores de una red utilizan la lista de búsqueda para minimizar el tráfico de datos necesario para realizar una búsqueda. En vez de que cada ordenador pregunte por la lista de ordenadores actualmente disponibles, estos pueden preguntar al buscador maestro local para obtener una lista completa y actualizada.

Para navegar por los recursos de un determinado ordenador, el usuario debe conectar a dicho ordenador; esta información no se puede obtener de la lista de búsqueda. La navegación por la lista de recursos compartidos de un ordenador se realiza haciendo doble *click* sobre el icono del ordenador que se presenta en el entorno de red. Como se veía al principio del capítulo, el ordenador responderá con una lista de los recursos que están accesibles una vez que el usuario se haya autentificado.

Cada servidor en un grupo de trabajo Windows necesita anunciar su presencia al brower maestro local, una vez que ha registrado su nombre NetBIOS, y (teóricamente) anuncia que va a dejar el grupo de trabajo cuando es desconectado. Es responsabilidad del buscador maestro local almacenar los servidores que se han anunciado.

Aviso

El entorno de red de Windows puede comportarse de manera extraña: hasta que se selecciona un ordenador, el entorno de red de Windows puede contener información no actualizada. Esto significa que el entorno de red de Windows puede mostrar ordenadores que se han caído o no informar de aquellos ordenadores que todavía no se han anunciado. Resumiendo, una vez seleccionado un servidor y realizada la conexión con el, puede estar seguro de que los recursos compartidos así como las impresoras existen realmente en la red.

A parte de los roles vistos con anterioridad, casi cualquier sistema Windows (incluyendo Windows para grupos de trabajo y Windows 95/98/Me o Windows NT/2000/XP) puede actuar como un buscador maestro local. Un buscador maestro local puede tener uno o más buscadores de respaldo en la subred local, que tomarán el relevo al buscador maestro local en el caso de que este falle o se vuelva inaccesible. Para asegurar operaciones fluidas, los buscadores de respaldo actualizarán frecuentemente su lista con la del buscador maestro local.

A continuación se muestra como calcular el número mínimo de buscadores de respaldo que se pueden asignar en un grupo de trabajo:

- Si la red está formada por hasta 32 máquinas Windows NT/2000/XP, o hasta 16 máquinas Windows 95/98/Me, el buscador maestro local asigna un buscador de respaldo a mayores del buscador maestro local
- Si el número de máquinas Windows NT/2000/XP está comprendido entre 33 y 64, o el número de máquinas Windows 95/98/Me está comprendido entre 17 y 32, el buscador maestro local asigna dos buscadores de respaldo
- Para cada grupo de 32 máquinas Windows NT/2000/XP o 16 ordenadores Windows 95/98/Me además de esto, el buscador maestro local asigna otro buscador de respaldo

No existe límite en cuanto al número máximo de buscadores de respaldo que pueden ser asignados por un buscador maestro local.

Elecciones para la navegación

La navegación es un aspecto crítico en cualquier grupo de trabajo Windows. Sin embargo, no todo funciona correctamente en todas las redes. Sirva el siguiente ejemplo para ilustrar este hecho: imagínese un ordenador con Windows ubicado en el despacho de un CEO de una pequeña compañía actúa como buscador maestro local -esto quiere decir, que será un buscador maestro local hasta que el CEO lo desconecte para recibir su masaje-. En este momento, la máquina Windows NT ubicada en la sección de piezas de recambio de un departamento está dispuesta a tomar el control del trabajo. Sin embargo, dicho ordenador está ejecutando un programa extremadamente grande y mal escrito que está consumiendo los recursos del procesador. La moraleja: los navegadores han de ser muy tolerantes con las idas y venidas de los servidores. Debido a que casi cualquier sistema Windows puede servir como buscador, ha de haber alguna forma de decidir en cualquier momento quien toma el trabajo. El proceso de decisión se denomina *elección*.

Casi cualquier sistema Windows tiene un algoritmo de elección, de forma que los sistemas se puedan poner de acuerdo en quien será el buscador maestro local y quien el buscador de respaldo local. Una elección puede ser forzada en cualquier momento. Por ejemplo, imagine que el CEO ha finalizado su masaje y reinicia el servidor. Como el servidor vuelve a estar disponible, anuncia su presencia, y tendrá lugar una elección para ver si el PC ubicado en la sección de piezas de recambio todavía continua siendo el buscador maestro local.

Cuando se ejecuta una elección, cada ordenador difunde información sobre sí mismo haciendo uso de datagramas. Esta información incluye:

- La versión del protocolo de elección utilizado
- El sistema operativo del ordenador

- La cantidad de tiempo que el ordenador ha estado conectado a la red
- El *hostname* del cliente

Estos valores determinan que sistema operativo tiene la veteranía y pueda cumplir con el rol de buscador maestro local[12]. La estructura desarrollada para lograr esto no es elegante y tiene problemas de seguridad implícitos. Mientras que un dominio de búsqueda puede ser integrado con un dominio de seguridad, el algoritmo de elección no tiene en cuenta que ordenadores van a ser buscadores. Esto es posible para cualquier ordenador que ejecute un servicio de búsqueda y se haya registrado como participante en la elección del buscador, una vez ha ganado es capaz de cambiar la lista de búsqueda. No obstante, la navegación es una característica llave en el funcionamiento de la red de Windows, y las características de compatibilidad hacia atrás garantizarán que seguirá en uso durante los años venideros.

Autentificación de Windows 95/98/Me

Existen tres tipos de claves cuando un sistema Windows 95/98/Me está interactuando en un grupo de trabajo Windows:

- Una clave de Windows
- Una clave de red Windows
- Una clave para cada uno de los recursos compartidos a los que se le ha asignado protección con contraseña

Las claves de Windows funcionan de tal forma que son la fuente de confusión para los administradores de sistemas Unix. No hay manera de prevenir el uso de los ordenadores por parte de usuarios sin autorización. (Si no se lo cree, pulse sobre el botón *Cancelar* del cuadro de diálogo de autentificación y compruebe lo que ocurre). En lugar de eso, la clave de Windows se utiliza para poder acceder a los archivos y recursos compartidos disponibles en la red de Windows que están protegidos con clave. Existe un archivo por cada usuario registrado en el sistema, este se puede encontrar en el directorio `C:\Windows` y su nombre será el de la cuenta del usuario, seguido por la extensión *.pwl*. Por ejemplo, si la cuenta de usuario es *sara*, el archivo será `C:\Windows\sara.pwl`. Este archivo está cifrado con la clave de Windows como llave de cifrado.

> **Sugerencia:** Como medida de seguridad, debería comprobar la existencia de archivos *.pwl* en los clientes Windows 95/98/Me, ya que pueden haber sido creados debido a los intentos de acceso fallidos por parte de los usuarios. Un archivo *.pwl* se puede romper con facilidad y puede contener claves válidas de cuentas Samba o recursos compartidos.

La primera vez que se accede a la red, Windows intenta utilizar la clave de Windows como clave de red. Si hay éxito, no se le preguntará al usuario por una clave de acceso a la red, de esta forma, los siguientes ingresos en el sistema Windows ingresarán automáticamente a su vez en la red de Windows, haciendo las cosas más sencillas al usuario.

Los recursos compartidos en un grupo de trabajo pueden tener asignados a su vez claves que limitan el acceso a los mismos. La primera vez que un usuario intenta acceder a este tipo de recursos, se le solicitará una clave, pudiendo seleccionar una opción en el cuadro de diálogo de autentificación para añadir la clave a su lista de claves. Esta opción está marcada por defecto; si se acepta, Windows

almacenará la clave en el fichero *.pwl* del usuario, siendo manejadas automáticamente por Windows ulteriores autentificaciones para dicho recurso.

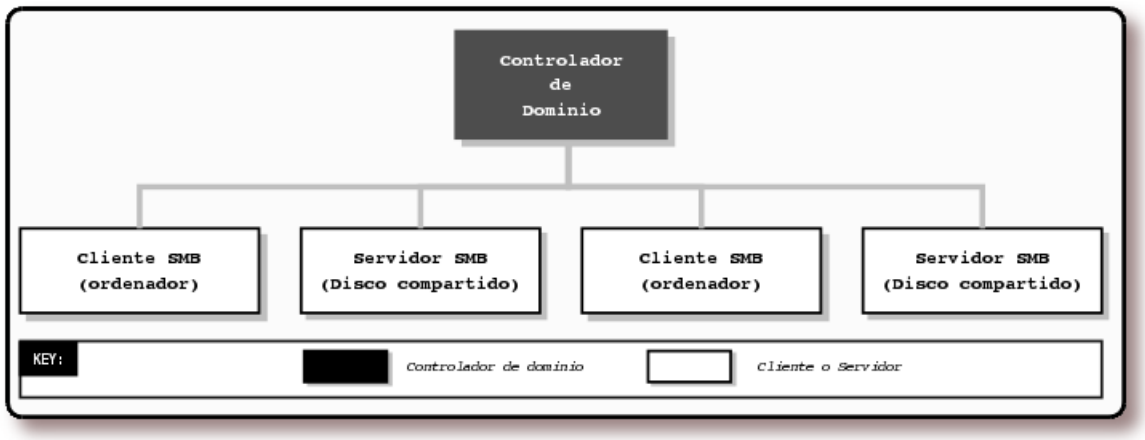
La estrategia de Samba para la autentificación en los grupos de trabajo es un poco diferente, y ha sido el resultado de mezclar el modelo de grupos de trabajo de Windows con el modelo Unix, donde se ejecuta Samba[13].

Dominios de Windows NT

El modelo de red punto-a-punto de los grupos de trabajo Windows funciona bastante bien siempre y cuando el número de ordenadores de la red sea pequeño y haya una comunidad de usuarios muy restringida. Sin embargo, en grandes redes la simplicidad de los grupos de trabajo llega a ser un factor limitador. Los grupos de trabajo ofrecen sólo el nivel más básico de seguridad, y debido a que cada recurso compartido puede tener su propia clave, es un inconveniente (por decir lo mínimo) para los usuarios tener que recordar la clave de cada recurso en una red de gran envergadura. Incluso si esto no fuese un problema, mucha gente encuentra frustrante tener que interrumpir su proceso de trabajo para teclear la clave del recurso compartido en el cuadro de diálogo cada vez que se accede a otro recurso de red.

Para soportar las necesidades de las grandes redes, tales como las que se encuentran en los departamentos computacionales, Microsoft introdujo los dominios con la versión 3.51 de Windows NT. Un dominio Windows NT es en esencia un grupo de trabajo de un ordenador SMB que tiene una característica añadida: el servidor que actúa como controlador de dominio (vea la Figura 6-12).

Figura 6-12. Un simple dominio Windows[14]



Controladores de dominio

Un controlador de dominio en un dominio Windows NT funciona de manera muy similar a un servidor NIS en una red Unix, manteniendo una base de datos del dominio que contiene la información de los usuarios y grupos, así como sus servicios asociados. Las responsabilidades de un controlador de dominio

están principalmente centradas en la seguridad, incluyendo la autentificación o la tarea de permitir o denegar el acceso a los recursos del dominio a un determinado usuario. Esto se realiza normalmente gracias al uso de un nombre de usuario y una clave. El servicio que mantiene la base de datos en los controladores de dominio se denomina *Security Account Manager* (SAM).

El modelo de seguridad de Windows NT gira en torno a los identificadores de seguridad (SIDs) y las listas de control de acceso (ACLs). Los identificadores de seguridad son utilizados para representar objetos en un dominio, que incluyen (pero no limitan) a los usuarios, los grupos, los ordenadores y los procesos. Los SIDs se escriben normalmente en un formulario ASCII como campos separados por guiones, tal y como se muestra en el Ejemplo 6-8:

Ejemplo 6-8. Muestra de un SID (*Security IDentifier*)

```
S-1-5-21-1638239387-7675610646-9254035128-545
```

Un SID comienza con el carácter “S”, seguido de un guión. El número inmediatamente posterior al primer guión se denomina *identificador relativo* (RID) y es un número único dentro del dominio que identifica a un usuario, un grupo, un ordenador o cualquier otro objeto. El número RID es análogo al *user ID* (UID) o al *group ID* (GID) en un sistema Unix o dentro de un dominio NIS.

Las ACLs proveen la misma funcionalidad que los permisos de los archivos “rwx” comunes en los sistemas Unix. Sin embargo, las ACLs son más versátiles. Los permisos de los archivos Unix sólo pueden establecer permisos para el propietario y el grupo al que el fichero pertenece, y “otros”, significa que cualquier otro usuario. Las ACLs de Windows NT/2000/XP permiten establecer permisos individuales para cualquier número arbitrario de usuarios y/o grupos. Las ACLs están constituidas por una o más entradas de control de acceso (ACE - Access Control Entries), cada una de las cuales contienen un SID y derechos de acceso asociados a este.

El soporte de ACLs ha sido incluido como una característica estándar en algunas variantes de Unix y están disponibles como añadidos para otras. Samba soporta el mapeo de las ACLs entre Windows y Unix[15].

Controladores de dominio primarios y secundarios

Ya se ha hablado sobre buscadores maestros y de respaldo. Los controladores de dominio se parecen a estos en que un dominio tiene un controlador primario (PDC) y puede tener uno o más controladores secundarios de dominio (BDCs). Si un PDC falla o no está accesible, sus tareas son automáticamente traspasadas a uno de los BDCs. Los BDCs sincronizan frecuentemente sus datos SAM con el PDC, por lo que si surge la necesidad cualquiera de ellos puede desempeñar inmediatamente los servicios del controlador primario, sin ningún tipo de impacto para los clientes. Sin embargo, tenga en cuenta que los BDCs tienen copias de solo lectura de la base de datos SAM; estos sólo pueden actualizar sus datos mediante la sincronización con un PDC. Un servidor en un dominio Windows puede hacer uso de la SAM de cualquier PDC o BDC para autentificar a un usuario que intente acceder a sus recursos e ingresar en el dominio.

Todas las versiones recientes de Windows pueden ingresar en un dominio como clientes para tener acceso a los recursos de los servidores de dominio. Los sistemas que son considerados miembros del dominio son una clase más exclusiva, compuesta de un PDC y uno o varios BDCs, así como los servidores miembros del dominio, que no son más que sistemas que se han unido como miembros al

domino, y son conocidos por los controladores de dominio debido a la cuenta existente para ellos en la base de datos SAM.

Autentificación

Cuando un usuario teclea su usuario y clave para ingresar en un dominio Windows, se invoca un *desafío* de seguridad y un protocolo de respuesta entre el ordenador cliente y el controlador de dominio para verificar que el usuario y la clave son válidos. Seguidamente el controlador de dominio envía el SID de nuevo al cliente, quien lo utilizará para crear un SAT (*Security Access Token*) que es válido únicamente para este sistema, que será utilizado para autentificaciones ulteriores. Esta señal de acceso contiene la información sobre el usuario codificada en su interior, la cual incluye el nombre de usuario, el grupo y los permisos que el usuario posee en el dominio. En este momento, el usuario está autentificado en el dominio.

Posteriormente, cuando el cliente intenta acceder a un recurso compartido dentro del dominio, el sistema cliente entra en un *desafío* de seguridad y un intercambio de respuestas con el servidor del recurso. Seguidamente el servidor entra en otro *desafío* de seguridad y conversación de respuesta con el controlador de dominio, para comprobar que el cliente es válido. (Lo que ocurre realmente es que el servidor utiliza la información que ha obtenido del cliente para hacerse pasar por este y autentificarse el mismo ante el controlador de dominio. Si el controlador de dominio valida sus credenciales, envía un SID al servidor, que utilizará para crear su propio SAT para el cliente, de esta forma habilita el acceso a sus recursos locales en beneficio del cliente.) En este punto, el cliente se encuentra autentificado para los recursos del servidor y se le permite acceder a ellos. El servidor utiliza el SID almacenado en el SAT para determinar que permisos de modificación y uso posee el cliente para el recurso en cuestión, esto lo consigue comparándolo con las entradas de las ACLs del recurso.

Aunque este método de autentificación pueda parecer demasiado complicado, permite a los clientes la autentificación sin enviar las claves en texto plano a través de la red, y es mucho más difícil de romper que la endeble seguridad que proporcionan los grupos de trabajo descritos anteriormente.

Servicio de nombres con WINS y DNS

El servicio de nombres de Internet de Windows (WINS) es una implementación de Microsoft del servidor de nombres NetBIOS (NBNS). Como tal, WINS hereda muchas de las características de NetBIOS. En primer lugar, WINS sólo puede tener nombres nombres simples o llanos para las máquinas, tales como *inca*, *mixtec* o navaho, y grupos de trabajo como PERU, MEXICO o USA. Otra característica es que WINS es dinámico: cuando un un cliente se conecta inicialmente a la red, este solicita un nombre, una dirección y un grupo de trabajo al servidor WINS local. Este servidor WINS almacenará la información mientras el cliente refresque periódicamente su registro WINS, lo que indicará que todavía está conectado a la red. Advierta que los servidores WINS no son específicos de un grupo de trabajo o un dominio; pueden contener información sobre múltiples dominios y/o grupos de trabajo, y pueden estar presentes en más de una subred.

Se pueden configurar múltiples servidores WINS para que se sincronicen unos con otros. Esto permite que las entradas de los ordenadores que aparecen y desaparecen de la red se propagarse de un servidor WINS a otro. Aunque que en teoría esto parece eficiente, podría volverse rápidamente problemático si hay varios servidores WINS en la red. Debido a que los servicios WINS pueden atravesar múltiples subredes (puede especificar la dirección del servidor WINS en cada uno de los clientes u obtenerla vía

DHCP), normalmente es más eficiente tener a cada cliente Windows, no importa cuántos dominios Windows haya, apuntando a un mismo servidor WINS. De esa forma, sólo habrá un servidor WINS dominante con la información correcta, en lugar de tener varios servidores WINS esforzándose por mantenerse sincronizados con los cambios más recientes.

El servidor WINS activo en un determinado momento es conocido como el servidor WINS primario. También puede instalar un servidor WINS secundario, el cual entrará en acción en el caso de que el primario falle o se vuelva inaccesible. Tanto el servidor primario como cualquier otro servidor WINS sincronizarán sus bases de datos de direcciones periódicamente.

En la familia de sistemas operativos Windows, sólo la edición de servidor Windows NT/2000 puede actuar como servidor WINS. Samba 2.2 puede funcionar como servidor WINS primario, pero no puede actualizar su base de datos con otros servidores WINS. Por este motivo, no puede actuar como servidor secundario WINS o como un servidor primario WINS de un servidor secundario WINS Windows.

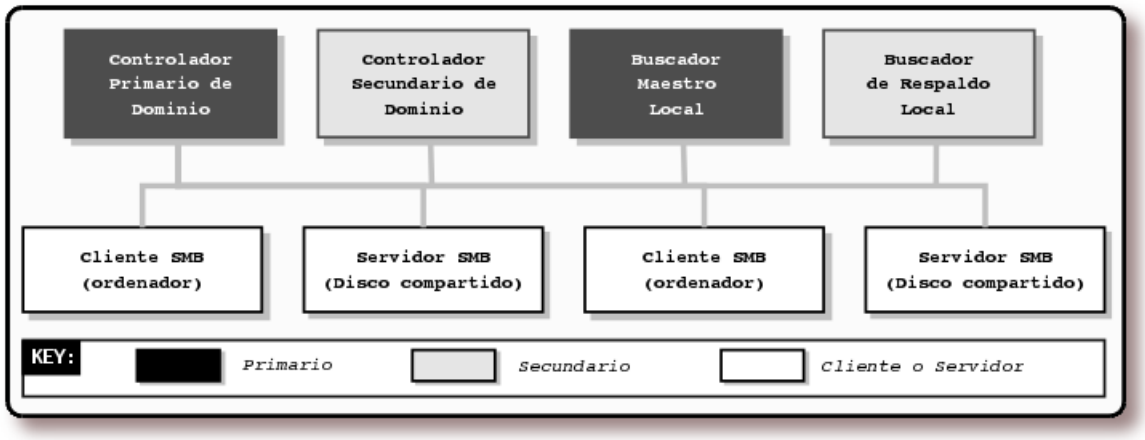
WINS maneja el servicio de nombres por defecto, aunque Microsoft añadió el DNS con Windows NT Server 4. Este es compatible con los DNSs que son estándar en virtualmente todos los sistemas Unix, y un servidor Unix (como el host Samba) puede ser utilizado para actuar de DNS.

Relaciones de confianza

Un aspecto adicional de los dominios Windows NT, que todavía no está soportado en Samba 2.2, es la posibilidad de configurar una relación de confianza entre dominios, permitiendo a los clientes de un dominio acceder a los recursos de otro sin necesidad de cualquier tipo de autentificación. El protocolo que está detrás de esto se denomina *pass-through authentication*, mediante el cual las credenciales de un usuario son pasadas de un cliente, en el primer dominio, a un servidor en el segundo dominio, quien consultará al controlador de dominio del primer dominio (de confianza) para comprobar que el usuario es válido antes de permitir el acceso a los recursos.

Ha de notar que en muchos aspectos, el comportamiento de un Windows para grupos de trabajo y un Windows NT concuerdan. Por ejemplo, el buscador maestro y de respaldo en un dominio son siempre el PDC y BDC, respectivamente. A continuación se actualizará el diagrama de dominios Windows para incluir tanto al buscador maestro local como el de respaldo. El resultado se muestra en la Figura 6-13.

Figura 6-13. Un dominio Windows con un buscador maestro local y uno de respaldo[16]



El parecido entre los grupos de trabajo y los dominios NT no es accidental, ya que el concepto de dominio Windows no se desarrolló hasta la versión 3.5 de Windows NT, y los dominios Windows se vieron forzados a mantener la compatibilidad hacia atrás con los grupos de trabajo presentes en Windows para grupos de trabajo.

Samba puede actuar como un controlador primario de dominio para clientes Windows 95/98/Me y Windows NT/2000/XP, con la única limitación de que sólo puede actuar de PDC, no de BDC.

Samba también puede funcionar como un servidor miembro de dominio, esto significa que tendrá una cuenta de equipo en la base de datos del PDC y por tanto será reconocido como parte del dominio. Un servidor miembro del dominio no puede autentificar a los usuarios que ingresan en el dominio, pero puede manejar funciones de seguridad (como los permisos de los archivos) para los usuarios del dominio que acceden a sus recursos.

Dominios de *Active Directory*

Dando comienzo con Windows 2000, Microsoft introdujo el *Active Directory* (Directorio Activo), el siguiente camino más allá de los dominios de Windows NT. No se va a entrar en mucho detalle con *Active Directory*, ya que es un tema extremadamente amplio. Samba 2.2 no soporta ninguna característica de *Active Directory*, y el soporte de la versión 3.0 de Samba se limita a actuar como un cliente. Desde ahora, sea consciente de que con *Active Directory*, el modelo de autentificación está centrado al rededor de LDAP, y el servicio de nombres lo suministra un DNS en lugar de un servidor WINS. Los dominios en *Active Directory* se pueden organizar en una estructura jerárquica en árbol, en la cual, cada controlador de dominio es fijo, no hay distinción entre controlador primario y secundario, como en los dominios Windows NT.

Los sistemas Windows 2000/XP pueden configurar un simple grupo de trabajo o un dominio de clientes Windows NT (que funcionaría con Samba). La edición *Server* de Windows 2000 puede configurarse para que ejecute *Active Directory* y dominios Windows NT para mantener la compatibilidad hacia atrás (modo mixto). En este caso, Samba 2.2 trabaja con los servidores Windows 2000 de la misma forma que lo hacía con los servidores Windows NT 4.0. Cuando se configura para que opere en modo nativo, los

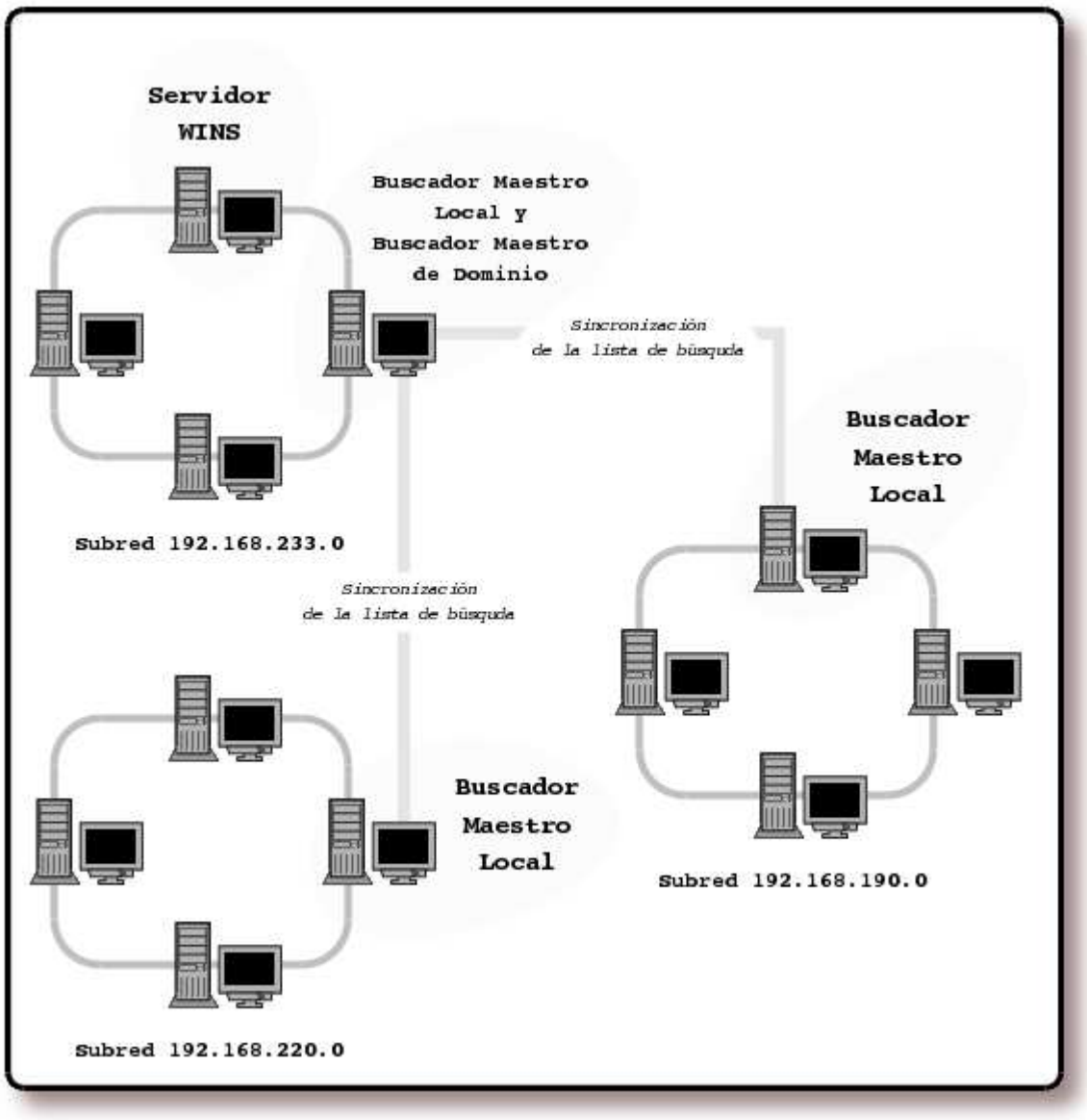
servidores Windows 2000 sólo soportan *Active Directory*. Incluso así, Samba 2.2 puede operar como un servidor en un dominio albergado por un servidor Windows 2000 en modo nativo, haciendo uso del modo emulación PDC de un servidor Windows 2000. Sin embargo, no es posible para Samba 2.2 o 3.0 operar como un controlador de dominio en un un dominio *Active Directory* de Windows 2000.

¿Puede un grupo de trabajo abarcar múltiples subredes?

Sí, pero la mayoría de la gente que ha hecho esto ha tenido muchos quebraderos de cabeza. Abarcar múltiples subredes no era parte del diseño inicial de Windows NT 3.5 o de Windows para grupos de trabajo. Como resultado, un dominio Windows que abarca dos o más subredes es, en realidad, un "encolado" de dos o más grupos de trabajo que comparten un nombre idéntico. La buena noticia es que todavía se puede hacer uso de un controlador primario de dominio para el control de autentificación a lo largo de cada subred. La mala noticia es que las cosas no son tan sencillas en la navegación.

Como se mencionó anteriormente, cada subred ha de tener su propio buscador maestro local. Cuando un dominio Windows abarca múltiples subredes, un administrador del sistema tendrá que asignar una de las máquinas como buscador maestro de dominio. El buscador maestro de dominio mantendrá una lista de búsqueda para todo el dominio Windows. Esta lista de búsqueda es creada por la sincronización periódica de la lista de búsqueda de cada buscador maestro local con la lista de búsqueda del buscador maestro de dominio. Después de la sincronización, el buscador maestro local y el buscador maestro de dominio deberían contener entradas idénticas. Observe la Figura 6-14 para ver un ejemplo.

Figura 6-14. Grupo de trabajo que abarca más de una subred[17]



¿Suena bien? pues no se acerca al "cielo" por las siguientes razones:

- Si existe, un PDC siempre juega el papel de buscador maestro de dominio. Debido al diseño de Microsoft, los dos siempre comparten el tipo de recurso NetBIOS <1B> y (desafortunadamente) no se pueden separar.
- En los equipos Windows 95/98/Me no pueden llegar a ser ni siquiera contactar con un buscador maestro de dominio. Esto significa que necesariamente se ha de tener, al menos, un sistema Windows NT/2000/XP (o un servidor Samba) en cada subred del grupo de trabajo multi-red

Cada buscador maestro local de cada subred continua manteniendo la lista de búsqueda para su subred, para la cual se vuelve dominante. De esta forma, si un ordenador desease ver la lista de los servidores de su propia subred, el buscador maestro local de esa subred sería interrogado. Si un ordenador quisiese ver una lista de servidores fuera de su subred, sólo podrá llegar hasta donde le lleve el buscador maestro local. Esto funciona debido a los intervalos fijados, la lista de búsqueda dominante del buscador maestro local de una subred se sincroniza con el buscador maestro de dominio, quien está sincronizado con el buscador maestro local de las otras subredes pertenecientes al dominio. Esto se denomina propagación de la lista de búsqueda.

Samba puede actuar como buscador maestro de dominio en un dominio Windows NT, o puede actuar como un buscador maestro local para una subred, sincronizando su lista de búsqueda con el buscador maestro de dominio.

Novedades de Samba 2.2

En la versión 2.2, Samba posee un soporte más avanzado para el sistema de red Windows, incluyendo la posibilidad de desempeñar las tareas más importantes necesarias para interactuar en un dominio Windows NT. A parte de esto, Samba 2.2 tiene algún soporte para las tecnologías que Microsoft introdujo en Windows 2000, aunque el grupo de desarrollo de Samba ha dejado el soporte de *Active Directory* para la versión 3.0.

Soporte PDC para clientes Windows 2000/XP

Anteriormente, Samba podía actuar como un PDC para autentificar sistemas Windows 95/98/Me y Windows NT 4. Esta funcionalidad ha sido extendida en la versión 2.2 para incluir a los sistemas Windows 2000 y Windows XP. De esta manera es posible disponer de un servidor Samba con soporte de autentificación en el dominio para los clientes Windows de la red, incluyendo las versiones más recientes. El resultado es una red más estable, de alto rendimiento y mucho más segura, con el beneficio de no tener que comprar Windows CALs a Microsoft.

Soporte Dfs de Microsoft

Microsoft Dfs permite que los recursos compartidos por un número determinado de servidores dispersos a lo largo de la red se junten y aparezcan, a los ojos de los usuarios, como si todos ellos existiesen en un sólo árbol de directorios de un servidor. Este método de organización hace la vida más fácil a los usuarios. En lugar de tener que buscar por la red, como si se tratase de un tesoro oculto, para encontrar un determinado recurso, los usuarios pueden ir directamente al servidor Dfs y coger lo que necesiten. Samba 2.2 ofrece soporte para servir Dfs, por lo que no se necesita un servidor Windows para este propósito.

Soporte de impresión en Windows NT/2000/XP

Windows NT/2000/XP poseen una interface de impresión basada en RPC diferente a la interfaz que poseen los sistemas Windows 95/98/Me. En la versión 2.2 de Samba, la interfaz de Windows

NT/2000/XP está soportada. Junto con esto, el equipo de desarrollo de Samba ha añadido soporte para bajarse automáticamente el controlador de impresión desde un servidor Samba mientras se añade una nueva impresora desde un cliente Windows.

ACLs

Samba ahora soporta ACLs en aquellos sistemas Unix que las tienen incorporadas. Esta lista incluye Solaris 2.6, 7 y 8, Irix, AIX, GNU/Linux (con cualquiera de los parches de soporte de ACLs para los sistemas de archivos ext2/ext3, disponible en http://acl.bestbits.at (http://acl.bestbits.at/) o cuando se hace uso del sistema de archivos XFS y FreeBSD (versión 5.0 y posterior). Cuando se hace uso del soporte de ACLs, Samba traduce entre las ACLs de Unix y las de Windows NT/2000/XP, haciendo al equipo que ejecuta samba parecer y actuar más parecido a un servidor Windows NT/2000/XP desde el punto de vista de los clientes Windows.

Soporte de las herramientas de administración de clientes Windows

Windows vienen con una herramienta que puede ser utilizada desde un cliente para administrar los recursos compartidos en un servidor Windows remotamente. Samba 2.2 permite a esas herramientas manejar los recursos compartidos en un servidor Samba también.

Integración con Winbind

Windbind es una ayuda que permite a los usuarios cuya información de autentificación está almacenada en una base de datos de dominio Windows, poder autentificarse en un sistema Unix. El resultado es un entorno unificado de autentificación, en el cual una cuenta de usuario se puede conservar entre un sistema Unix o un controlador de dominio Windows NT/2000/XP. Esto facilita enormemente la administración de cuentas, debido a que los administradores ya no necesitarán mantener los dos sistemas sincronizados, permitiendo a los usuarios cuyas cuentas estén asociadas a un dominio Windows, autentificarse cuando accedan a un recurso compartido por Samba.

Extensiones CIFS en Unix

Las extensiones CIFS de Unix fue desarrollado por Hewlett-Packard e introducido en la versión 2.2.4 de Samba. Estas permiten a los servidores Samba soportar los atributos de los sistemas de archivos Unix, como los enlaces y los permisos, cuando se comparten archivos con otros sistemas Unix. Esta característica permite utilizar Samba como una alternativa a NFS para la compartición de archivos entre sistemas Unix. La ventaja de utilizar Samba es que autentifica a usuarios individualmente, mientras que NFS autentifica solamente clientes (basándose en su dirección IP, que es un modelo muy pobre en cuanto a la seguridad). Esto da un empujón en el área de seguridad a Samba, a parte de su gran capacidad de configuración. Consulte el capítulo 5 de la entrada bibliográfica TsEcksteinCollier-Brown01 para ver como operar con los sistemas Unix como clientes Samba.

Y más...

Como ya viene siendo habitual, el código posee muchas mejoras que no se ven a un nivel administrativo de forma inmediata u obvia. Actualmente Samba funciona mejor en los sistemas que utilizan PAM, y existe un nuevo soporte para perfiles. El soporte de Samba para los *oplocks* ha sido reforzado, ofreciendo mejor integración con los servidores NFS (actualmente sólo en Irix y GNU/Linux) y en el sistema de archivos local, con los bloqueos SMB mapeados a bloqueos POSIX (que es dependiente la implementación de los bloqueos POSIX de cada variante Unix). Y por supuesto, también han tenido lugar las correcciones normales de *bugs*.

Novedades de Samba 3.0

La principal característica que distingue a la versión 3.0 de Samba es que incluye soporte para la autentificación mediante Kerberos 5 y LDAP, que es imprescindible para actuar como un cliente en un dominio *Active Directory*. Otra nueva característica es el soporte de Unicode, lo que simplificará mucho el soporte de lenguajes internacionales.

¿Qué puede hacer Samba?

A continuación se verá donde puede ayudar Samba y cuales son sus limitaciones. La Tabla 6-6 resume los roles que Samba puede o no puede jugar en un dominio Windows NT o *Active Directory* o en un grupo de trabajo. Muchos de los protocolos del dominio de Windows son propietarios y no han sido documentados por Microsoft, por este motivo el equipo de desarrollo de Samba ha tenido que utilizar la ingeniería inversa para poder soportarlos. En la versión 3.0, Samba no puede actuar como servidor secundario en muchos de los roles y todavía no soporta completamente *Active Directory*.

Tabla 6-6. Roles de Samba en la versión 3.0

Rol	¿Puede desempeñarlo?
Servidor de archivos	Sí
Servidor de impresión	Sí
Servidor Dfs de Microsoft	Sí
Controlador de dominio primario	Sí
Controlador de dominio secundario	No
Controlador de dominio *Active Directory*	No
Autentificación de clientes Windows 95/98/Me	Sí
Autentificación de clientes Windows NT/2000/XP	Sí
Buscador maestro local	Sí
Buscador de respaldo local	Sí
Buscador maestro de dominio	Sí
Servidor primario WINS	Sí

Rol	¿Puede desempeñarlo?
Servidor secundario WINS	No

Visión general de la distribución Samba

Como se mencionó anteriormente, actualmente Samba contiene muchos programas que prestan distintos servicios pero que tienen propósitos relacionados. A continuación se hará una breve introducción a cada uno de ellos y se describirá como trabajan en conjunción.

La mayoría de los programas que vienen con Samba se centran en sus dos demonios. Las siguientes líneas mostrarán las responsabilidades de cada demonio:

nmbd

El demonio **nmbd** es un simple servidor de nombres que suministra la funcionalidad de WINS. Este demonio espera peticiones del servidor de nombres y proporciona la dirección IP apropiada cuando se le requiere. También provee una lista de búsqueda para el entorno de red y participa en la elección de búsqueda.

smbd

El demonio **smbd** maneja los recursos compartidos entre el servidor Samba y sus clientes. Provee los servicios de servidor de archivos, impresión y búsqueda a los clientes SMB a través de una o más redes y maneja todas las notificaciones entre el servidor Samba y la red de clientes. A parte de esto, es el responsable de la autentificación de usuarios, bloqueo de recursos y compartición de datos a través del protocolo SMB.

Añadido en la versión 2.2, hay otro nuevo demonio:

winbind

Este demonio se utiliza junto con el servicio de nombres para obtener la información de los usuarios y grupos desde un servidor Windows NT y permitir a Samba autorizar a los usuarios dentro de un servidor Windows NT/2000.

La distribución de samba también viene con un conjunto de pequeñas herramientas para consola:

findsmb

Un programa que realiza búsquedas de ordenadores en la red local que respondan al protocolo SMB e imprime información sobre los mismos.

make_smbcodepage

Un programa utilizado cuando se trabaja con la característica de internacionalización de Samba para informarle sobre como convertir entre mayúsculas y minúsculas en los distintos conjuntos de caracteres.

make_unicodemap

Otro programa de internacionalización utilizado con Samba para compilar un mapa Unicode que utilizará Samba para traducir los códigos de páginas de DOS o los conjuntos de caracteres de Unix en formato Unicode de 16 bits.

net

Un nuevo programa distribuido con Samba 3.0 que puede ser utilizado para realizar una administración remota de los servidores.

nmblookup

Un programa que realiza búsquedas de nombres sobre NBT para encontrar direcciones IP de ordenadores cuando se da su nombre de máquina.

pdbedit

Nuevo programa distribuido con la versión 3.0 de Samba que ayuda en el manejo de las cuentas de usuario almacenadas en las bases de datos SAM.

rpcclient

Un programa que se puede utilizar para ejecutar las funciones MS-RPC en los clientes Windows.

smbcacls

Un programa que se utiliza para establecer o mostrar ACLs en un sistema de archivos Windows NT

smbclient

Un cliente Unix similar a un cliente ftp, que se puede utilizar para conectarse a los recursos compartidos SMB y operar con ellos. El capítulo 5 de la entrada bibliográfica TsEcksteinCollier-Brown01 discute esta orden con más detalle.

smbcontrol

Una simple utilidad de administración que envía mensajes a **nmbd** o **smbd**.

smbgroupedit

Una orden que se puede utilizar para definir mapeos entre los grupos de Windows NT y los de Unix. Esta es una funcionalidad nueva en Samba 3.0.

smbmnt

Una utilidad utilizada junto con **smbmount**.

smbmount

Un programa que monta un sistema de archivos *smbfs*, permitiendo que recursos remotos SMB sean montados en el sistema de archivos local de la máquina Samba.

smbpasswd

Un programa que permite a un administrador cambiar la clave utilizada por Samba.

smbsh

Una herramienta que funciona de manera similar a una shell, permitiendo el acceso a sistemas de archivos SMB remotos, y permite a las herramientas de Unix operar con ellos. Esta orden se describe con mayor profundidad en el capítulo 5 de la entrada bibliográfica TsEcksteinCollier-Brown01

smbspool

Un programa de cola de impresión que se utiliza para enviar archivos a impresoras remotas que están compartidas en la red SMB.

smbstatus

Un programa que reporta las conexiones de red realizadas a los recursos compartidos en el servidor Samba actualmente.

smbtar

Un programa similar a la orden **tar** de Unix, que permite archivar datos en los recursos compartidos de SMB.

smbumount

Un programa que trabaja junto con **smbmount** para desmontar los sistemas de archivos *smbfs*.

testparm

Un programa que comprueba el archivo de configuración de Samba.

testprns

Un programa que comprueba si las impresoras en la máquina Samba están reconocidas por el demonio **smbd**

wbinfo

Una utilidad utilizada para realizar peticiones al demonio **winbind**.

Cada liberación mayor de Samba se somete a un chequeo intensivo antes de anunciarla. A parte de esto, se actualiza rápidamente después de liberada si ocurren problemas o se encuentran efectos inesperados.

Información adicional sobre el proyecto

Página principal

El Proyecto Samba dispone de una página principal, http://www.samba.org/, desde donde puede obtener mucha información sobre el proyecto. De hecho, para elaborar esta sección ha utilizado la información allí disponible.

Cómo obtener Samba

Las distribuciones del código fuente y de los binarios de Samba están disponibles en muchos mirrors a lo largo de Internet. La página principal de Samba es http://www.samba.org/. Desde allí, se puede seleccionar un mirror que esté geográficamente cerca de usted.

Las distintas formas de distribución de Samba desde la página oficial se pueden ver en http://www.samba.org/download.html.

La mayoría de las distribuciones de GNU/Linux y muchos distribuidores de Unix disponen de paquetes binarios de Samba. Suele ser más conveniente hacer uso de esos paquetes antes que el código fuente o los binarios del equipo de desarrollo de Samba, ya que los distribuidores se esfuerzan en suministrar paquetes que se adapten a las especificaciones de sus productos.

Documentación

Desde la página principal del proyecto Samba se puede acceder a distintos enlaces con documentación sobre el proyecto. Hay dos grandes formas de obtener la documentación:

- en formato electrónico, para lo cual hay que acceder a: http://www.samba.org/docs/
- comprando alguno de los libros disponibles sobre el tema. Para obtener un listado de algunos de ellos, visite: http://www.samba.org/books.html

Información de soporte

La página dedicada al soporte (http://www.samba.org/support/index.html) y al contacto (http://www.samba.org/contacts.html) de Samba, informa sobre los distintos métodos existentes para obtener ayuda en un determinado momento. Los métodos más importantes para obtener ayuda son los siguientes:

Listas de correo: El proyecto Samba dispone de varias listas de correo, desde donde se puede obtener información fiable y directa. El las siguientes páginas se pueden ver las listas disponibles y la forma de inscribirse a las mismas: http://www.samba.org/archives.html y http://lists.samba.org/.

Grupos de news: Otro de los métodos disponibles para obtener ayuda, es el grupo de news comp.protocols.smb (news:comp.protocols.smb).

Canales de IRC: Samba también dispone de dos canales en el servidor de IRC http://freenode.net/. El canal dedicado al desarrollo de Samba es #samba-technical y el dedicado a las preguntas de los usuarios y la discusión en general es el #samba.

Servicio técnico de terceros: Muchas empresas ofrecen servicio técnico a la comunidad de Samba, un listado de las mismas se puede obtener desde: http://www.samba.org/support/countries.html.

Reporte de bugs

Samba dispone de un Sistema de seguimiento de tareas (https://bugzilla.samba.org), desde donde se pueden reportar errores y bugs relacionados con Samba (tanto en lo relativo al software como a la

documentación) y hacer peticiones de nuevas características.

Si se quiere reportar un error grave de seguridad, lo más conveniente es utilizar el correo: security%40samba.org (mailto:security%40samba.org).

Si lo que se quiere es remitir un parche o una mejora para Samba, se ha de enviar un correo a samba-technical@samba.org (mailto:samba-technical@samba.org) o bien visitar: http://samba.org/samba-patches/.

Más detalles de las formas de reportar errores y parches en el siguiente enlace: http://www.samba.org/bugreports.html.

Cómo contactar

Para obtener más información sobre Samba, puede contactar con el Proyecto en la siguiente dirección:

```
Samba Team
26 Carstensz st
Griffith, ACT
2603 Australia
```

Notas

1. En inglés *Windows Internet Name Service*
2. En inglés *Client Access Licenses* (CALs)
3. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/samba-configuracion-red-simple-con-servidor-samba.dia).
4. También puede hacer *click* con el botón derecho en el recurso compartido y seleccionar la entrada del menú “Conectar a Unidad de Red” (*Map Network Drive*).
5. Tenga en cuenta que muchas veces la aceptación de la licencia de usuario final prohibe instalar un programa en red, de forma que varios clientes puedan acceder a el. Compruebe el acuerdo legal que acompaña al producto para asegurarse.
6. También se puede ver la abreviación NetBT, utilizada comúnmente en la literatura de Microsoft.
7. El gráfico ha sido obtenido de la entrada bibliográfica Sharpe01.
8. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/samba-protocolos-sobre-los-que-se-ejecuta-sbm.dia) .
9. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/samba-registro-de-nombres-broadcast-vs-NBNS.dia) .
10. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/samba-resolucion-de-nombres-broadcast-vs-NBNS.dia) .
11. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/samba-estructura-de-nombres-netbios.dia).

12. El capítulo 7 de la entrada bibliográfica TsEcksteinCollier-Brown01 describe en más detalle el proceso de elección.
13. Para más detalles, vea el capítulo 9 de la entrada bibliográfica TsEcksteinCollier-Brown01
14. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/samba-un-simple-dominio-windows.dia).
15. Para más información, consulte el capítulo 8 de la entrada bibliográfica TsEcksteinCollier-Brown01
16. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/samba-dominio-windows-con-un-buscador-maestro-local-y-de-respaldo.dia).
17. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/samba-grupo-de-trabajo-que-abarca-mas-de-una-subred.dia).

Capítulo 7. Instalación

Consideraciones previas

El servidor Samba se instalará y configurará para que actúe como PDC de la red local en la que esté presente. La información de las cuentas de los usuarios se almacenará en un directorio LDAP y proveerá servicios de impresión y perfiles móviles, entre otras cosas.

En la parte dedicada a OpenLDAP,
Parte I en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*, se dejó listo el servicio de directorio para autentificar usuarios en las máquinas GNU/Linux. Lo único que falta para que esto sea posible, es introducir la estructura necesaria en la base de datos LDAP.

En este apartado no sólo veremos como realizar esto, sino que también se dará soporte, en la estructura del directorio LDAP, para almacenar los datos relativos a una cuenta de usuario Samba.

Una vez se haya incorporado esta estructura en el directorio LDAP, los usuarios que ahí se almacenen tendrán la posibilidad de autentificarse en cualquier sistema GNU/Linux y/o Windows que haga uso del servidor LDAP para la autentificación de usuarios. La particularidad es que tendrán la misma cuenta de acceso para los todos sistemas, tanto en GNU/Linux como en Windows, de toda la red.

Se ha seleccionado la versión 3.0.* de Samba, que acompaña a la versión en desarrollo de Debian GNU/Linux.

Pasos para la instalación

Se ha de diferenciar la instalación de un servidor Samba de la instalación de un cliente. En las siguientes secciones se verá como instalar uno y otro, así como los requisitos para que todo funcione correctamente.

En muchas ocasiones un mismo ordenador puede actuar como cliente y servidor Samba. En esta documentación se entenderá por servidor Samba, aquel ordenador que preste servicios (autentificación, compartición de unidades y archivos, etc.), y un cliente será aquel que los utilice (acceso a los recursos compartidos, autentificación, montaje de sistemas de archivos compartidos, etc.).

> **Nota:** En el apéndice Apéndice D se pueden ver las distintas opciones que han de seleccionar si se desea poder montar sistemas de archivos servidos por Samba.

Instalación de un servidor

El paquete principal del servidor Samba es “samba”, a continuación se muestra la información relativa al mismo:

Ejemplo 7-1. Información sobre el paquete “samba”

```
$ /usr/bin/apt-cache show samba
```

```
Package: samba
Priority: optional
Section: net
Installed-Size: 6036
Maintainer: Eloy A. Paris <peloy@debian.org>
Architecture: i386
Version: 3.0.7-1
Replaces: samba-common (<= 2.0.5a-2)
Depends: samba-common ❶ (= 3.0.7-1), netbase, logrotate,
libacl1 (>= 2.2.11-1), libc6 (>= 2.3.2.ds1-4), libcomerr2 (>= 1.33-3),
libcupsys2-gnutls10 (>= 1.1.20final-1), libkrb53 (>= 1.3.2),
libldap2 (>= 2.1.17-1), libpam0g (>= 0.76), libpopt0 (>= 1.7),
debconf (>= 0.5) | debconf-2.0, libpam-runtime (>= 0.76-13.1),
libpam-modules
Suggests: samba-doc ❷
Filename: pool/main/s/samba/samba_3.0.7-1_i386.deb
Size: 2412814
MD5sum: b60a9942c8057c2f7ef3868bc79954a0
Description: a LanManager-like file and printer server for Unix
 The Samba software suite is a collection of programs that
 implements the SMB protocol for unix systems, allowing you to serve
 files and printers to Windows, NT, OS/2 and DOS clients. This protocol
 is sometimes also referred to as the LanManager or NetBIOS protocol.
 .
 This package contains all the components necessary to turn your
 Debian GNU/Linux box into a powerful file and printer server.
 .
 Currently, the Samba Debian packages consist of the following:
 .
  samba - LanManager-like file and printer server for Unix.
  samba-common - Samba common files used by both the server and the client.
  smbclient - LanManager-like simple client for Unix.
  swat - Samba Web Administration Tool
  samba-doc - Samba documentation.
  smbfs - Mount and umount commands for the smbfs (kernels 2.2.x and above).
  libpam-smbpass - pluggable authentication module for SMB password database
  libsmbclient - Shared library that allows applications to talk to SMB servers
  libsmbclient-dev - libsmbclient shared libraries
  winbind: Service to resolve user and group information from Windows NT servers
  python2.3-samba: Python bindings that allow access to various aspects of Samba
 .
 It is possible to install a subset of these packages depending on
 your particular needs. For example, to access other SMB servers you
 should only need the smbclient and samba-common packages.
Task: file-server, print-server
```

❶ Una de las dependencias del paquete “samba” es “samba-common”

❷ El paquete “samba” sugiere la instalación de la documentación asociada al mismo. Aun siendo recomendable instalar dicha documentación, será tarea del administrador la elección de su instalación.

Ejemplo 7-2. Información sobre el paquete “samba-common”

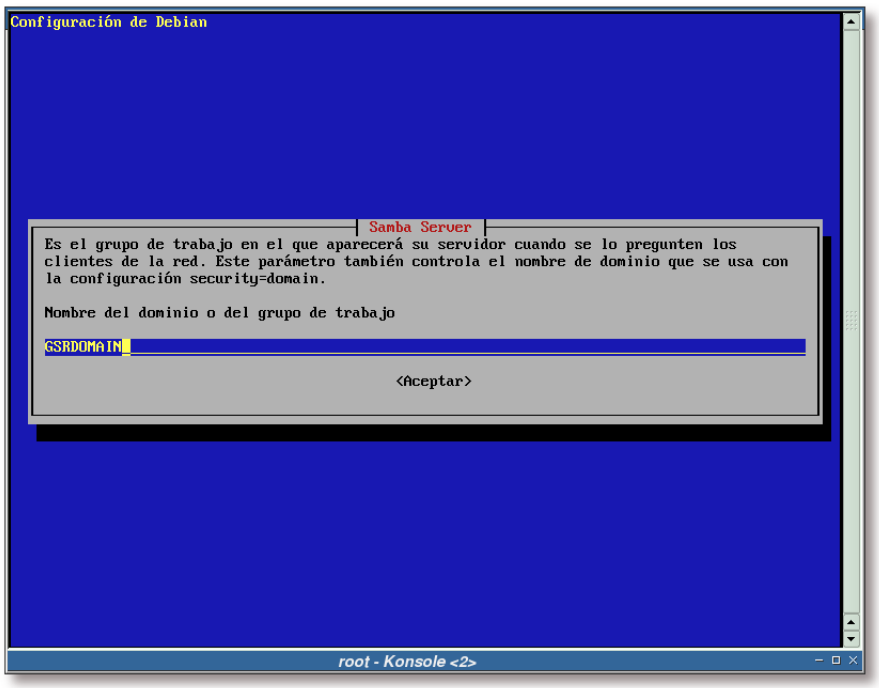
```
$ /usr/bin/apt-cache show samba-common
Package: samba-common
Priority: optional
Section: net
Installed-Size: 4456
Maintainer: Eloy A. Paris <peloy@debian.org>
Architecture: i386
Source: samba
Version: 3.0.7-1
Replaces: samba (<< 2.999+3.0.alpha21-4)
Depends: debconf, libpam-modules, libc6 (>= 2.3.2.ds1-4),
libcomerr2 (>= 1.33-3), libkrb53 (>= 1.3.2), libldap2 (>= 2.1.17-1),
libpopt0 (>= 1.7)
Filename: pool/main/s/samba/samba-common_3.0.7-1_i386.deb
Size: 1904980
MD5sum: 46ffe1e90eaf4dea5337ea7d87ea7732
Description: Samba common files used by both the server and the client
 The Samba software suite is a collection of programs that
 implements the SMB protocol for unix systems, allowing you to serve
 files and printers to Windows, NT, OS/2 and DOS clients. This protocol
 is sometimes also referred to as the LanManager or NetBIOS protocol.
 .
 This package contains the common files that are used by both the server
 (provided in the samba package) and the client (provided in the smbclient
 package).
```

Una vez obtenida la información sobre los paquetes que se van a instalar, se procede con la instalación de Samba:

Ejemplo 7-3. Instalación de “samba” (primera parte)

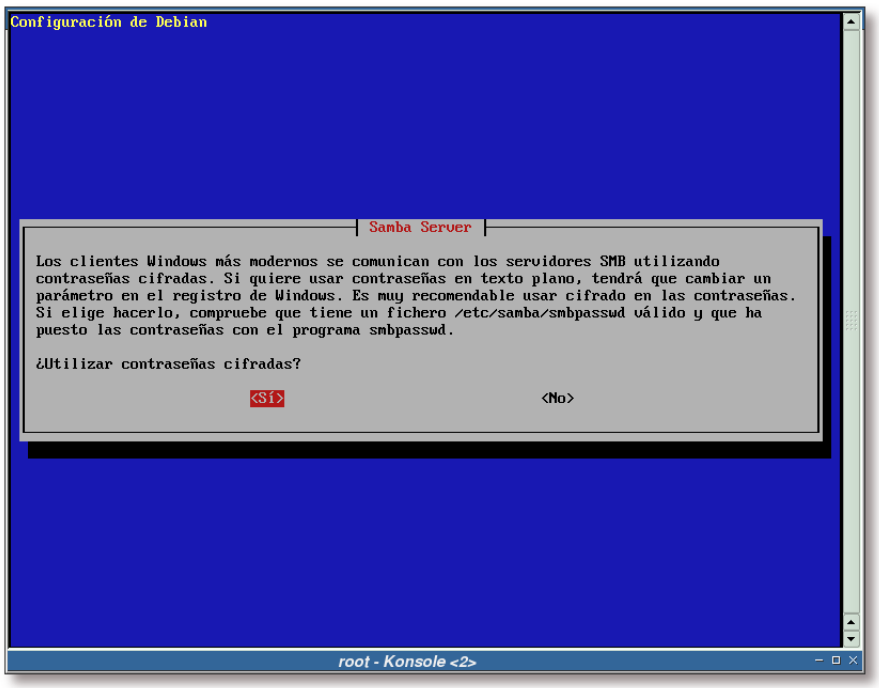
```
# /usr/bin/apt-get install samba
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  samba-common
Paquetes sugeridos:
  samba-doc
Se instalarán los siguientes paquetes NUEVOS:
  samba samba-common
0 actualizados, 2 se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 0B/4318kB de archivos.
Se utilizarán 10,7MB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n] S
Preconfiguring packages ...
```

Figura 7-1. Configuración del grupo de trabajo/dominio de samba mediante debconf



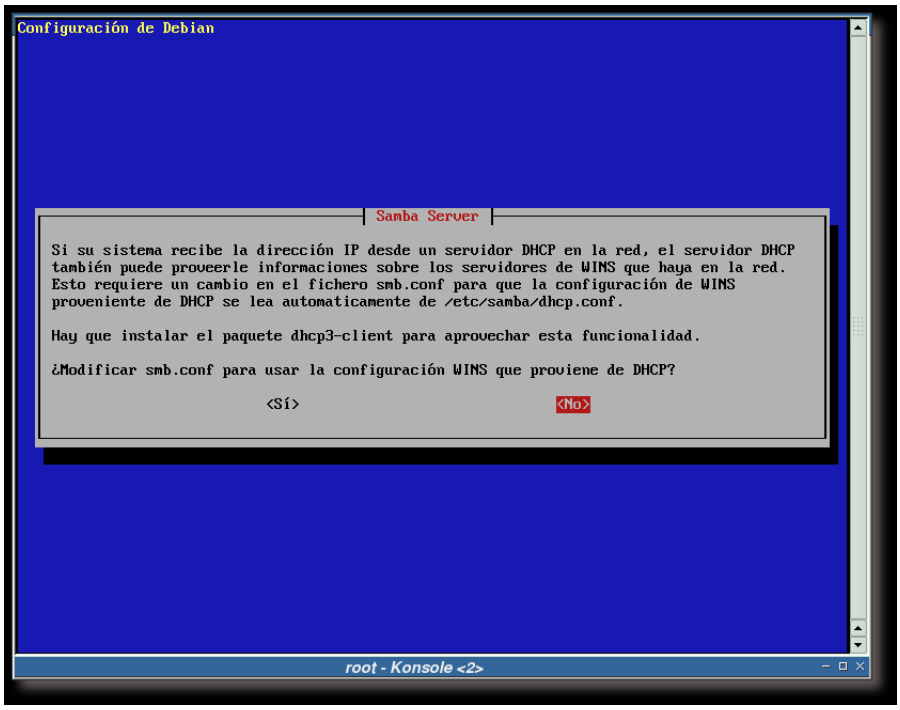
Elección del grupo de trabajo/dominio que servirá el servidor Samba sujeto a la instalación. En este caso “GSRDOMAIN”.

Figura 7-2. ¿Contraseñas cifradas?



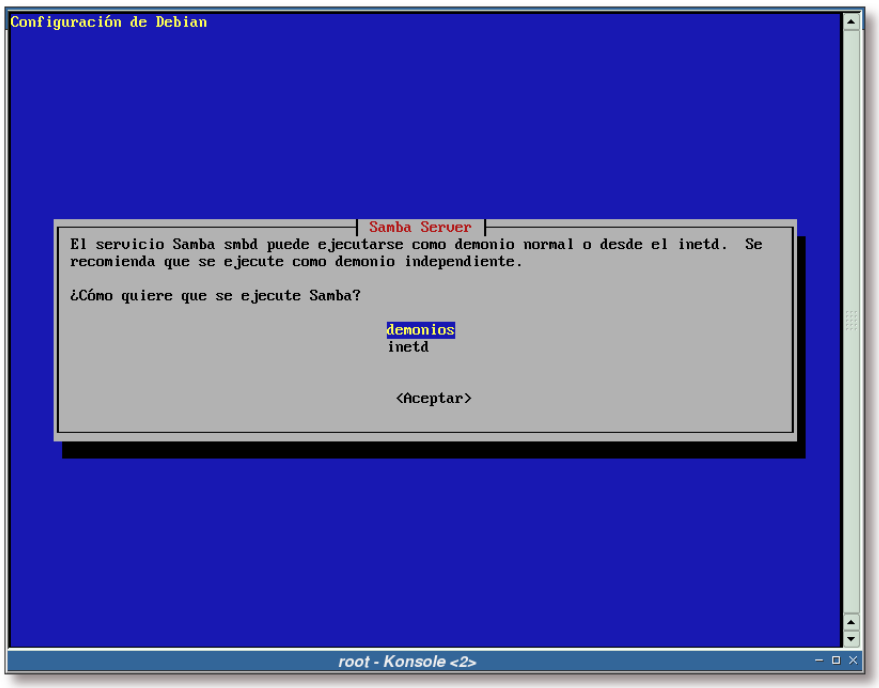
Se responde afirmativamente a esta pregunta, de esta forma se hará uso de cifrado para el intercambio/almacén de contraseñas.

Figura 7-3. ¿Utilizar la información del DHCP para configurar WINS?



En esta documentación no se van a utilizar servidores WINS ni DHCP, por lo que se responde que no a esta pregunta.

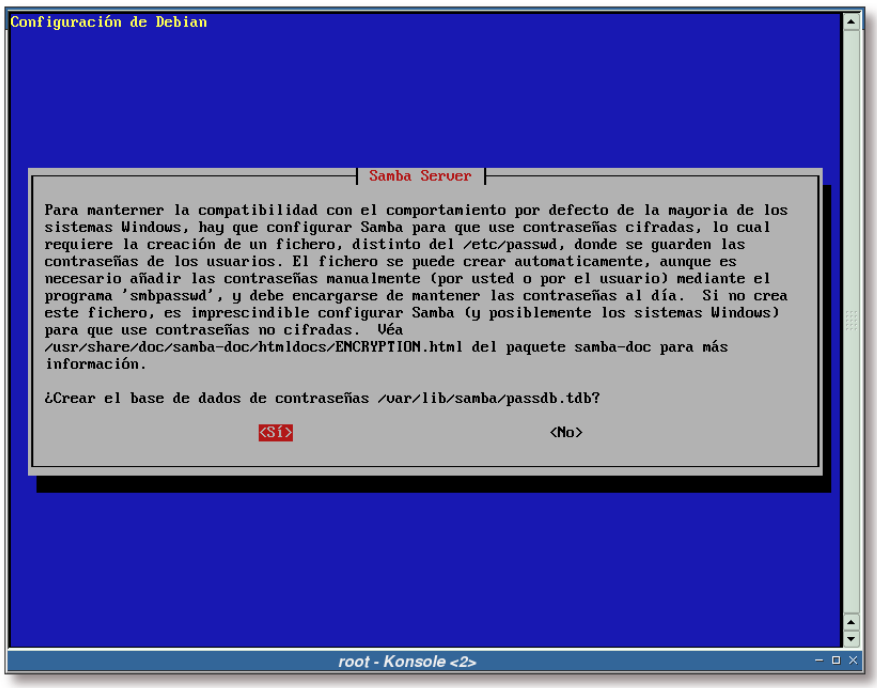
Figura 7-4. ¿Cómo ejecutar Samba (demonios/inetd)?



Momento para la elección sobre como se quiere ejecutar Samba, ya sea utilizando el superservidor inetd o mediante demonios.

La elección realizada para esta documentación ha sido la ejecución mediante demonios, ya que en un entorno donde el uso de Samba sea frecuente, es mucho más eficiente ejecutarlo desde los demonios que desde un superservidor inetd. De todas formas, en el Apéndice C puede ver como ejecutar Samba desde un superservidor (x)inetd.

Figura 7-5. Creación de la base de datos de contraseñas



Se responde que sí a esta pregunta, de esta forma se creará un archivo destinado al almacén de las contraseñas para los usuarios de Samba.

Ejemplo 7-4. Instalación de "samba" (segunda parte)

```
Seleccionando el paquete samba-common previamente no seleccionado.
(Leyendo la base de datos ...
133203 ficheros y directorios instalados actualmente.)
Desempaquetando samba-common (de .../samba-common_3.0.7-1_i386.deb) ...
Seleccionando el paquete samba previamente no seleccionado.
Desempaquetando samba (de .../samba_3.0.7-1_i386.deb) ...
Configurando samba-common (3.0.7-1) ...

Configurando samba (3.0.7-1) ...
Generating /etc/default/samba... ❶
TDBSAM version too old (0), trying to convert it.
TDBSAM converted successfully.
--------- IMPORTANT INFORMATION FOR XINETD USERS ---------- ❷
The following line will be added to your /etc/inetd.conf file:

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/smbd

If you are indeed using xinetd, you will have to convert the
above into /etc/xinetd.conf format, and add it manually. See
/usr/share/doc/xinetd/README.Debian for more information.
```

```
------------------------------------------------------------

Starting Samba daemons: nmbd smbd.

localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

❶ Archivo destinado a las opciones por defecto de los scripts de inicio del servidor Samba.

❷ Información para los usuarios de xinetd (servidor que reemplaza al superservidor de Internet -inetd-), importante si pretende utilizarlo para ejecutar Samba.

Nota: Si a la hora de instalar el paquete no se le han realizado todas las preguntas que se han mostrado en el proceso de instalación, puede forzarlo tecleando la siguiente orden:

Ejemplo 7-5. Configuración preliminar de "samba"

```
# /usr/sbin/dpkg-reconfigure --priority=low samba
```

En estos momentos el servidor Samba ya se encontraría instalado e inicialmente configurado. En el siguiente capítulo se verá como adecuar la configuración a sus necesidades, pero antes se tratará la instalación de los clientes en la siguiente sección.

Instalación de un cliente

Hay dos paquetes importantes para un cliente Samba: "smbclient" y "smbfs", a continuación se verá su descripción:

Ejemplo 7-6. Información sobre los paquetes "smbclient" y "smbfs"

```
$ /usr/bin/apt-cache show smbclient smbfs
Package: smbclient
Priority: optional
Section: net
Installed-Size: 5988
Maintainer: Eloy A. Paris <peloy@debian.org>
Architecture: i386
Source: samba
Version: 3.0.7-1
Replaces: samba (<< 2.999+3.0.alpha21-4)
Provides: samba-client
Depends: samba-common ❶  (= 3.0.7-1),
libc6 (>= 2.3.2.ds1-4), libcomerr2 (>= 1.33-3), libkrb53 (>= 1.3.2),
libldap2 (>= 2.1.17-1), libncurses5 (>= 5.4-1), libpopt0 (>= 1.7),
libreadline4 (>= 4.3-1)
Suggests: smbfs ❷
```

```
Filename: pool/main/s/samba/smbclient_3.0.7-1_i386.deb
Size: 2411216
MD5sum: 3c4fdf54182fce094b94a6f3e420e6f9
Description: a LanManager-like simple client for Unix
 The Samba software suite is a collection of programs that
 implements the SMB protocol for unix systems, allowing you to serve
 files and printers to Windows, NT, OS/2 and DOS clients. This protocol
 is sometimes also referred to as the LanManager or NetBIOS protocol.
 .
 This package contains some client components of the Samba suite. In
 particular it includes the command line utilities smbclient, smbtar,
 and smbspool. If you want to mount shares exported from Microsoft
 Windows machines or a Samba server you must install the smbfs package.
Task: file-server, print-server

Package: smbfs
Priority: optional
Section: otherosfs
Installed-Size: 720
Maintainer: Eloy A. Paris <peloy@debian.org>
Architecture: i386
Source: samba
Version: 3.0.7-1
Replaces: smbfsx
Depends: netbase (>= 2.02), samba-common ❸ (= 3.0.7-1),
libc6 (>= 2.3.2.ds1-4), libcomerr2 (>= 1.33-3), libkrb53 (>= 1.3.2), libldap2 (>= 2.1.17-1)
Suggests: smbclient ❹
Conflicts: smbfsx, suidmanager (<< 0.50)
Filename: pool/main/s/samba/smbfs_3.0.7-1_i386.deb
Size: 311844
MD5sum: 3051f174f56f0b1cc5056364847daa50
Description: mount and umount commands for the smbfs (for kernels >= than 2.2.x)
 Smbfs is a filesystem which understands the SMB protocol.
 This is the protocol Windows for Workgroups, Windows NT or
 LAN Manager use to talk to each other. It was inspired by
 samba, the program by Andrew Tridgell that turns any unix
 site into a file server for DOS or Windows clients.
 .
 If you want to use command-line utilities like smbclient, smbtar
 and/or smbspool you just need to install the smbclient package.
 .
 Starting with the Debian Samba packages version 2.2.0-1, the old smbfs
 utilities for 2.0.x have been removed. There are no wrapper scripts
 that call a specific smbmount/smbumount depending on the kernel
 version.  If you are using a 2.0.x kernel please upgrade or use the
 latest Samba 2.0.7 Debian package.
Task: file-server, print-server
```

❶❸ Como se puede ver, tanto el paquete “smbclient” como el paquete “smbfs” dependen de “samba-common”, al igual que el paquete “samba” (vea el Ejemplo 7-1).

❷❹ Se puede comprobar que ambos paquetes, “smbclient” y “smbfs”, se recomiendan mutuamente, normalmente suele ser buena idea instalar ambos.

Ahora que ya se tiene la información de los paquetes que se van a instalar en el cliente, se procede con su instalación:

Ejemplo 7-7. Instalación de “smbclient” y “smbfs”

```
# /usr/bin/apt-get install smbclient smbfs
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  smbclient smbfs
0 actualizados, 2 se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 0B/2723kB de archivos.
Se utilizarán 6869kB de espacio de disco adicional después de desempaquetar.
Seleccionando el paquete smbclient previamente no seleccionado.
(Leyendo la base de datos ...
133280 ficheros y directorios instalados actualmente.)
Desempaquetando smbclient (de .../smbclient_3.0.7-1_i386.deb) ...
Seleccionando el paquete smbfs previamente no seleccionado.
Desempaquetando smbfs (de .../smbfs_3.0.7-1_i386.deb) ...
Configurando smbclient (3.0.7-1) ...
Configurando smbfs (3.0.7-1) ...
localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

Una vez se ha completado el proceso de instalación, el sistema tendrá disponibles las siguientes herramientas (para saber que hace cada una, se pueden consultar las páginas del manual que traen adjuntas):

Ejemplo 7-8. Herramientas suministradas por los paquetes “smbclient” y “smbfs”

```
$ /usr/bin/dpkg -L smbclient  | /bin/grep bin
/usr/bin/smbclient
/usr/bin/smbtar
/usr/bin/rpcclient
/usr/bin/smbspool
/usr/bin/smbtree
/usr/bin/smbcacls
/usr/bin/smbcquotas
$ /usr/bin/dpkg -L smbfs  | /bin/grep bin
/usr/bin/smbmount
/usr/bin/smbumount
/usr/bin/smbmnt
/sbin/mount.smbfs
/sbin/mount.smb
```

Capítulo 8. Primeros ajustes en la configuración de OpenLDAP

Antes de continuar con la configuración de Samba, es necesario realizar algunas modificaciones y ajustes en la configuración de OpenLDAP, de forma que quede preparado para soportar las características de Samba.

Lo primero que se ha de hacer es copiar el esquema de samba al directorio de esquemas de OpenLDAP. El Ejemplo 8-2 muestra como hacerlo.

Importante: El archivo de esquemas para Samba se encuentra en el paquete samba-doc, por lo que si no lo ha instalado en su sistema, puede hacerlo en este momento:

Ejemplo 8-1. Instalación del paquete "samba-doc"

```
# /usr/bin/apt-get install samba-doc
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  samba-doc
0 actualizados, 1 se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 0B/11,6MB de archivos.
Se utilizarán 18,1MB de espacio de disco adicional después de desempaquetar.
Seleccionando el paquete samba-doc previamente no seleccionado.
(Leyendo la base de datos ...
133336 ficheros y directorios instalados actualmente.)
Desempaquetando samba-doc (de .../samba-doc_3.0.7-1_all.deb) ...
Configurando samba-doc (3.0.7-1) ...
localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

Ejemplo 8-2. Copiado del esquema de Samba al directorio de esquemas de OpenLDAP

```
# /bin/cp -v /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema
'/usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz' -> '/etc/ldap/schema/samba.schema.gz'
# /bin/gunzip -v /etc/ldap/schema/samba.schema.gz
/etc/ldap/schema/samba.schema.gz:        81.0% -- replaced with /etc/ldap/schema/samba.schema
# /bin/chown -v slapd.slapd /etc/ldap/schema/samba.schema
cambiado el propietario de '/etc/ldap/schema/samba.schema' a slapd:slapd
# /bin/chmod -v 644 /etc/ldap/schema/samba.schema
el modo de '/etc/ldap/schema/samba.schema' cambia a 0644 (rw-r--r--)
```

Por último, sólo queda añadir el nuevo esquema en el archivo de configuración de slapd y reiniciar el demonio. Para ello se ha de editar el archivo `/etc/ldap/slapd.conf` y añadir en la sección "# Schema and objectClass definitions" la siguiente línea:

Importante: El orden en el que se coloquen los esquemas dentro del archivo `/etc/ldap/slapd.conf` es importante. Si ha seguido todos los pasos hasta este punto, añada la siguiente línea al final de la lista de esquemas, para evitar errores al arrancar el demonio slapd.

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

Importante: La clase objeto (objectClass) *sambaSamAccount* definida en el esquema *samba.schema* depende de los siguientes esquemas:

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

Acto seguido, se ha de reiniciar el demonio slapd:

Ejemplo 8-3. Reinicio del demonio slapd

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

Capítulo 9. Configuración de Samba

Introducción

Este capítulo está dedicado a la configuración de Samba, primero se mostrará como es la estructura de un archivo de configuración para Samba y luego se procederá a mostrar las distintas opciones de configuración para obtener el resultado esperado.

> **Nota:** Para obtener la configuración de Samba se han utilizado las siguientes entradas bibliográficas, a parte de las páginas del manual que provee Samba: Lemaire01, Syroid01, Syroid02, Milne01, Milne02, TsEcksteinCollier-Brown01, VernooijTerpstraCarter01, Coupeau01.

Estructura del archivo `smb.conf`

La configuración de Samba se almacena en el archivo `smb.conf`, que en el sistema Debian GNU/Linux se encuentra en el directorio `/etc/samba/`. La edición de este archivo se puede hacer utilizando un editor de textos o haciendo uso de herramientas gráficas, como la que provee Samba: SWAT (vea el Apéndice E para más información).

Sintaxis

El archivo `smb.conf` utiliza la misma sintaxis que los antiguos ficheros .ini de Windows 3.1: cada archivo consistía en varias secciones, las cuales comenzaban con el nombre de la sección entre corchetes ([]) en una nueva línea. Cada una contenía cero o más pares llave/valor separados por un signo de igualdad (=). El archivo de configuración de Samba es un archivo en texto plano, por lo que se puede editar con cualquier editor de textos.

Cada sección en el archivo `smb.conf` representa un recurso compartido en el servidor Samba. La sección “global” es especial, ya que contiene opciones que se aplican a todo el servidor Samba y no sólo a un recurso compartido en particular.

Un archivo de configuración realmente pequeño, podría ser:

Ejemplo 9-1. Un archivo `smb.conf` mínimo

```
[global]
workgroup = GRUPODETRABAJO
netbios name = MINOMBRE

[recurso-compartido1]
path = /tmp

[recurso-compartido2]
path = /otro_directorio_compartido
```

```
comment = Algunos archivos aleatorios
```

Comprobando el archivo `smb.conf`

Es importante validar el contenido del archivo `smb.conf` haciendo uso del programa **testparm**. Si **testparm** se ejecuta correctamente, listará los servicios cargados.

En el Ejemplo 9-2 se comprobará el archivo que viene por defecto (vea el apéndice Apéndice AC) con el paquete de Samba de la distribución Debian GNU/Linux, una vez instalado el paquete.

Ejemplo 9-2. Comprobando el archivo por defecto `smb.conf` con testparm

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

[ENTER]
# Global parameters
[global]
        workgroup = GSRDOMAIN
        server string = %h server (Samba %v)
        obey pam restrictions = Yes
        passdb backend = tdbsam, guest
        passwd program = /usr/bin/passwd %u
        passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n .
        syslog = 0
        log file = /var/log/samba/log.%m
        max log size = 1000
        dns proxy = No
        panic action = /usr/share/samba/panic-action %d
        invalid users = root

[homes]
        comment = Home Directories
        create mask = 0700
        directory mask = 0700
        browseable = No

[printers]
        comment = All Printers
        path = /tmp
        create mask = 0700
        printable = Yes
        browseable = No

[print$]
```

```
comment = Printer Drivers
path = /var/lib/samba/printers
```

Ajustando el archivo de configuración de Samba

Introducción

En esta sección se configurará Samba como un Controlador Primario de Dominio que almacena su base de datos SAM en un servidor OpenLDAP.

Para la configuración se asumirá que:

- El nombre del dominio será: *GSRDOMAIN*
- El nombre del servidor Netbios será: *TODOSCSI*
- El directorio home de los usuarios estará en: `/home/samba/users/NOMBREUSUARIO`
- Los perfiles móviles se almacenarán en: `/home/samba/profiles/NOMBREUSUARIO`

[global] - sección global

En la sección global se configurarán los parámetros globales del servidor. Entre otras cosas, se definirán los programas que serán utilizados para que un usuario pueda cambiar su clave (*passwd program*) y el diálogo que se establecerá entre el servidor y el usuario durante este cambio.

La opción “add user script” permite al demonio smb añadir, como usuario root, una nueva máquina. Cuando una máquina contacta con el dominio, este script es llamado y la nueva máquina es añadida al dominio. Esto hace que la administración de las cuentas para las máquinas sea muy sencilla. Por razones de seguridad, no todas las máquinas pueden entrar en el dominio, sólo aquellas cuyo administrador tenga una cuenta con los privilegios suficientes.

En las secciones siguientes se mostrarán los parámetros más importantes de la configuración de Samba, en el Apéndice AD se muestra un archivo de configuración completo para Samba.

[global] - Búsqueda/Identificación

```
[global]
   workgroup = GSRDOMAIN ❶
   netbios name = TODOSCSI ❷
   server string = SAMBA-LDAP PDC server ❸
```

❶ Definición del nombre del dominio.

❷ Nombre Netbios por el cual el servidor Samba se va a conocer.

❸ Descripción del servidor.

[global] - Autentificación

```
security = user ❶
encrypt passwords = true ❷
passdb backend = ldapsam:ldap://gsr.pt ❸
guest account = guest ❹
invalid users = root ❺
unix password sync = yes ❻
passwd program = /usr/sbin/smbldap-passwd -o %u ❼
passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n
```

❶ Opción necesaria para la administración de dominios por parte de Samba.

❷ Se activa el cifrado para el almacenado de las claves

❸ Se asigna a esta opción el valor: “ldapsam:ldap://gsr.pt”, indicándole a Samba que las claves se almacenarán y recuperarán del servidor LDAP definido.

❹ Nombre del usuario “invitado”, este podrá acceder a aquellos recursos con el parámetro “guest ok” sin autentificarse.

❺ Lista de usuarios a los cuales no se le permite el acceso a Samba.

❻ Se activa la sincronización entre las claves Unix y las claves Samba.

❼ Programa utilizado durante el cambio de clave de un usuario. Vea el Apéndice H para saber como obtener esta herramienta.

❽ Texto que se mostrará durante el cambio de una clave mediante Samba.

[global] - LDAP

```
ldap admin dn = cn=admin,dc=gsr,dc=pt ❶
;  ldap server = gsr.pt ❷
;  ldap port = 389 ❸
ldap ssl = start_tls ❹
ldap delete dn = no ❺
ldap filter = (&(uid=%u)(objectclass=sambaSamAccount)) ❻
ldap suffix = ou=people,dc=gsr,dc=pt ❼
ldap user suffix = ou=people ❽
ldap group suffix = ou=groups ❾
ldap machine suffix = ou=machines (10)
```

❶ Esta línea le dice a Samba quien es el administrador del directorio LDAP. Este será el usuario empleado por Samba cuando se realicen operaciones de añadir, borrar o modificar cuentas de usuario.

❷ Parámetro que contiene el FQDN del servidor ldap. Se necesita para encontrar la información sobre las cuentas de usuario. Este parámetro se comenta, ya que parece que Samba no lo reconoce.

❸ Indica en que puerto está escuchando LDAP. El puerto 389 es el puerto estándar para las conexiones sin cifrado; el 636 es el puerto estándar para las conexiones con cifrado. Si la línea “ldap ssl” posee

el valor “on”, Samba intentará automáticamente conectarse por el puerto 636 para contactar con el servidor LDAP. Este parámetro se comenta, ya que parece que Samba no lo reconoce.

❹ Opción que determina si cifrar o no las comunicaciones entre el servidor Samba y el servidor LDAP. Se ha seleccionado la conexión por TLS, como ya viene siendo habitual a lo largo de toda la documentación.

❺ Este parámetro especifica si al realizar una operación de borrado en ldapsam, se borra la entrada completa o solamente los atributos específicos de Samba.

❻ Filtro de búsqueda para LDAP.

❼ Parámetro que especifica la base para todas las búsquedas en LDAP.

❽ Parámetro que indica donde se añaden los usuarios dentro del árbol.

❾ Parámetro que indica donde se añaden los grupos de usuarios dentro del árbol.

(10) Parámetro que indica donde se añaden las máquinas dentro del árbol.

[global] - impresión

```
   load printers = yes ❶
   printing = cups ❷
   printcap name = cups ❸
   printer admin = @domainadmins ❹
```

❶ Se cargan automáticamente la lista de impresoras disponibles.

❷❸ Estilo de impresión ha utilizar, en este caso se utilizará la impresión con CUPS (vea la Parte III en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota* dedicada a CUPS.)

❹ Grupo de usuarios que tienen permiso para añadir y configurar impresoras, a parte del usuario “root”.

[global] - Controlador de dominio

```
   os level = 80 ❶
   preferred master = yes ❷
   domain master = yes ❸
   local master = yes ❹
   domain logons = yes ❺
   logon path = \\%L\profiles\%u ❻
   logon drive = H: ❼
   logon home = \\%L\%u\.profile ❽
   logon script = ❾
;   domain admin group = @domainadmins (10)
```

❶ Parámetro que controla el nivel en el que Samba se anunciará como elección de búsqueda. El valor de este parámetro determinará si el demonio nmbd tendrá alguna posibilidad de llegar a ser un buscador primario local para el grupo de trabajo en el área de broadcast local.

❷❸❹❺Estos parámetros juegan un papel fundamental asegurando el control del dominio y el soporte de autentificación en red. Una descripción más detallada de los mismos se encuentra en la página del manual smb.conf(5).

❻❼❽❾Opciones que facilitan las operaciones de autentificado de clientes y facilitan el control automatizado para la administración de redes sobrecargadas. Más información en la página del manual smb.conf(5).

(10) Parámetro que acepta usuarios y grupos de usuarios que serán administradores de dominio. Este parámetro se comenta, ya que parece que Samba no lo reconoce.

[global] - Misceláneo

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192 ❶
idmap uid = 10000-20000 ❷
idmap gid = 10000-20000 ❸
template shell = /bin/bash ❹
add user script = /usr/sbin/smbldap-useradd -w %u ❺
```

❶ Distintas opciones que mejoran el rendimiento del servidor Samba.

❷❸ Estos dos parámetros especifican el rango de los ids de usuario y grupo, respectivamente, que serán utilizados en el mapeado de usuarios/grupos Unix en SIDs de usuarios/grupos NT.

❹ Shell que el demonio winbindd añadirá a la información de un usuario, cuando este valor no sea omitido.

❺ Se hace uso de las herramientas *smbldap-tools* para añadir maquinas (En el Apéndice H se muestra un ejemplo de instalación y configuración de estas herramientas).

[homes] - directorios personales

Esta sección permite la compartición del directorio *home* de los usuarios, de forma que, dependiendo que usuario se haya autentificado en el sistema, Samba compartirá su directorio personal únicamente a él.

Los parámetros más importantes de esta sección se muestran a continuación:

```
browseable = yes ❶
writeable = yes ❷
create mask = 0700 ❸
directory mask = 0700 ❹
```

❶ Indica si este recurso aparecerá en la lista de recursos compartidos o no. En este caso, si se mostrará.

❷ Esta opción permite escribir datos en los directorios *home*, si su valor fuese “no”, los directorios *home* se compartirían como sólo lectura.

❸ Máscara de creación de archivos, el valor de este parámetro indicará los permisos que tendrán los archivos de nueva creación.

❹ Máscara de creación de directorios, el valor de este parámetro indicará los permisos que tendrán los directorios de nueva creación.

[netlogon]

El recurso compartido *NETLOGON* juega un papel fundamental en el soporte de inicio de sesión en un dominio y Miembro de Dominio. Este recurso compartido se provee en todos los Controladores de Dominio de Microsoft. Se utiliza para proveer de scripts de inicio de sesión, para almacenar archivos de Políticas de Grupo (`NTConfig.POL`), así como la localización de otras herramientas comunes que se puedan necesitar para el proceso de inicio de sesión. Este es un recurso esencial en un Controlador de dominio.

Los parámetros más importantes de esta sección se muestran a continuación:

```
path = /home/samba/netlogon ❶
writeable = no ❷
write list = @domainadmins ❸
```

❶ Directorio donde se van a alojar los scripts.

❷ No se permite escribir en el recurso compartido, sólo lectura.

❸ Lista de usuarios/grupos que tienen permiso de escritura en el recurso compartido.

[profiles] - perfiles móviles

Este recurso compartido se utiliza para almacenar los perfiles de escritorio de los usuarios. Cada usuario ha de tener un directorio en el raíz de este recurso compartido. Este recurso ha de tener permisos de escritura para los usuarios y debería tener la permisos de lectura globales. Samba-3 tiene un módulo VFS denominado “fake_permissions” (permisos “falsos”) que se deberían instalar en este recurso. Este módulo permitiría a un administrador de Samba hacer el directorio de sólo lectura para todo el mundo. Por supuesto, esto sólo es útil una vez se ha creado correctamente el perfil.

Los parámetros más importantes de esta sección se muestran a continuación:

```
path = /home/samba/profiles ❶
writeable = yes ❷
browseable = no ❸
create mask = 0600 ❹
directory mask = 0700 ❺
```

❶ Directorio donde se almacenarán los perfiles móviles, bajo este directorio, cada usuario tendrá una carpeta con su nombre.

❷ Se permite escribir en el recurso compartido.

❸ Indica si este recurso aparecerá en la lista de recursos compartidos o no. En este caso, no se mostrará.

❹ Máscara de creación de archivos, el valor de este parámetro indicará los permisos que tendrán los archivos de nueva creación.

❺ Máscara de creación de directorios, el valor de este parámetro indicará los permisos que tendrán los directorios de nueva creación.

[printers] - impresoras

Este es un recurso compartido especial que crea automáticamente servicios de impresión. La forma en que trabaja es la siguiente: si se crea un recurso compartido con el nombre [printers] en el archivo de configuración, Samba leerá automáticamente el archivo de definición de sus impresoras y creará una impresora compartida para cada impresora que aparezca en el archivo. Por ejemplo, si posee tres impresoras definidas: una *lp* otra *pcl* y una última *ps*, Samba proveerá tres impresoras compartidas con esos nombres, cada una configurada con las opciones que aparezcan en el recurso compartido [printers].

Los parámetros más importantes de esta sección se muestran a continuación:

```
browseable = no ❶
path = /tmp ❷
printable = yes ❸
guest ok = no ❹
writable = no ❺
create mask = 0700 ❻
```

❶ Indica si este recurso aparecerá en la lista de recursos compartidos o no. En este caso, no se mostrará.

❷ Directorio que utilizará Samba como cola de impresión.

❸ Como este parámetro tiene el valor *yes*, los clientes que se conecten al servidor, podrán abrir, escribir en y enviar archivos a la cola de impresión, es decir, al directorio especificado por la variable *path*.

❹ No se permitirán las conexiones sin autentificación a este recurso.

❺ No se permite escribir en el recurso compartido.

❻ Máscara de creación de archivos, el valor de este parámetro indicará los permisos que tendrán los archivos de nueva creación.

[print$] - controladores de impresión

Al igual que un servidor de impresión Windows NT, para soportar la descarga de controladores por parte de clientes con distintas arquitecturas, se han de crear varios subdirectorios dentro del servicio [print$]. Estos se corresponderán con cada una de las arquitecturas soportadas. Samba también sigue este esquema. Así como el nombre del recurso compartido ha de ser [print$], los subdirectorios han de ser exactamente los nombres que se listan a continuación (puede obviar aquellos subdirectorios para las arquitecturas que no necesite soporte).

Por lo tanto, se ha de crear la estructura de directorios que se muestra a continuación, bajo el directorio compartido por [print$]. Cree aquellos directorios para aquellas arquitecturas que quiera dar soporte:

Ejemplo 9-3. [print$] - Subdirectorios para las distintas arquitecturas

```
[print$]--+
          |--W32X86           # controladores para Windows NT x86
```

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

Nota: El paquete “samba” de Debian GNU/Linux crea esta estructura de directorios bajo `/var/lib/samba/printers`.

Los parámetros más importantes de esta sección se muestran a continuación:

```
path = /var/lib/samba/printers ❶
browseable = yes ❷
writeable = no ❸
guest ok = no ❹
write list = root, @domainadmins ❺
```

❶ Directorio donde se almacenarán los controladores de impresión para las distintas arquitecturas.

❷ Indica si este recurso aparecerá en la lista de recursos compartidos o no. En este caso, si se mostrará.

❸ No se permite escribir en el recurso compartido.

❹ No se permitirán las conexiones sin autentificación a este recurso.

❺ Lista de usuarios/grupos que tienen permiso de escritura en el recurso compartido.

[tmp] - Directorio temporal

A modo de ejemplo, se va a compartir el directorio temporal `/tmp` con los siguientes parámetros:

```
comment = Temporal ❶
writeable = yes ❷
path = /tmp ❸
guest ok = no ❹
```

❶ Comentario del recurso compartido.

❷ Se permite la escritura en este recurso.

❸ Directorio compartido dentro del sistema.

❹ No se permiten conexiones anónimas al directorio, todo usuario ha de autentificarse para acceder a este recurso.

[cdrom] - CDROM

Otro ejemplo de compartición será el CDROM del sistema. Los parámetros empleados en esta ocasión serán:

```
comment = Samba server’s CD-ROM ❶
writable = no ❷
```

```
locking = no ❸
path = /cdrom ❹
guest ok = yes ❺
```

❶ Comentario del recurso compartido.

❷ No se permite la escritura en este recurso compartido.

❸ No se bloquearán realmente los archivos a petición de los clientes, simplemente se informará de que el bloqueo ha sido efectivo.

❹ Ruta hacia el recurso compartido.

❺ Se permitirá el acceso a este recurso a los usuarios invitados, es decir, aquellos usuarios que no se han autentificado.

Sugerencia: Normalmente, para acceder al contenido de un CDROM es necesario montarlo primero. Por lo que se recomienda instalar el parche supermount (http://supermount-ng.sourceforge.net/) en el núcleo Linux, de forma que el montado y desmontado del CDROM sea transparente al usuario. Cuando se intenta acceder al recurso, el CDROM se montará automáticamente.

Una vez aplicado el parche en el núcleo y seleccionado para la compilación, se ha de modificar la entrada para el CDROM dentro del archivo `/etc/fstab`, de forma que quede algo similar a:

```
<file system> <mount point> <type>     <options>                              <dump><pass>
none          /cdrom        supermount dev=/dev/cdrom,fs=auto,ro,auto,user,exec  0     0
```

Capítulo 10. Ajustes finales en el sistema

Introducción

Antes de considerar Samba completamente instalado y configurado, se han de realizar una serie de modificaciones en el sistema, y estas modificaciones se abarcan en este capítulo.

Estableciendo la clave del administrador de LDAP

Samba necesita conocer la clave del administrador del directorio LDAP para poder acceder al mismo. Por este motivo es necesario indicársela, para ello ejecute:

Ejemplo 10-1. Especificando la clave del administrador de LDAP en Samba

En la captura de pantalla que se muestra a continuación, sustituya la palabra “clave” por la clave del administrador del servidor LDAP:

```
# /usr/bin/smbpasswd -w clave
Setting stored password for "cn=admin,dc=gsr,dc=pt" in secrets.tdb
```

> **Aviso**
>
> Si varía el valor de la opción “ldap admin dn” del archivo de configuración de Samba, la clave del administrador del directorio LDAP ha de resetearse, ejecutando de nuevo la orden presente en el Ejemplo 10-1.

Nueva regla de control de acceso en `/etc/ldap/slapd.conf`

Debido a que a partir de ahora se almacenarán las claves relacionadas con Samba en el directorio LDAP, se añade en el archivo `/etc/ldap/slapd.conf` una nueva regla de control de acceso que impida, a todos aquellos usuarios distintos del administrador de LDAP, el acceso a los “hashes” de las distintas claves allí almacenadas. Las líneas que se han de añadir al archivo son:

```
# allow the "ldap admin dn" access, but deny everyone else
# (Samba related)
access to attribute=sambaLMPassword,sambaNTPassword
     by dn="cn=admin,dc=gsr,dc=pt" write
     by dn="cn=readadmin,dc=gsr,dc=pt" read
     by * none
```

Para que la nueva configuración tenga efecto, ha de reiniciar el demonio slapd, en el Ejemplo 3-7 se muestra como hacerlo.

Especificación de nuevos índices en `/etc/ldap/slapd.conf`

Con el objetivo de mejorar el rendimiento de las búsquedas dentro del directorio LDAP, se van a añadir una serie de índices al archivo de configuración del demonio slapd.

Los índices que se presentan a continuación, incrementan la velocidad en las búsquedas realizadas sobre la clases objeto *sambaSamAccount*, y posiblemente también sobre las clases objeto *posixAccount* y *posixGroup*.

```
# Requerido por OpenLDAP
index objectclass            eq

index default                sub
index cn                     pres,sub,eq
index sn                     pres,sub,eq
index mail                   eq,subinitial
index givenname              eq,subinitial

# Requerido para soportar pdb_getsampwnam
index uid                    pres,sub,eq

# Requerido para soportar pdb_getsambapwrid()
index displayName            pres,sub,eq

# Descomente las siguientes líneas si está almacenando entradas
# posixAccount y posixGroup en el directorio
index uidNumber              eq
index gidNumber              eq
index memberUid              eq

# Samba 3.*
index sambaSID             eq
index sambaPrimaryGroupSID  eq
index sambaDomainName       eq
```

Una vez realizados los cambios en el archivo `/etc/ldap/slapd.conf` se han de regenerar los índices, para ello ejecute:

Ejemplo 10-2. Regenerando los índices de slapd

```
# /usr/sbin/slapindex -vf /etc/ldap/slapd.conf
indexing id=00000001
indexing id=00000002
indexing id=0000000a
indexing id=0000000b
indexing id=0000000c
```

Ahora sólo queda reiniciar el servidor slapd:

Ejemplo 10-3. Reiniciando el servidor slapd

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

Creando la estructura de directorios en el *home*

En el Capítulo 9 se han definido una serie de directorios dedicados a distintas tareas dentro de Samba, como pueden ser alojar los perfiles móviles de los usuarios, los scripts para Netlogon o el directorio home de los usuarios.

En esta sección se van a crear los anteriores directorios para preparar el sistema para alojar usuarios:

Ejemplo 10-4. Creación de los directorios necesarios para Samba

```
# mkdir -vpm 755 /home/samba/
mkdir: se ha creado el directorio ‘/home/samba’
# mkdir -vpm 755 /home/samba/netlogon /home/samba/users
mkdir: se ha creado el directorio ‘/home/samba/netlogon’
mkdir: se ha creado el directorio ‘/home/samba/users’
# /bin/chgrp -v domainadmins /home/samba/netlogon/ ❶
cambiado el grupo de ‘netlogon/’ a domainadmins
# mkdir -vpm 1757 /home/samba/profiles
mkdir: se ha creado el directorio ‘/home/samba/profiles’
```

❶ El grupo *domainadmins* se crea en el proceso de configuración de la herramienta *LDAP Account Manager* (vea el Apéndice F, concretamente la imagen Figura F-24).

Capítulo 11. Comprobando que todo funciona

Introducción

En esta sección se va a comprobar que todo lo que se ha realizado hasta ahora funciona; esto significa añadir usuarios al directorio LDAP y comprobar que tanto desde Samba como desde el propio sistema se puede hacer uso de dichos usuarios.

La administración de usuarios se va a realizar con el programa LDAP Account Manager (http://lam.sourceforge.net/). El proceso de instalación se encuentra en el Apéndice F.

Otro de los programas empleados en la administración de LDAP es: phpLDAPadmin (http://phpldapadmin.sourceforge.net/). El Apéndice G muestra la manera de instalarlo y configurarlo.

Para finalizar, son necesarias las herramientas *smbldap-tools*, ya que internamente Samba hace uso de ellas, como se ha definido en algunas partes de su configuración (vea las secciones:
la sección de nombre *[global] - Autentificación* en Capítulo 9 y
la sección de nombre *[global] - Misceláneo* en Capítulo 9 para más detalles). El Apéndice H muestra el proceso de instalación y configuración de este conjunto de herramientas.

> **Importante:** Se recomienda seguir el siguiente orden de instalación de las herramientas anteriormente expuestas: 1º *LDAP Account Manager*, 2º *phpLDAPadmin* y 3º *smbldap-tools*.

Verificación del archivo de configuración y reinicio de los demonios

En el capítulo Capítulo 9 se mostró la forma de configurar un servidor Samba. El resultado de esa configuración ha sido el archivo disponible en el Apéndice AD. En estos momentos, sólo queda comprobar si dicho archivo está bien, para ello se hará uso del programa **testparm**, como se muestra en el siguiente ejemplo:

Ejemplo 11-1. Comprobando la nueva configuración (soporte LDAP)

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

```
[ENTER]
# Global parameters
[global]
        workgroup = GSRDOMAIN
        server string = SAMBA-LDAP PDC server
        obey pam restrictions = Yes
        passdb backend = ldapsam:ldap://gsr.pt
        guest account = guest
        passwd program = /usr/sbin/smbldap-passwd -o %u
        passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n .
        unix password sync = Yes
        syslog = 0
        log file = /var/log/samba/log.%m
        max log size = 1000
        name resolve order = lmhosts host wins bcast
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        add user script = /usr/sbin/smbldap-useradd.pl -w %u
        logon path = \\%L\profiles\%u
        logon drive = H:
        logon home = \\%L\%u\.profile
        domain logons = Yes
        os level = 80
        preferred master = Yes
        domain master = Yes
        dns proxy = No
        ldap admin dn = cn=admin,dc=gsr,dc=pt
        ldap group suffix = ou=groups
        ldap machine suffix = ou=machines
        ldap suffix = dc=gsr,dc=pt
        ldap user suffix = ou=people
        panic action = /usr/share/samba/panic-action %d
        idmap uid = 10000-20000
        idmap gid = 10000-20000
        template shell = /bin/bash
        printer admin = @domainadmins

[homes]
        comment = Home Directories
        read only = No
        create mask = 0700
        directory mask = 0700
        browseable = No

[netlogon]
        comment = Network Logon Service
        path = /home/samba/netlogon
        write list = @domainadmins
        guest ok = Yes
        share modes = No

[profiles]
        comment = User’s Profiles
```

```
        path = /home/samba/profiles
        read only = No
        create mask = 0600
        directory mask = 0700
        guest ok = Yes
        browseable = No

[printers]
        comment = All Printers
        path = /tmp
        printable = Yes
        browseable = No

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/printers
        write list = root, @domainadmins

[tmp]
        comment = Temporal
        path = /tmp
        read only = No

[cdrom]
        comment = Samba server's CD-ROM
        path = /cdrom
        guest ok = Yes
        locking = No
```

Una vez el archivo de configuración está listo y libre de posibles errores, el servidor Samba ha de releer su configuración. La forma de hacer esto se muestra en el Ejemplo 11-2.

Ejemplo 11-2. Releyendo la configuración de Samba

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

Aunque con releer la configuración de Samba es suficiente para que tengan efecto los cambios introducidos en el mismo, se van a reiniciar los demonios de Samba y ver que muestran los archivos de log de los mismos. Esta última parte se muestra en el Ejemplo 11-3.

Ejemplo 11-3. Reinicio los demonios de Samba

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

Tras el reinicio de los demonios de samba, se echa un vistazo en los archivos de log siguientes: `/var/log/samba/log.nmbd` y `/var/log/samba/log.smbd`. El resultado es el siguiente:

- Archivo `/var/log/samba/log.nmbd`

```
[2004/10/03 13:15:26, 0] nmbd/nmbd.c:terminate(54)
  Got SIGTERM: going down...
[2004/10/03 13:15:30, 0] nmbd/nmbd.c:main(664)
  Netbios nameserver version 3.0.7-Debian started.
  Copyright Andrew Tridgell and the Samba Team 1994-2004
[2004/10/03 13:15:30, 0] nmbd/nmbd_logonnames.c:add_logon_names(163)
  add_domain_logon_names:
  Attempting to become logon server for workgroup GSRDOMAIN on subnet 192.168.3.3
[2004/10/03 13:15:30, 0] nmbd/nmbd_become_dmb.c:become_domain_master_browser_bcast(282)
  become_domain_master_browser_bcast:
  Attempting to become domain master browser on workgroup GSRDOMAIN on subnet 192.168.3
[2004/10/03 13:15:30, 0] nmbd/nmbd_become_dmb.c:become_domain_master_browser_bcast(295)
  become_domain_master_browser_bcast: querying subnet 192.168.3.3 for domain master bro
  on workgroup GSRDOMAIN
[2004/10/03 13:15:34, 0] nmbd/nmbd_logonnames.c:become_logon_server_success(124)
  become_logon_server_success: Samba is now a logon server for workgroup GSRDOMAIN
  on subnet 192.168.3.3
[2004/10/03 13:15:38, 0] nmbd/nmbd_become_dmb.c:become_domain_master_stage2(113)
  *****

  Samba server TODOSCSI is now a domain master browser for workgroup GSRDOMAIN
  on subnet 192.168.3.3

  *****
[2004/10/03 13:15:53, 0] nmbd/nmbd_become_lmb.c:become_local_master_stage2(396)
  *****

  Samba name server TODOSCSI is now a local master browser for workgroup GSRDOMAIN
  on subnet 192.168.3.3

  *****
```

Se puede comprobar que Samba se ha convertido en un controlador de dominio bajo al subred 192.168.3.3. El dominio que está administrando es *GSRDOMAIN*.

- Archivo `/var/log/samba/log.smbd`

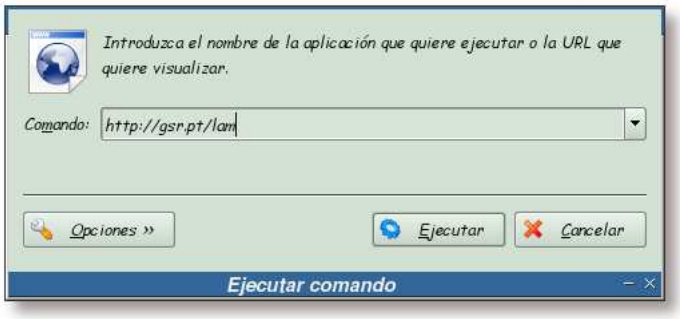
```
[2004/10/03 13:15:30, 0] smbd/server.c:main(760)
  smbd version 3.0.7-Debian started.
  Copyright Andrew Tridgell and the Samba Team 1992-2004
[2004/10/03 13:15:30, 0] printing/print_cups.c:cups_printer_fn(119)
  Unable to connect to CUPS server localhost - Conexión rehusada
```

Como en estos momentos no se ha instalado el servidor de impresión CUPS, Samba no puede contactar con él. Vea la Parte III en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota* dedicada a CUPS para obtener más información sobre como instalarlo y configurarlo.

Adición de un usuario al sistema

Como se ha comentado anteriormente, se va a emplear la herramienta *LDAP Account Manager* para la gestión de usuarios. Las capturas de pantalla que se muestran a continuación mostrarán los pasos que hay que seguir para añadir un usuario al sistema:

Figura 11-1. URL donde está instalado LAM



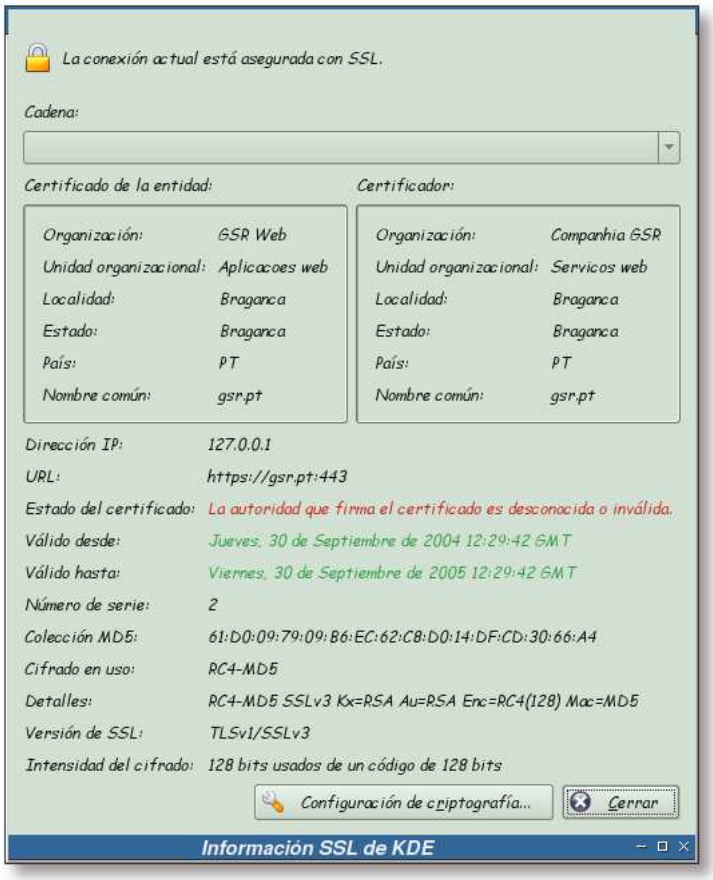
Si se encuentra en un entorno de escritorio con KDE, teclee **Alt**+**F2** e introduzca la dirección donde se encuentre instalado LAM.

Figura 11-2. Aviso acerca del certificado del servidor web I

Si ha configurado correctamente el servidor web, a la hora de acceder a la aplicación LAM por el protocolo *http*, Apache le tendría que redireccionar a la misma dirección, pero bajo el protocolo *https* (más información en: la sección de nombre *Introducción* en Apéndice I y la sección de nombre *Configuración relativa a Apache* en Apéndice F)

Esto es lo que ha ocurrido en esta pantalla, Apache ha redirigido la petición realizada (http://gsr.pt/lam/) hacia el protocolo *https*. Por este motivo, y debido a que la entidad certificadora que se ha creado es desconocida, sale este aviso. Pulse sobre el botón *Detalles* para obtener más información.

Figura 11-3. Información SSL



En esta pantalla se muestra la información del certificado y la entidad certificadora que ha creado dicho certificado. Si se fija, aquí aparecerán los datos tecleados en el Apéndice I. Pulse sobre el botón *Cerrar* para continuar.

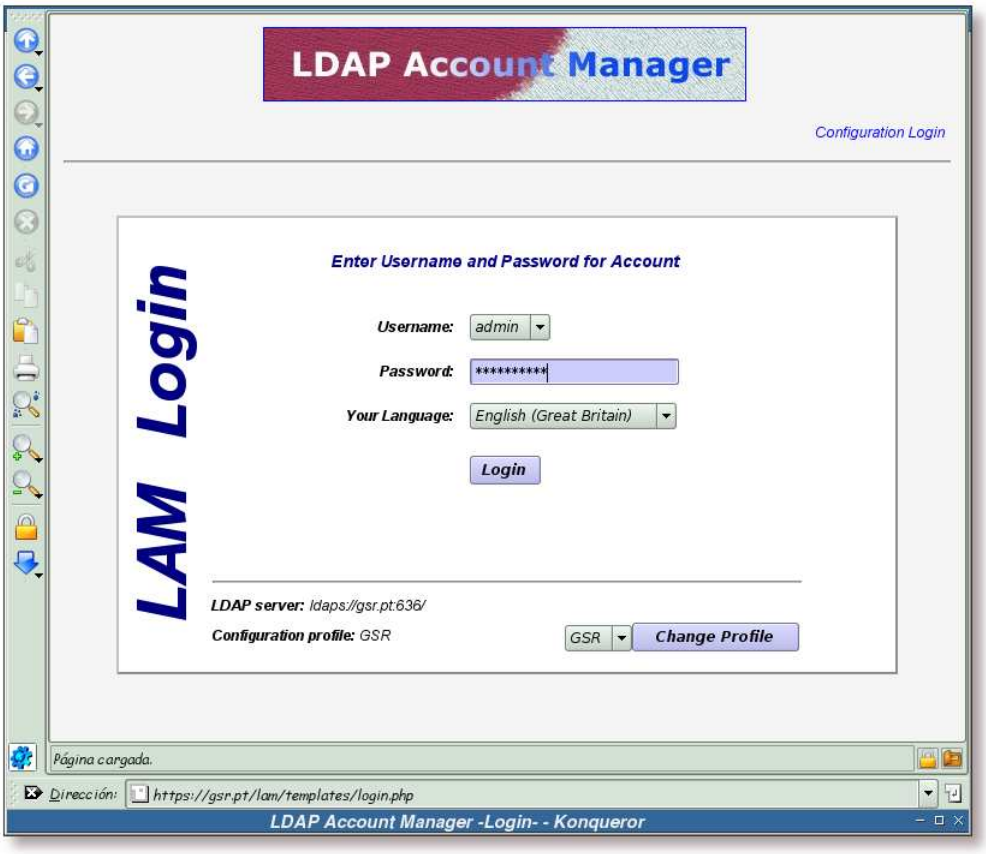
Figura 11-4. Aviso acerca del certificado del servidor web II

Pulse ahora sobre el botón *Continuar* para seguir con la carga de la página.

Figura 11-5. Período de aceptación del certificado

Seleccione la opción deseada y pulse sobre ella.

Figura 11-6. Ingreso en LAM



Si no está seleccionado, elija el perfil *GSR* y pulse sobre: *Change Profile*. Una vez seleccionado el perfil adecuado, se ha de teclear la clave del administrador del directorio LDAP y pulsar sobre *Login*.

Figura 11-7. Edición de perfiles

La sección predeterminada, tras el ingreso en la herramienta, es la gestión de usuarios. Antes de añadir usuarios, se creará un nuevo perfil de usuarios, personalizado para el sistema de ejemplo. Para proceder a la edición de perfiles, se ha de pulsar sobre el enlace *Profile Editor*.

Figura 11-8. Edición de un perfil de usuario

En el cuadro de *User Profiles* se selecciona la opción *Create a new User Profile* y se pulsa sobre el botón *Submit*.

Figura 11-9. Opciones de las cuentas (primera parte)

El cuadro destinado a las cuentas Unix (*Unix account*) permite configurar una serie de opciones comunes a todos los usuarios, como son:

- *Primary group*: selección del grupo principal de los usuarios, por defecto será el grupo *domainusers*.
- *Additional groups*: selección del grupo o grupos adicionales para los usuarios, a mayores se seleccionará el grupo *domainguest*.
- *Home Directory*: localización del home de los usuarios. La ruta donde se establecerán los archivos personales de cada usuario será: `/home/samba/users/$user`, donde la variable *$user* se sustituirá por el nombre del usuario a la hora de su creación.
- *Login shell*: se establece la shell *bash* como shell por defecto para los usuarios.
- *Account expires on*: se establece la fecha en la cual la cuenta va a caducar. Se ha fijado en el máximo disponible por la aplicación.

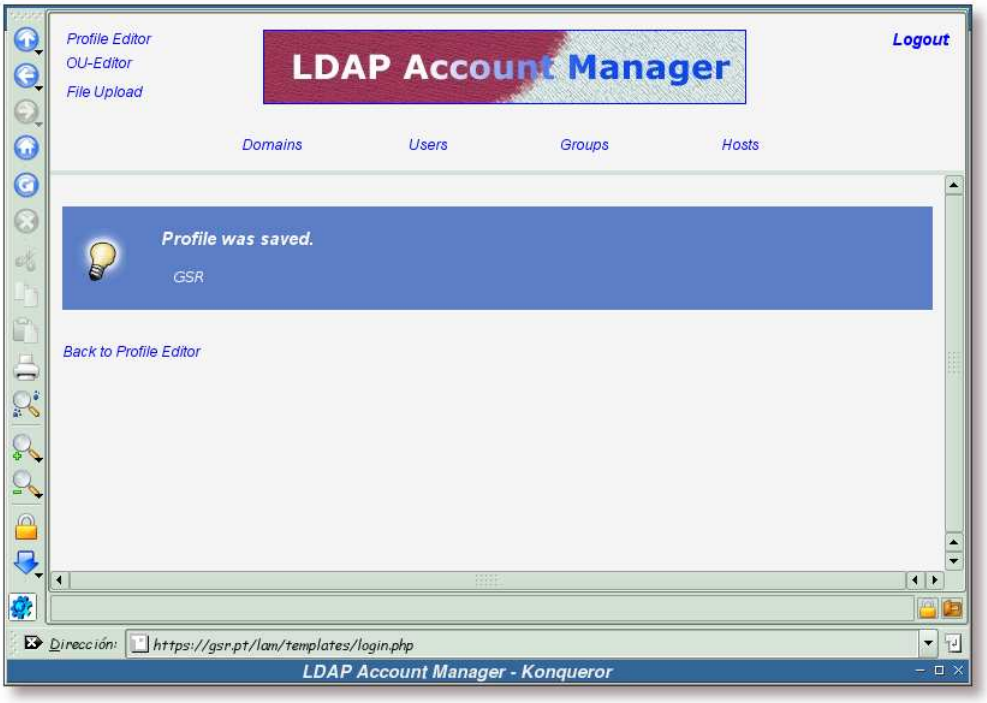
Figura 11-10. Opciones de las cuentas (segunda parte)

En el cuadro destinado a las cuentas de Samba (*Samba account*) especifique la ruta al directorio home (*todoscsi**$user*) y la ruta al directorio para los perfiles móviles de los usuarios (*todoscsi**profiles**$user*). Al igual que en las cuentas Unix, la variables *$user* se sustituirá por el nombre del usuario a la hora de crear una nueva cuenta.

El campo *Profile name* se rellena con el nombre del perfil que se quiere crear, en este caso: *GSR*.

Para continuar, pulse sobre el botón *Save*.

Figura 11-11. Perfil guardado



Esta pantalla informa de que el perfil *GSR* se ha guardado correctamente.

Se pulsa sobre el enlace *Users* para proceder a la adición de un nuevo usuario.

Figura 11-12. Creación de un nuevo usuario

Se pulsa sobre el botón: *New user* para comenzar el proceso de creación de un nuevo usuario.

Figura 11-13. Selección del perfil

Antes de comenzar a completar los campos con los datos del nuevo usuario, se ha de seleccionar el perfil anteriormente creado, *GSR*. Una vez seleccionado, se pulsa sobre el botón: *Load Profile*.

Figura 11-14. Datos generales

Con el perfil *GSR* cargado, sólo se han de completar los campos: *Username* con el nombre que va a tener el usuario en el sistema, *First name* con el nombre real del usuario, *Last name* con el primer apellido del usuario y, opcionalmente, el campo *Gecos* con una descripción del usuario.

Para continuar, se ha de pulsar sobre el botón *Unix*.

Figura 11-15. Datos generales, completado automático de información

Antes de acceder a la información sobre Unix, la aplicación completa automáticamente el campo *UID number* y sustituye las variables *$group* y *$user* por sus valores reales en el campo *Home directory*.

Pulsando en este momento, nuevamente, sobre el botón *Unix* se accederá a la información sobre Unix para el usuario.

Figura 11-16. Propiedades sobre Unix

En esta pantalla se completa la clave que tendrá el usuario, campos *Password* y *Repeat password*. Seguidamente pulse sobre el botón: *Samba*.

Figura 11-17. Propiedades sobre Samba (primera parte)

En esta pantalla se completa el campo *Display name*, de forma que ilustre quien es el usuario de la cuenta.

Una vez realizado esto, pulse sobre el botón *Personal*.

Figura 11-18. Propiedades sobre Samba (segunda parte)

Antes de acceder a la información personal, la aplicación sustituye las variables *$group* y *$user* por sus valores reales en los campos *Home path* y *Profile path*.

Vuelva a pulsar sobre el botón *Personal*.

Figura 11-19. Propiedades personales

En esta pantalla no se completa ningún campo, de todas formas es libre de seleccionar aquellos campos que quiera completar.

Se pulsa sobre el botón *Final* para continuar.

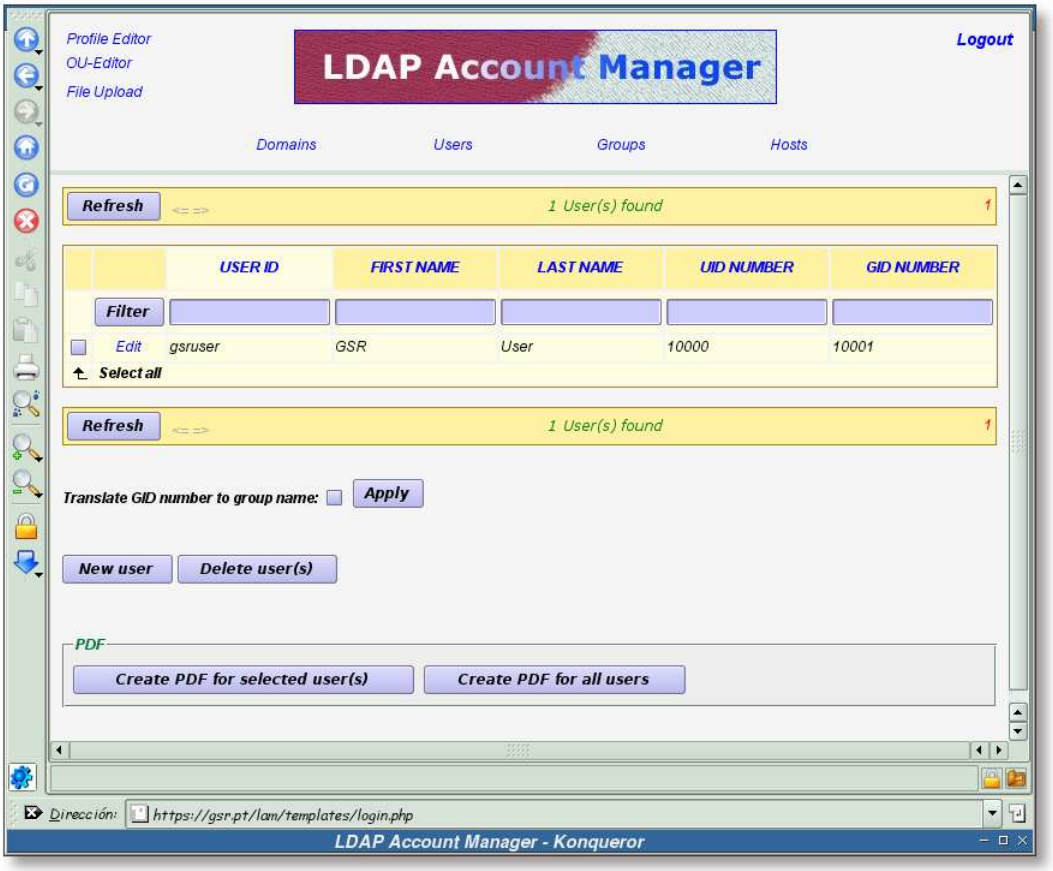
Figura 11-20. Creación del usuario

Para completar la creación del usuario, se ha de pulsar sobre el botón *Create Account*.

Figura 11-21. Usuario creado

Esta pantalla indica que el usuario se ha creado satisfactoriamente, se va a comprobar accediendo a la lista de usuarios, para ello pulse sobre el botón *Back to user list*.

Figura 11-22. Lista de usuarios



Se puede comprobar en esta pantalla que el usuario *gsruser* ya se encuentra en el directorio LDAP.

Acceso con la nueva cuenta en un sistema Unix

A continuación se va a probar el acceso por ssh, con el nuevo usuario, a una shell de Unix. Para ello se tecleará:

Ejemplo 11-4. Acceso a una shell Unix por ssh

```
$ /usr/bin/ssh -l gsruser gsr.pt
password: [clave]
Creating directory '/home/samba/users/gsruser'. ❶
Creating directory '/home/samba/users/gsruser/Maildir'.
Creating directory '/home/samba/users/gsruser/Maildir/cur'.
Creating directory '/home/samba/users/gsruser/Maildir/new'.
Creating directory '/home/samba/users/gsruser/Maildir/tmp'.
todoscsi-[gsruser]-13:39:04:~$
```

❶ Gracias a la opción comentada en el Ejemplo 5-12, al entrar por primera vez con la cuenta *gsruser* y no tener creado el directorio *home* para este usuario, el módulo *pam_mkhomedir* se encarga de crearlo, copiando el contenido del directorio `/etc/skel` al recién creado home.

Acceso con la nueva cuenta a Samba

Por último, se va a verificar el acceso a los recursos compartidos mediante Samba. Para ello se va a utilizar la orden **smbclient** y el navegador Konqueror, para ver dos formas de acceso a los recursos.

Uso de smbclient

smbclient es un cliente parecido al cliente **ftp**, que permite el acceso a los recursos compartidos de un servidor mediante SMB/CIFS.

En primer lugar se listarán los recursos que tiene compartido un determinado servidor, para ello se ha de teclear:

Ejemplo 11-5. Mostrando los recursos compartidos con smbclient

```
$ /usr/bin/smbclient -L TODOSCSI --user=gsruser
Password: [clave]
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk      Network Logon Service
        print$          Disk      Printer Drivers
        tmp             Disk      Temporal
        cdrom           Disk      Samba server's CD-ROM
        IPC$            IPC       IPC Service (SAMBA-LDAP PDC server)
        ADMIN$          IPC       IPC Service (SAMBA-LDAP PDC server)
        gsruser         Disk      Home Directories
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]

        Server               Comment
        ---------            -------
        TODOSCSI             SAMBA-LDAP PDC server

        Workgroup            Master
        ---------            -------
        GSRDOMAIN            TODOSCSI
```

El ejemplo anterior muestra los recursos compartidos que posee el servidor *TODOSCSI*. A continuación se va a acceder a uno de estos recursos para listar su contenido y realizar algunas operaciones dentro del mismo:

Ejemplo 11-6. Accediendo a un recurso compartido con smbclient

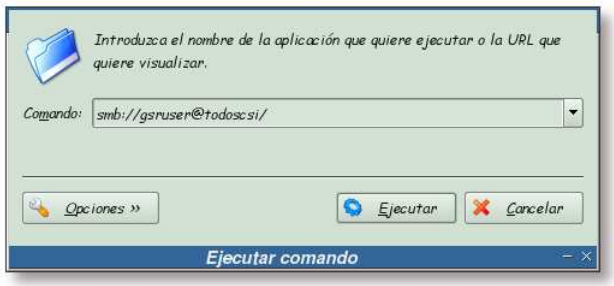
```
$ /bin/ls -la
total 56
drwxr-xr-x  3 gsruser domainusers  408 2004-10-09 13:38 .
drwxr-sr-x  3 root    staff         72 2004-10-09 13:38 ..
-rw-r--r--  1 gsruser domainusers 1363 2004-10-09 13:38 .bash_aliases
-rw-r--r--  1 gsruser domainusers  337 2004-10-09 13:38 .bash_logout
-rw-r--r--  1 gsruser domainusers  239 2004-10-09 13:38 .bash_profile
-rw-r--r--  1 gsruser domainusers 6198 2004-10-09 13:38 .bashrc
-rw-r--r--  1 gsruser domainusers   45 2004-10-09 13:38 .cvsrc
-rw-r--r--  1 gsruser domainusers  618 2004-10-09 13:38 .dir_colors
-rw-r--r--  1 gsruser domainusers  357 2004-10-09 13:38 .ldaprc
drwxr-xr-x  5 gsruser domainusers  120 2004-10-09 13:38 Maildir
-rw-r--r--  1 gsruser domainusers 4267 2004-10-09 13:38 .muttrc
-rw-r--r--  1 gsruser domainusers  105 2004-10-09 13:38 .procmailrc
-rw-r--r--  1 gsruser domainusers   87 2004-10-09 13:38 .screenrc
-rw-r--r--  1 gsruser domainusers  287 2004-10-09 13:38 .tidyrc
-rw-r--r--  1 gsruser domainusers 2686 2004-10-09 13:38 .vimrc
$ /usr/bin/smbclient  --user=gsruser //todoscsi/gsruser
Password: [clave]
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
smb: \> ls
  .                                   D        0  Sat Oct  9 13:38:52 2004
  ..                                  D        0  Sat Oct  9 13:38:52 2004
  .bashrc                             H     6198  Sat Oct  9 13:38:52 2004
  .ldaprc                             H      357  Sat Oct  9 13:38:52 2004
  .bash_logout                        H      337  Sat Oct  9 13:38:52 2004
  .muttrc                             H     4267  Sat Oct  9 13:38:52 2004
  .dir_colors                         H      618  Sat Oct  9 13:38:52 2004
  .tidyrc                             H      287  Sat Oct  9 13:38:52 2004
  .procmailrc                         H      105  Sat Oct  9 13:38:52 2004
  .bash_aliases                       H     1363  Sat Oct  9 13:38:52 2004
  Maildir                             D        0  Sat Oct  9 13:38:52 2004
  .cvsrc                              H       45  Sat Oct  9 13:38:52 2004
  .vimrc                              H     2686  Sat Oct  9 13:38:52 2004
  .screenrc                           H       87  Sat Oct  9 13:38:52 2004
  .bash_profile                       H      239  Sat Oct  9 13:38:52 2004

                43910 blocks of size 524288. 1201 blocks available
smb: \> mkdir directorio-de-ejemplo
smb: \> ls
  .                                   D        0  Sat Oct  9 13:45:39 2004
  ..                                  D        0  Sat Oct  9 13:38:52 2004
  .bashrc                             H     6198  Sat Oct  9 13:38:52 2004
  .ldaprc                             H      357  Sat Oct  9 13:38:52 2004
  directorio-de-ejemplo               D        0  Sat Oct  9 13:45:39 2004
  .bash_logout                        H      337  Sat Oct  9 13:38:52 2004
  .muttrc                             H     4267  Sat Oct  9 13:38:52 2004
  .dir_colors                         H      618  Sat Oct  9 13:38:52 2004
  .tidyrc                             H      287  Sat Oct  9 13:38:52 2004
  .procmailrc                         H      105  Sat Oct  9 13:38:52 2004
  .bash_aliases                       H     1363  Sat Oct  9 13:38:52 2004
```

```
  Maildir                             D        0  Sat Oct  9 13:38:52 2004
  .cvsrc                              H       45  Sat Oct  9 13:38:52 2004
  .vimrc                              H     2686  Sat Oct  9 13:38:52 2004
  .screenrc                           H       87  Sat Oct  9 13:38:52 2004
  .bash_profile                       H      239  Sat Oct  9 13:38:52 2004

                43910 blocks of size 524288. 1201 blocks available
smb: \> exit
~$ /bin/ls -la
total 56
drwxr-xr-x    3 gsruser  domainusers      336 2004-06-01 12:27 ./
drwxr-xr-x    3 root     root            72 2004-05-31 02:46 ../
-rw-r--r--    1 gsruser  domainusers     1,4K 2004-05-31 02:46 .bash_aliases
-rw-r--r--    1 gsruser  domainusers      337 2004-05-31 02:46 .bash_logout
-rw-r--r--    1 gsruser  domainusers      239 2004-05-31 02:46 .bash_profile
-rw-r--r--    1 gsruser  domainusers     6,3K 2004-05-31 02:46 .bashrc
-rw-r--r--    1 gsruser  domainusers       45 2004-05-31 02:46 .cvsrc
-rw-r--r--    1 gsruser  domainusers      618 2004-05-31 02:46 .dir_colors
drwx------    2 gsruser  domainusers       48 2004-06-01 12:27 directorio-de-ejemplo/
-rw-r--r--    1 gsruser  domainusers     4,3K 2004-05-31 02:46 .muttrc
-rw-r--r--    1 gsruser  domainusers      287 2004-05-31 02:46 .tidyrc
-rw-r--r--    1 gsruser  domainusers     2,7K 2004-05-31 02:46 .vimrc
$ /bin/rmdir -v directorio-de-ejemplo
rmdir: borrando el directorio, directorio-de-ejemplo/
```

Uso de konqueror

En esta sección se verá la forma de acceso a los recursos compartidos mediante Samba con konqueror. Las siguientes capturas de pantalla muestran los pasos para conseguirlo:

Figura 11-23. Dirección de acceso a los recursos de Samba



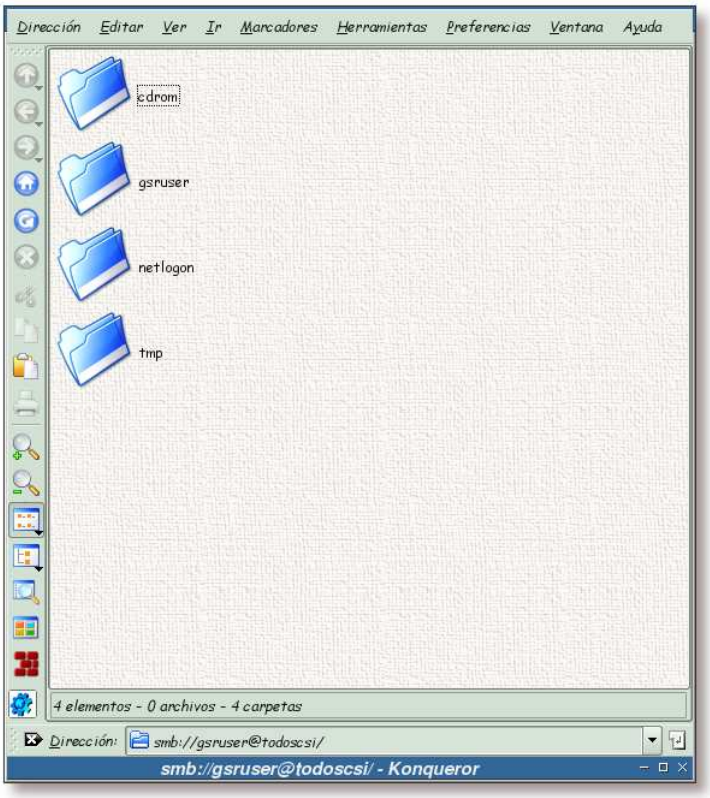
Konqueror permite el acceso a los recursos compartidos desde un servidor samba; para ello hay que teclear direcciones del tipo: *smb://usuario@SERVIDOR-SAMBA/*.

En este caso, se va a acceder al servidor “TODOSCSI” con el usuario “gsruser”.

Figura 11-24. Clave del usuario *gsruser*

En esta pantalla se ha de teclear la clave para el usuario gsruser.

Figura 11-25. Recursos compartidos



En esta pantalla se muestran los recursos compartidos. El directorio `gsruser` se corresponde con el directorio Home del usuario *gsruser*.

Capítulo 12. Añadiendo clientes al dominio

Introducción

Este capítulo se ha realizado gracias a las entradas bibliográficas: Syroid02 y Milne02. En la elaboración de esta documentación no se ha tenido acceso a ningún cliente Windows para la realización de pruebas, por lo tanto, todo lo que se expone en este capítulo es teórico.

Windows 95/98/ME

Los clientes Windows 9x no tienen implementada completamente la función de miembro de dominio, por este motivo es fácil unirlos a un dominio. Los pasos que se han de seguir para añadir a un cliente de este tipo a un dominio son:

1. Primero se ha de comprobar que el *Cliente para Redes Microsoft* está instalado; si no lo está, instálelo (Panel de Control -> Red -> Cliente para Redes Microsoft). Para instalarlo, coloque el CD de Windows en la unidad de CDROM y seleccione *Añadir* desde el antes mencionado cuadro de diálogo, luego: Cliente -> Añadir... -> Microsoft -> Cliente para Redes Microsoft.
2. Asegúrese de que el *Cliente para Redes Microsoft* es el protocolo de red primario (Panel de Control -> Red -> Autentificación de Red Primaria).
3. El siguiente paso es: Panel de Control -> Red -> Cliente para Redes Microsoft -> Propiedades -> Autentificarse en un Dominio NT.
4. Si ha hecho uso de la opción *add user script* en el archivo de configuración de Samba, seleccione el *checkbox Crear una Cuenta de Máquina en el Dominio*; Si no ha sido así, se ha de asegurar que la cuenta de la máquina existe para el cliente.
5. Complete el dominio y pulse sobre *Aceptar*

Windows NT

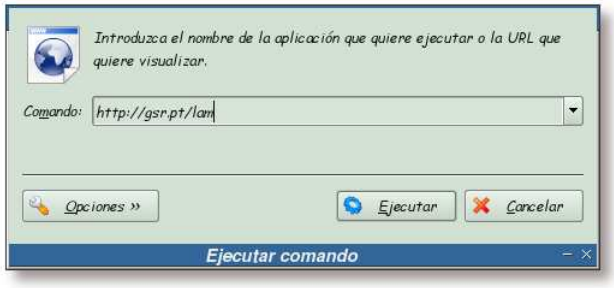
Los clientes Windows NT tienen una implementación completa de dominio, y mejor seguridad por defecto. Cada máquina posee su propia clave, que controla que máquina puede autentificarse desde el dominio. Todas estas máquinas necesitan su propia entrada en el archivo “smbpassswd” (o en el directorio LDAP).

Hay que diferenciar entre cuentas de usuario y de máquina: las cuentas de máquina son diferentes a las de usuario por terminar en el símbolo *$*. Para los clientes Windows NT puede crear estas cuentas manualmente. Vea el la sección de nombre *Windows 2000* para saber como hacer esto más sencillamente.

Creación de cuentas para las máquinas

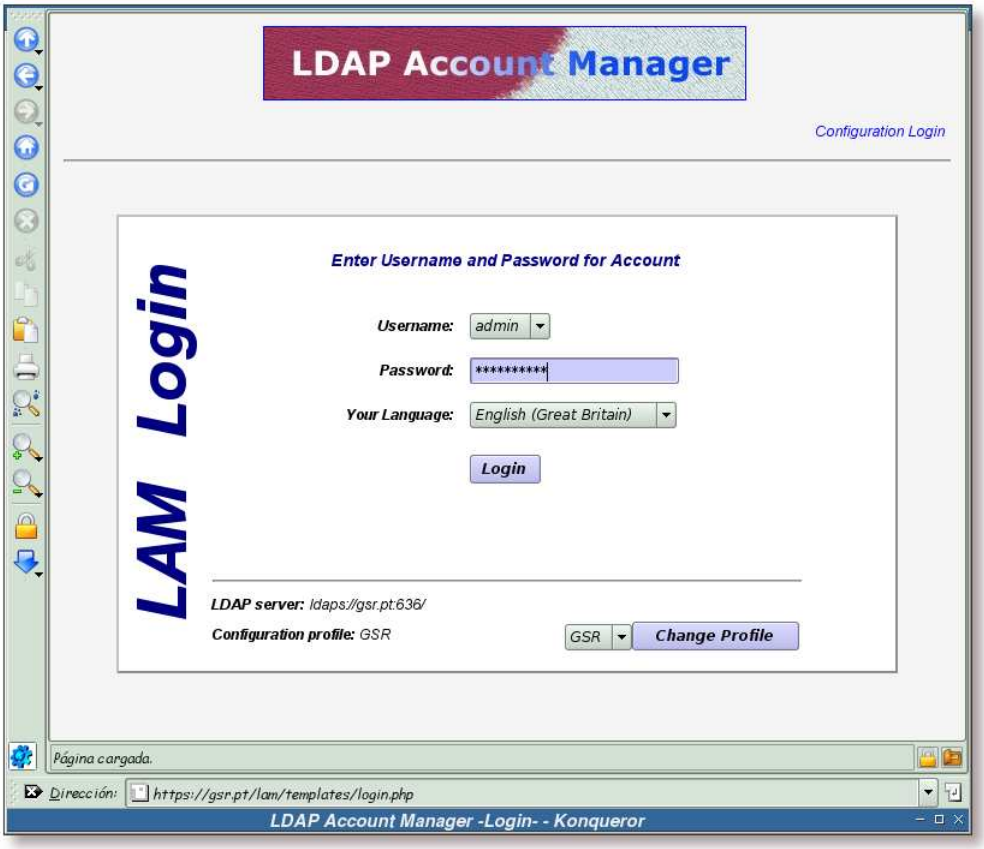
La forma de añadir cuentas de máquina en Samba se detalla en las siguientes capturas de pantalla:

Figura 12-1. Acceso a la herramienta LDAP Account Manager



Si se encuentra en un entorno de escritorio con KDE, teclee **Alt**+**F2** e introduzca la dirección donde se encuentre instalado LAM.

Figura 12-2. Ingreso en LAM



Si en estos momentos no tiene un perfil creado para LAM, vea el Apéndice F para saber como hacerlo.

Una vez creado el perfil personalizado, seleccionelo y pulse sobre *Change Profile*. Una vez seleccionado el perfil adecuado, se ha de teclear la clave del administrador del directorio LDAP y pulsar sobre *Login*.

Figura 12-3. Sección *Hosts*

Tras el ingreso en la herramienta, se ha de pulsar sobre el enlace *Hosts* para proceder con la adición de una cuenta de máquina.

Figura 12-4. Crear nueva máquina

Cuando se ha cargado la sección de hosts, se pulsa sobre el botón *New Host* para comenzar el proceso.

Figura 12-5. Completado de los campos

En esta pantalla se completan los campos *Host name* y *Gecos* con el nombre de la máquina y una descripción de la misma, respectivamente.

Una vez realizado esto, se pulsa sobre el botón *Create Account*.

Figura 12-6. Corrección de los “errores” cometidos

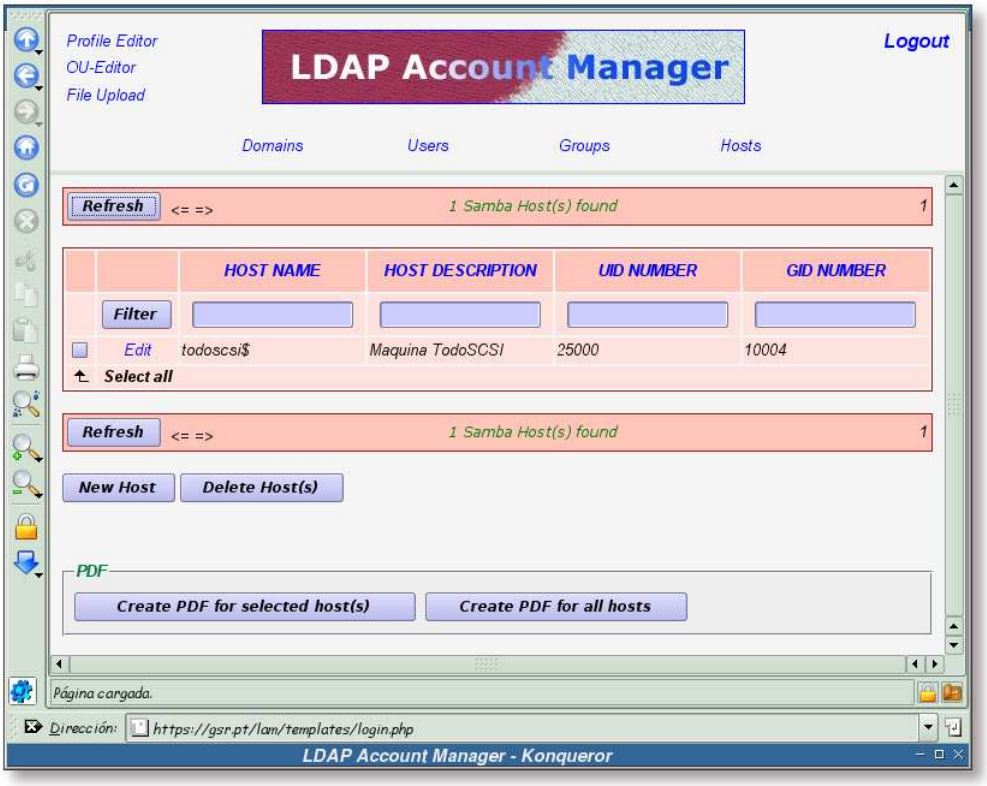
Antes de la creación de la cuenta, LAM detecta y trata de corregir los posibles errores cometidos. En este caso no se ha tecleado el nombre del host de forma correcta, pues tiene que terminar en el signo *$* (LAM lo ha introducido automáticamente) y se ha dejado en blanco el campo *UID number*, el cual rellena LAM de forma automática.

Se vuelve a pulsar sobre el botón *Create Account* para finalizar la creación de la cuenta.

Figura 12-7. Cuenta creada

LAM informa de la creación de la cuenta para la máquina y propone una serie de acciones. Pulse sobre el botón *Back to hosts list*.

Figura 12-8. Lista de Hosts

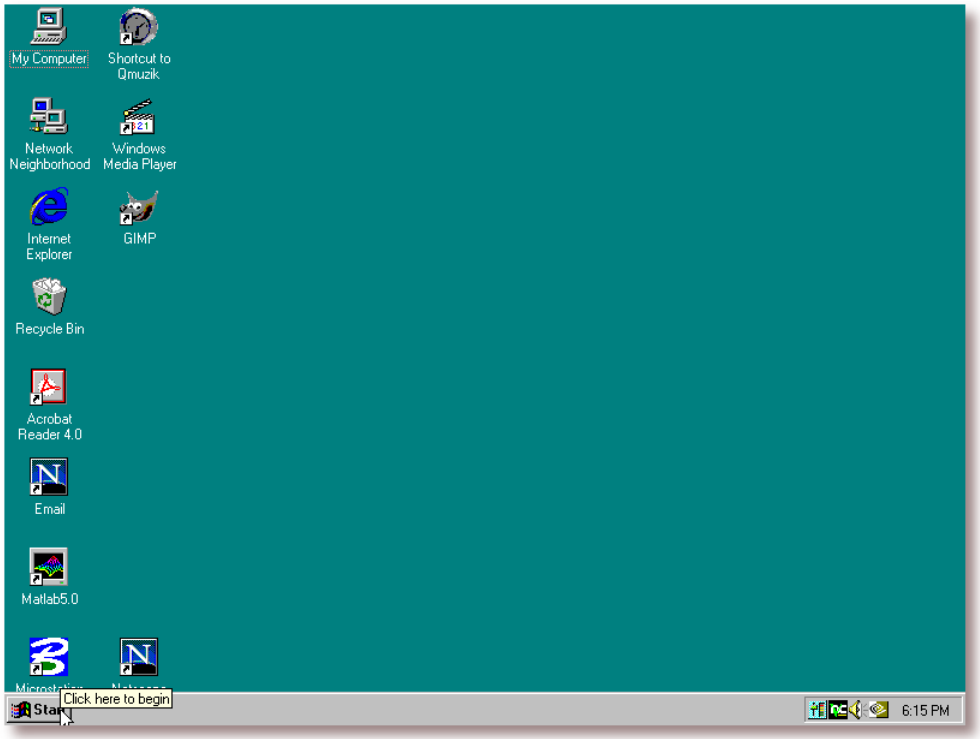


Ahora aparece, en la lista de hosts, la nueva cuenta creada.

Uniendo un cliente Windows NT a un dominio

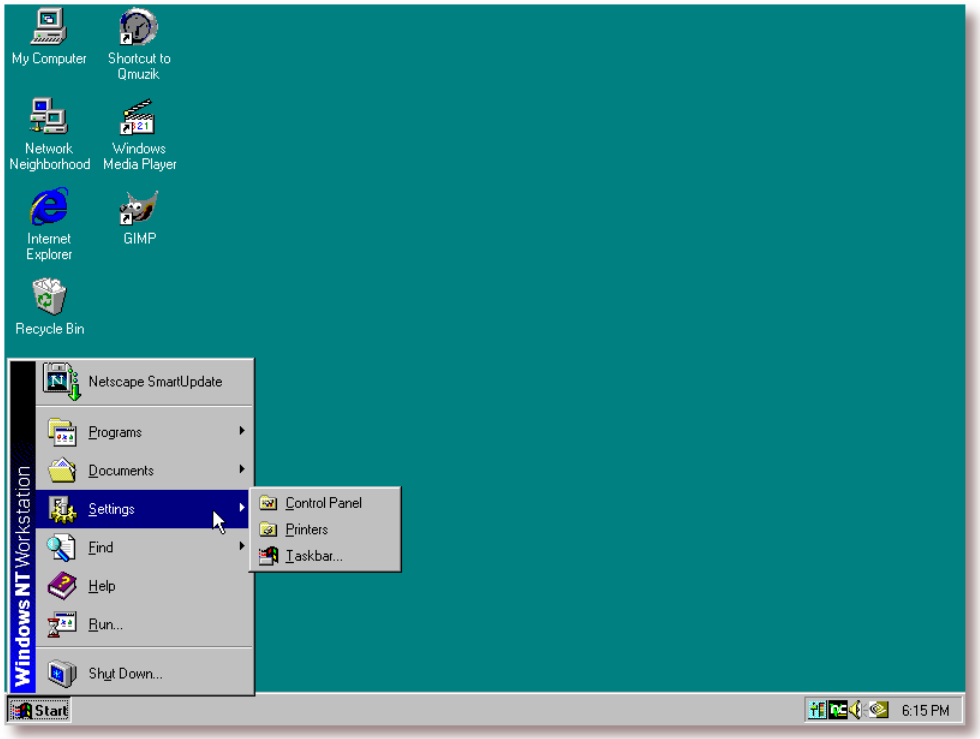
Los pasos que se muestran a continuación son los que se han de seguir para añadir un cliente Windows NT a un dominio:

Figura 12-9. “Inicio”



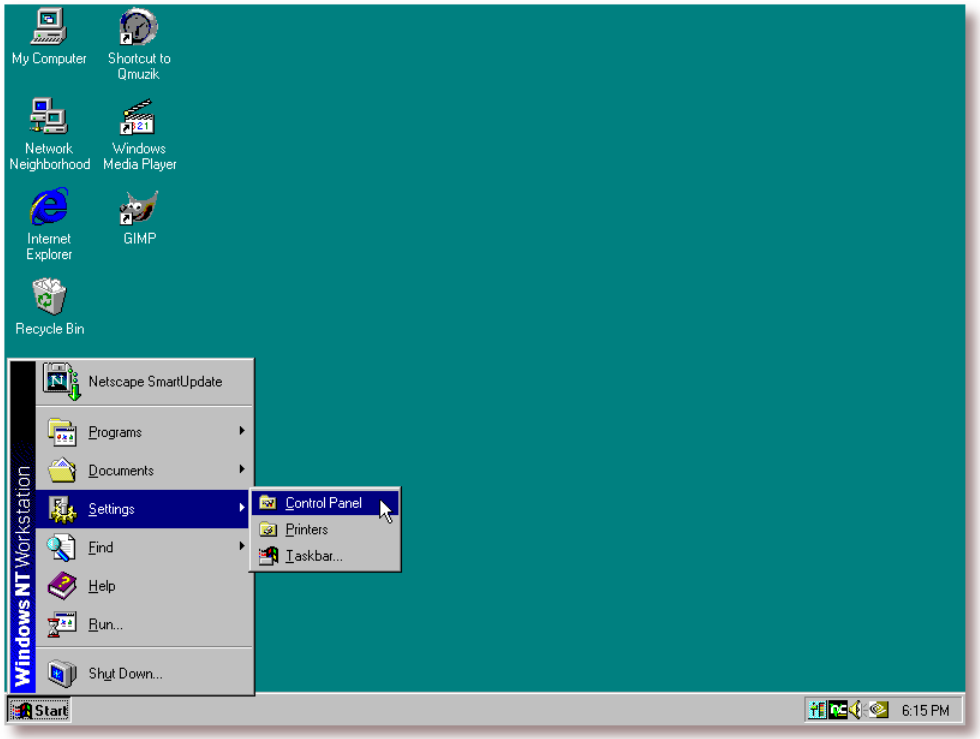
Se comienza el proceso con la pulsación sobre el botón “Inicio”.

Figura 12-10. “Configuración”



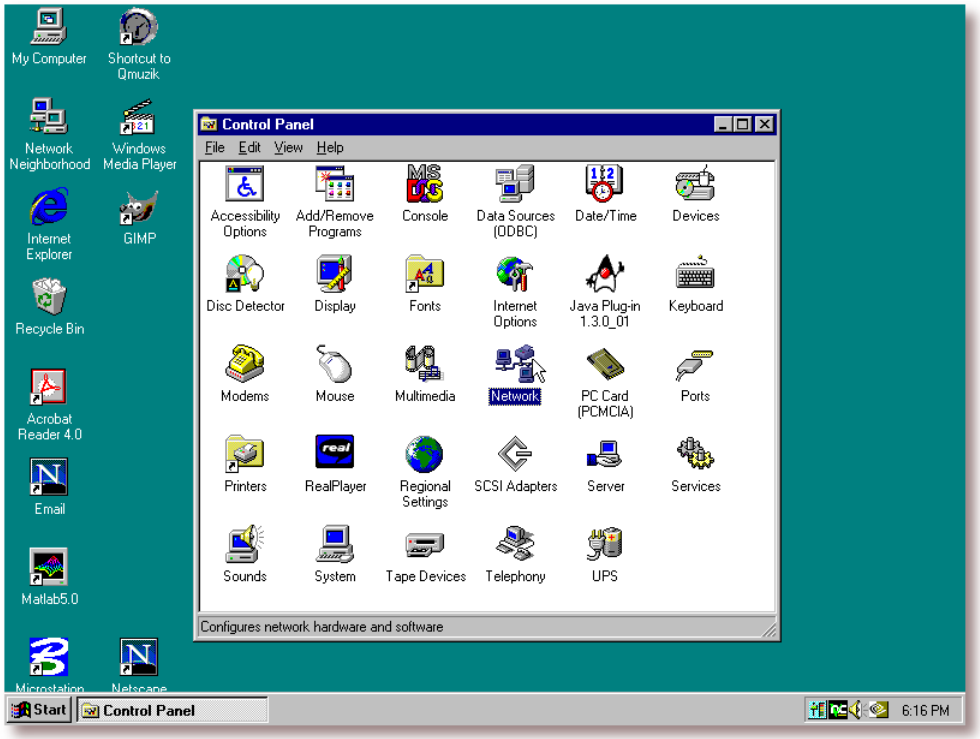
Se selecciona el menú “Configuración”.

Figura 12-11. “Panel de Control”



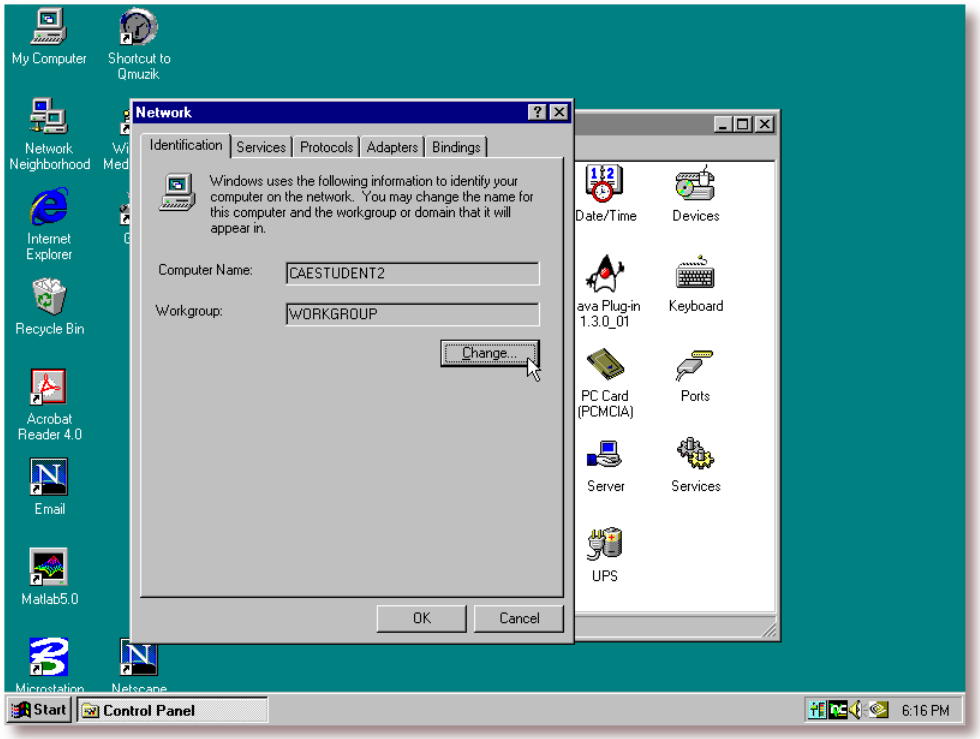
Luego la opción “Panel de Control”.

Figura 12-12. “Red”



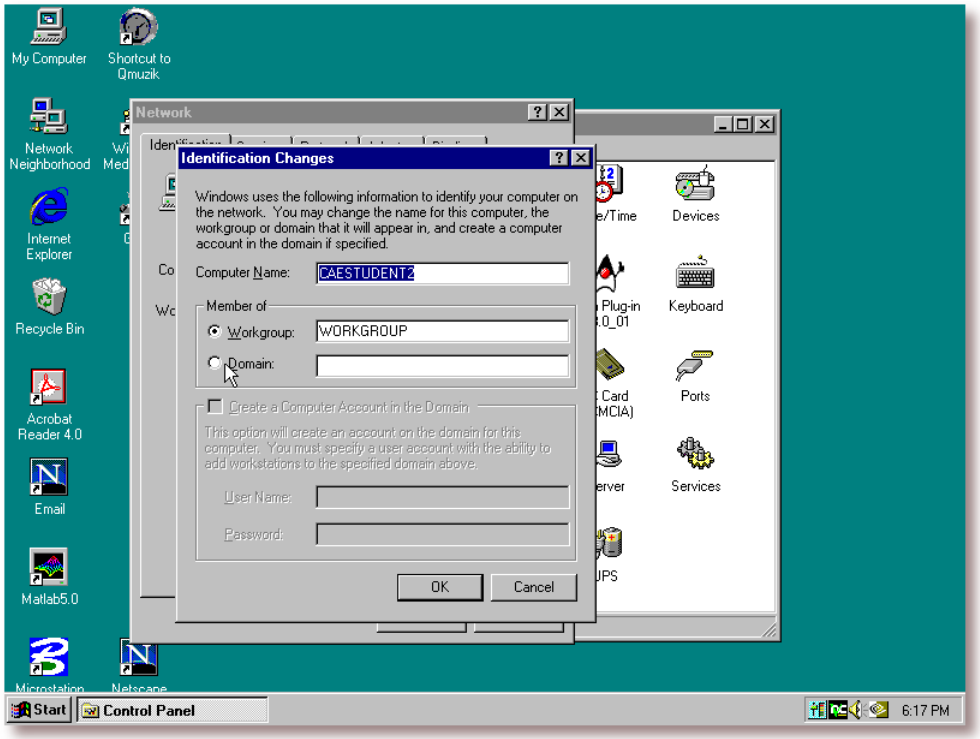
Abierta la ventana del *Panel de Control*, se hace doble clic sobre el icono de “Red”.

Figura 12-13. Cuadro de diálogo “Red”



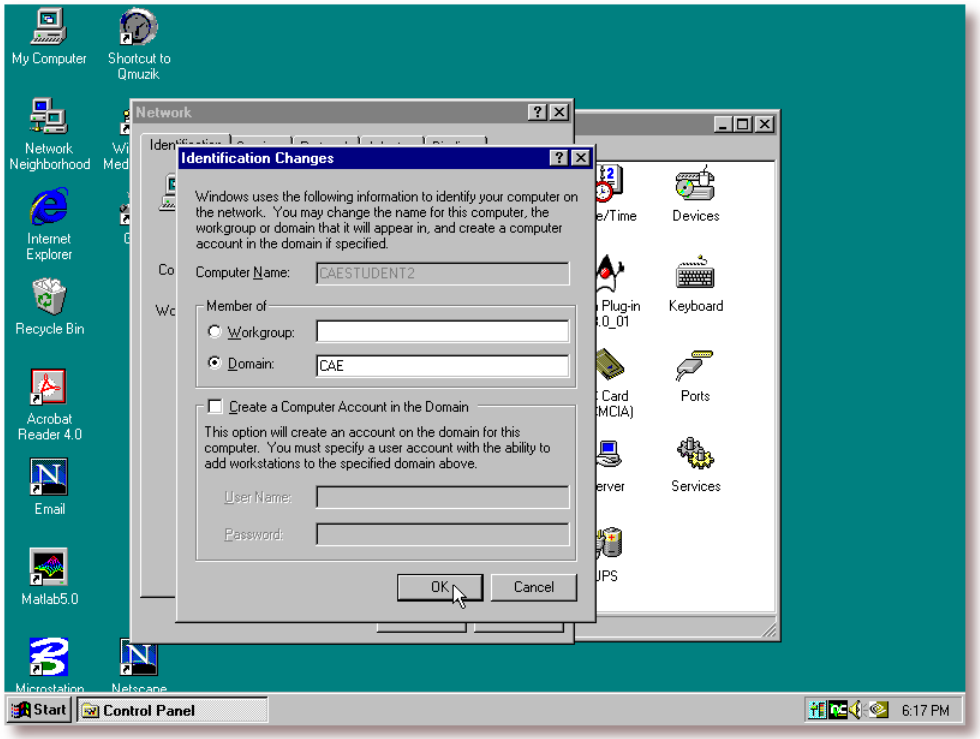
Se pulsa sobre el botón “Cambiar...” que aparece en el cuadro de diálogo de *Red*.

Figura 12-14. Miembro de dominio



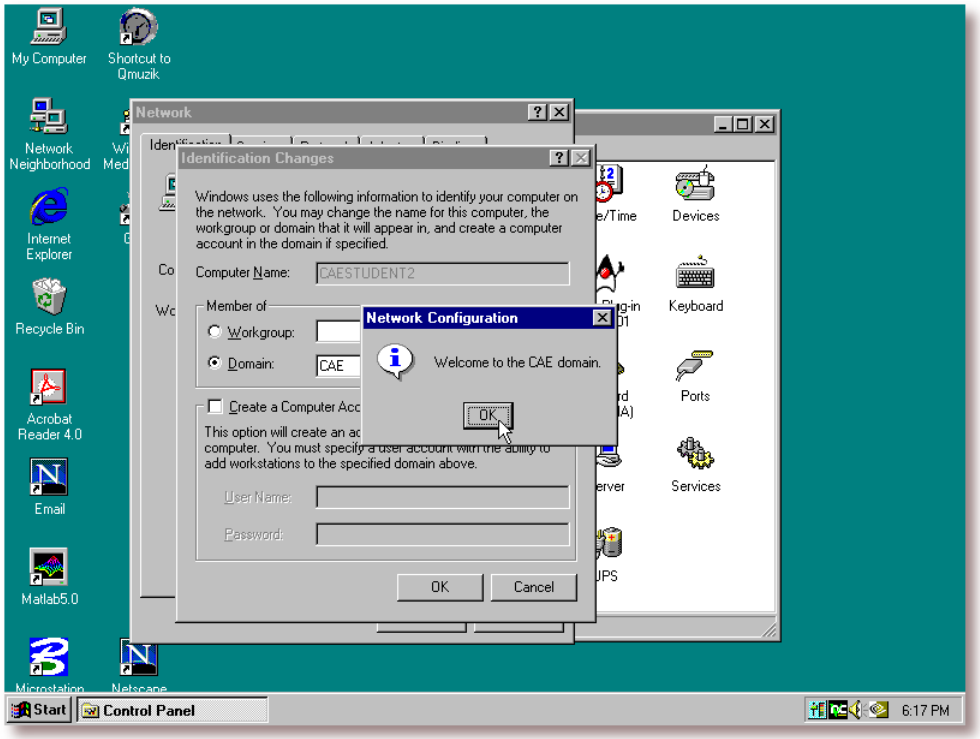
Se selecciona la opción de *Miembro de* “dominio”.

Figura 12-15. Nombre del dominio



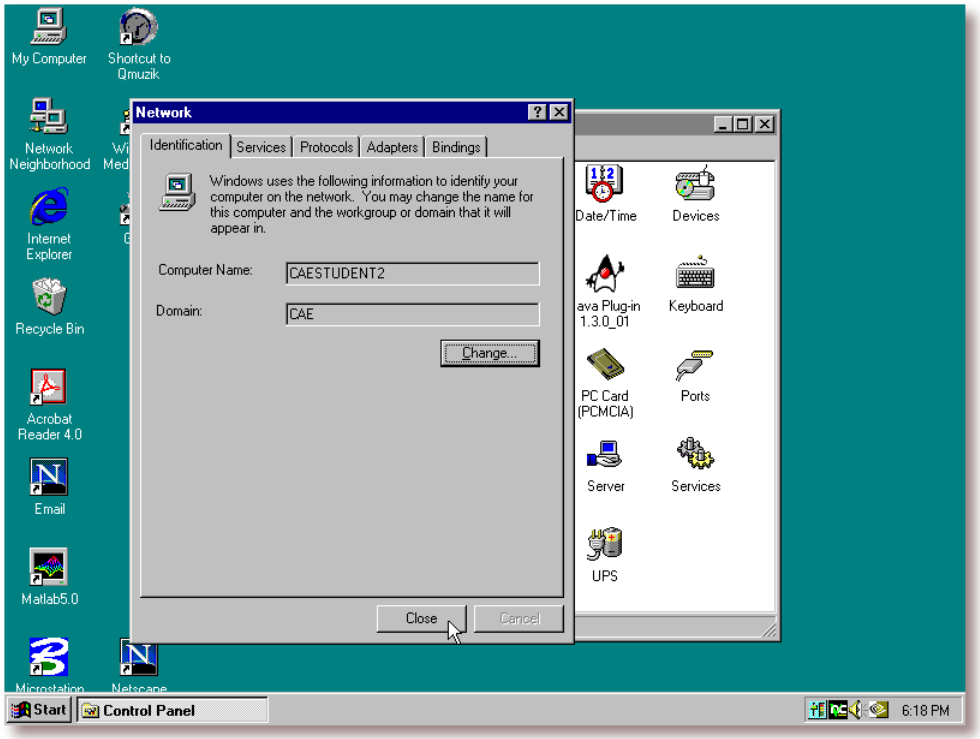
Se completa el campo “dominio” con nombre del dominio al cual se quiere añadir el cliente y se pulsa sobre el botón *Aceptar*.

Figura 12-16. Bienvenida



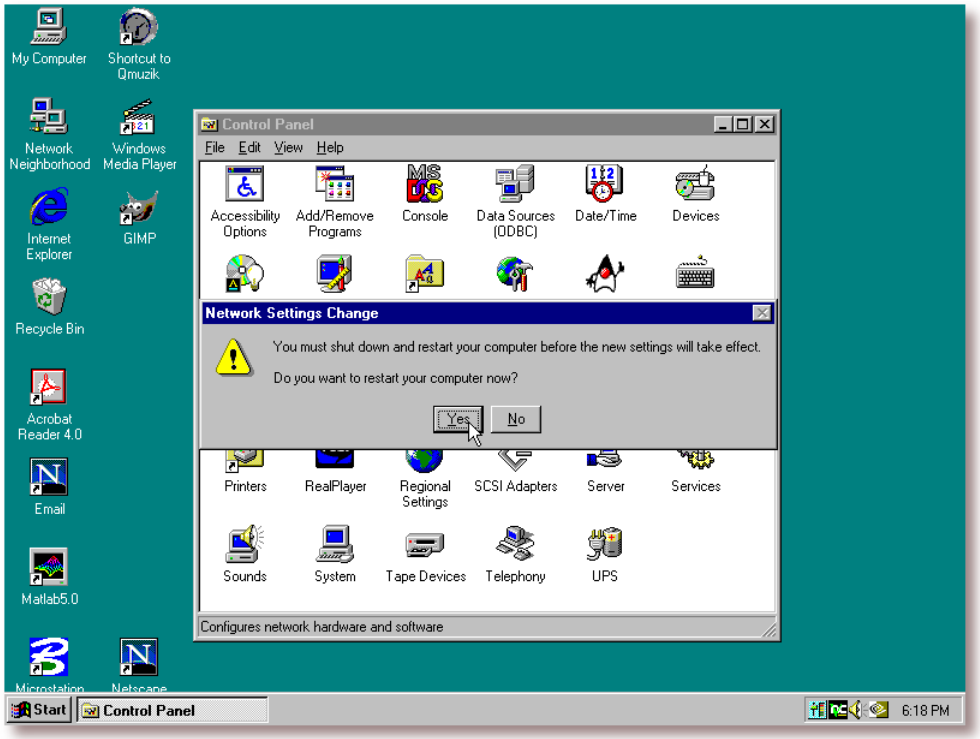
Se da la bienvenida al nuevo dominio; pulse sobre el botón *Aceptar* para continuar.

Figura 12-17. Cierre del cuadro de diálogo “Red”



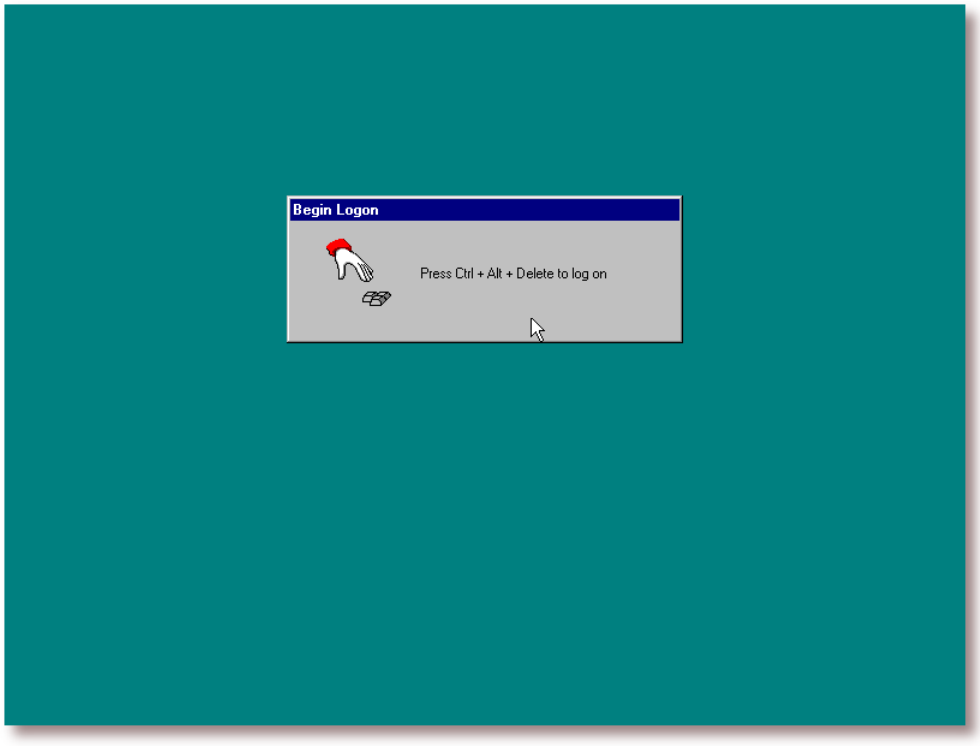
Pulse sobre el botón “Cerrar” para cerrar el cuadro de diálogo “Red”.

Figura 12-18. Reinicio del sistema



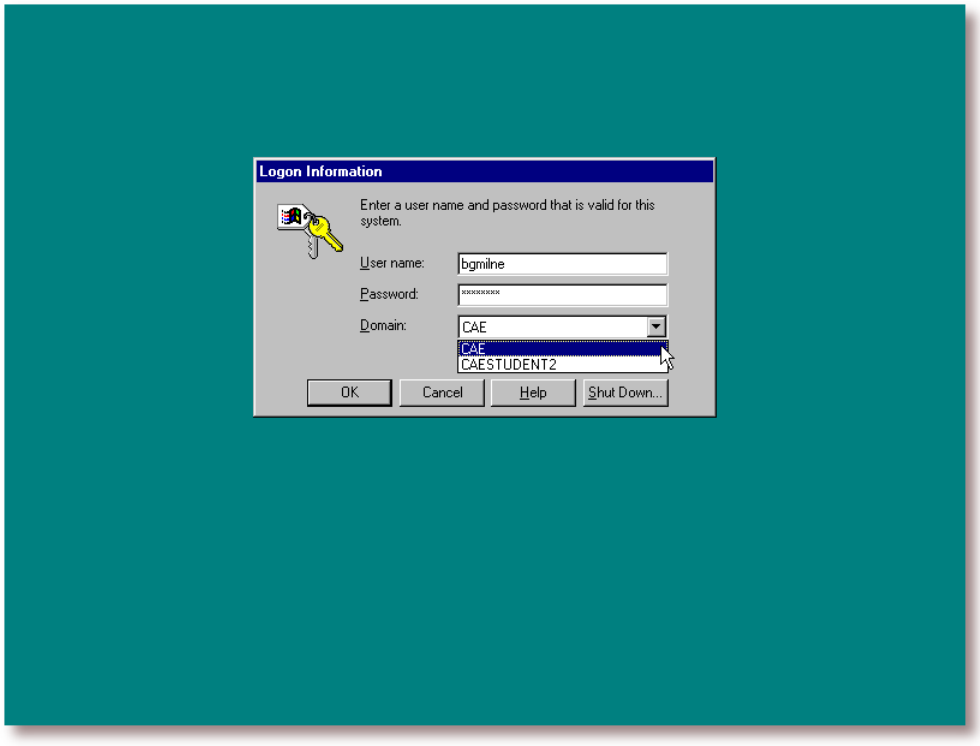
Se sugiere un reinicio del sistema para que los cambios tengan efecto, se pulsa sobre el botón “Sí” para continuar.

Figura 12-19. Ctrl+Alt+Supr



Se pulsa la combinación de teclas: **Ctrl**+**Alt**+**Supr** para poder iniciar una nueva sesión en el sistema.

Figura 12-20. Selección del nuevo dominio



En el cuadro de diálogo de ingreso en el sistema, se selecciona el dominio al cual se acaba de añadir al cliente Windows NT y se teclea una cuenta válida en el dominio para proceder con el ingreso.

Windows 2000

Windows 2000 es ligeramente diferente de Windows NT. Si se añade una máquina Windows NT a la red, como se ha visto en la sección anterior (la sección de nombre *Windows NT*), habrá notado un *checkbox* con la leyenda: “Crear una cuenta para esta máquina en el dominio”, que no se ha utilizado. Esta opción permite la creación de cuentas de máquina “al vuelo”; esta es la única forma de unir un cliente Windows 2000 a un dominio.

En la la sección de nombre *[global] - Misceláneo* en Capítulo 9 se mostró la opción *add user script*, que permitía añadir cuentas de máquina automáticamente a Samba. Esta opción es necesaria para poder añadir a los clientes Windows 2000 al dominio.

Añadiendo el usuario “root” a Samba

De momento, el único usuario que puede crear cuentas automáticamente es el usuario “root”. Esto significa que ha de hacer un “smbpasswd” (como el usuario “root”) para el usuario “root”. El siguiente

ejemplo muestra como hacerlo:

Ejemplo 12-1. Estableciendo la clave de root en Samba

```
# /usr/bin/smbpasswd -a
New SMB password: [clave]
Retype new SMB password: [clave]
Added user root.
```

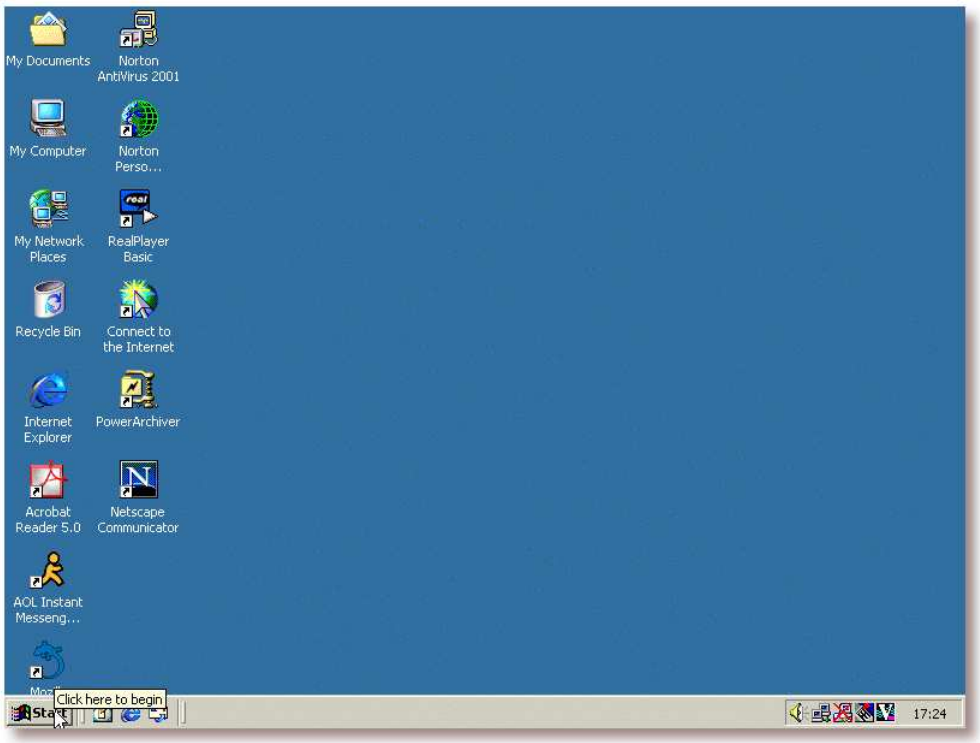
Sugerencia: Se sugiere utilizar una clave diferente a la del usuario “root” del sistema Linux por cuestiones de seguridad.

Nota: Tal vez sea necesario comentar la línea “invalid users = root” del archivo de configuración de Samba, para permitir al usuario *root* añadir los clientes MS Windows al dominio.

Uniendo un cliente Windows 2000 a un dominio

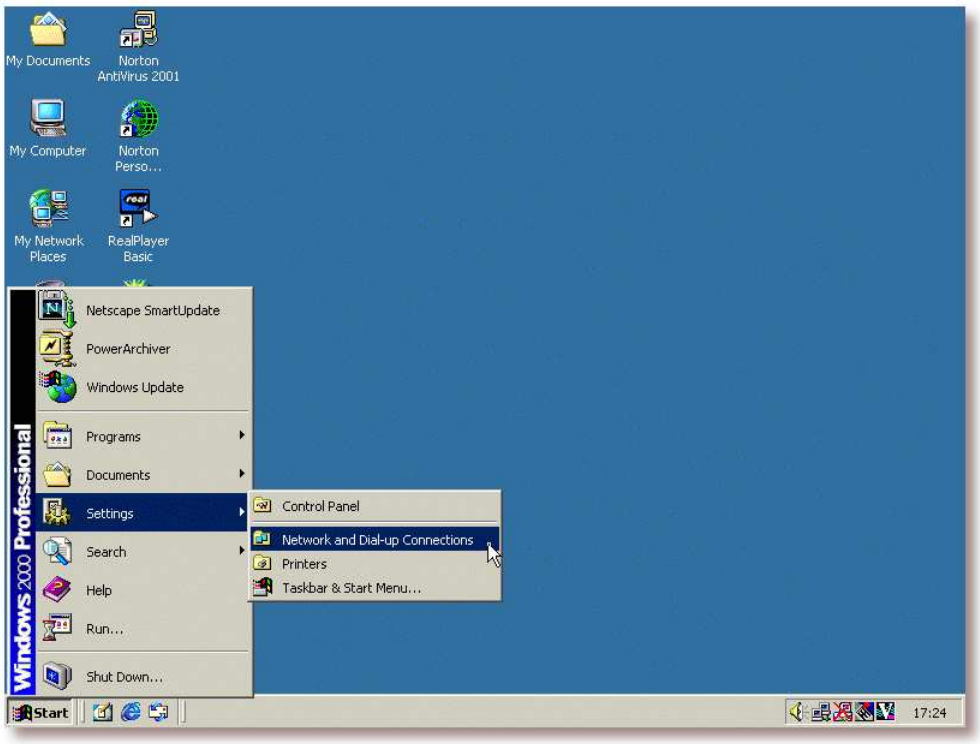
Ha de seguir los siguientes pasos para añadir un cliente Windows 2000 a un dominio:

Figura 12-21. “Inicio”



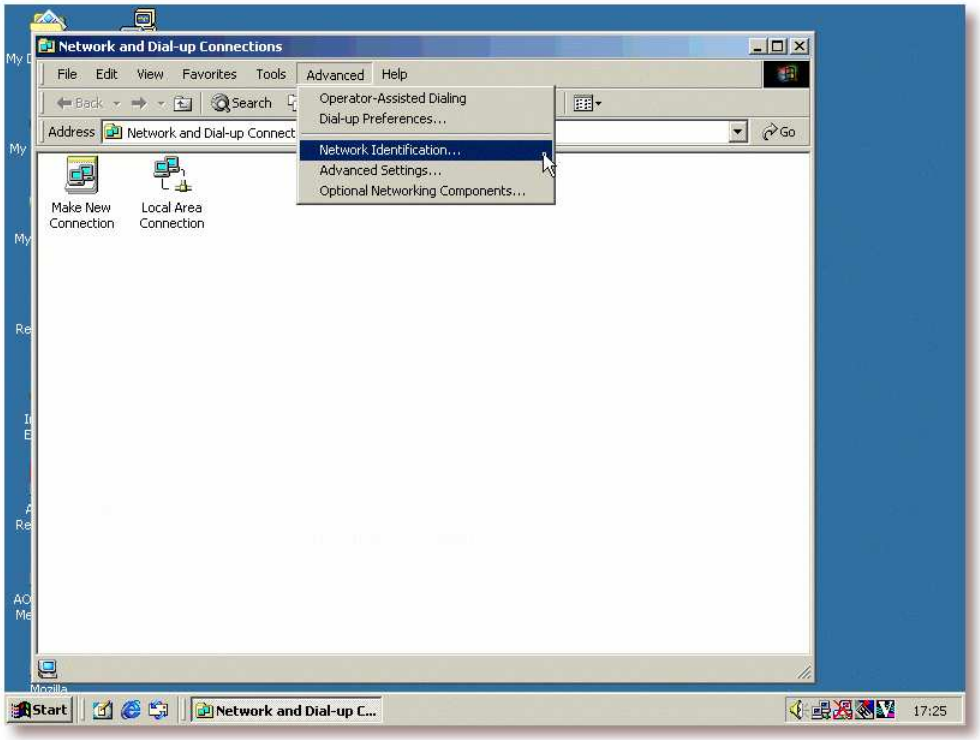
Se comienza el proceso con la pulsación sobre el botón “Inicio”:

Figura 12-22. “Conexiones de Red”



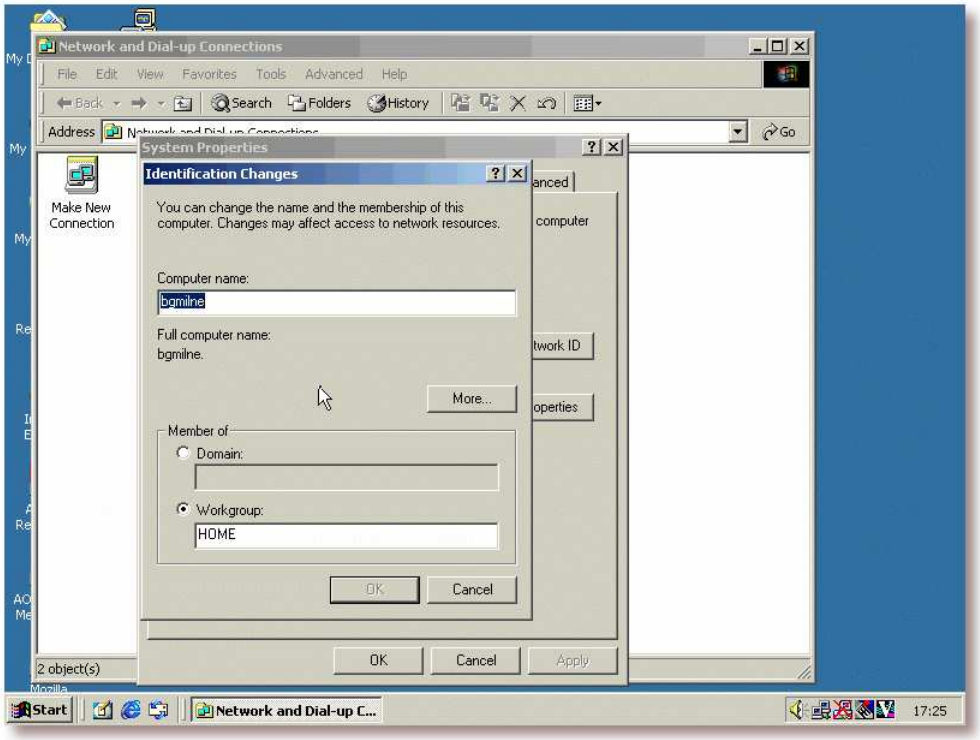
Se pulsa sobre la opción “Conexiones de Red” (Configuración -> Conexiones de Red).

Figura 12-23. “Identificación de Red”



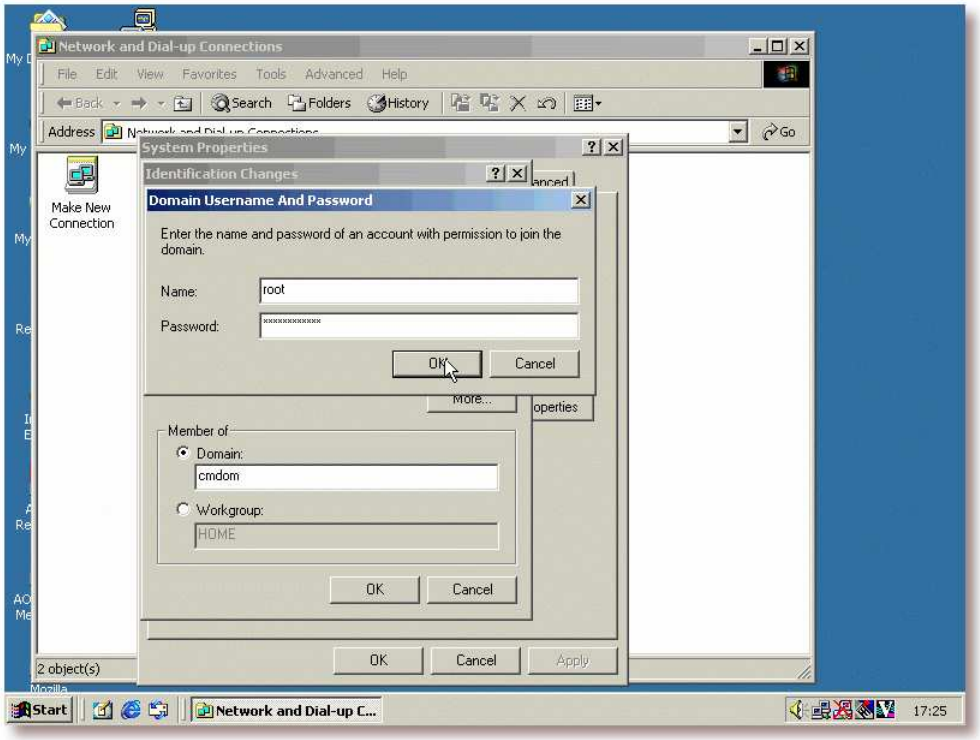
Sobre la ventana de *Conexiones de Red*, se pulsa sobre el menú “Avanzado” y luego sobre la entrada: “Identificación de Red”

Figura 12-24. Selección del dominio



Se pulsa sobre el botón “Propiedades” del cuadro de diálogo *Propiedades del Sistema*. En la ventana resultante de la acción anterior, se pulsa sobre la opción “Dominio” y se teclea el nombre del dominio al cual se quiere añadir el cliente Windows 2000. Para finalizar, se pulsa sobre el botón *Aceptar*.

Figura 12-25. Cuenta para añadir la máquina al dominio

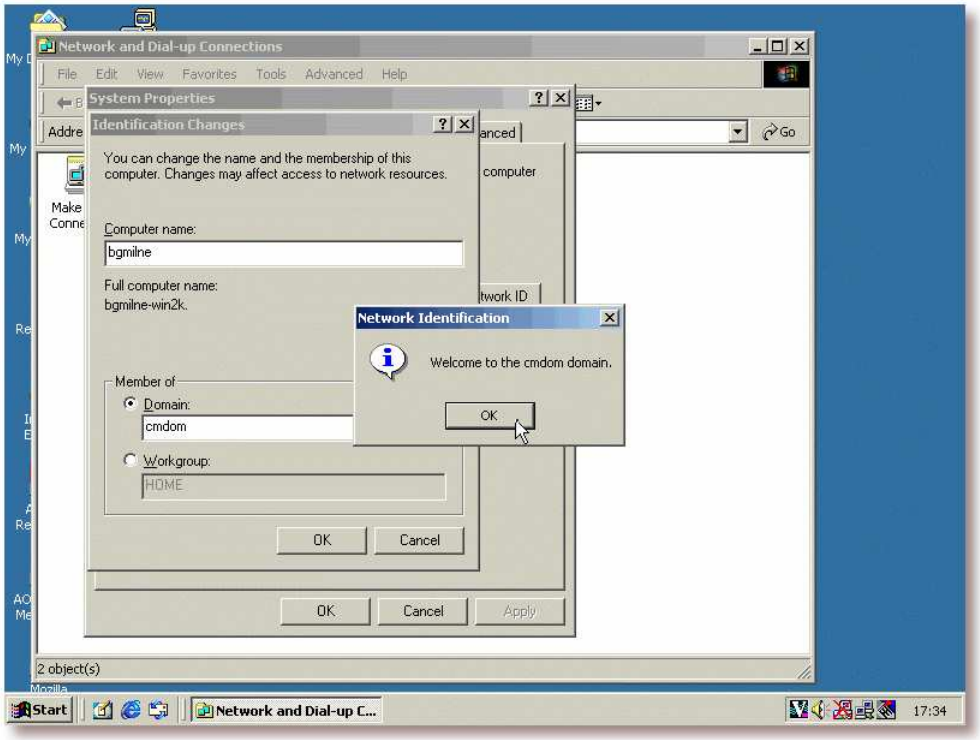


La acción anterior tendrá como consecuencia la apertura de una ventana, en la que se solicita una cuenta de dominio que tenga permisos suficientes para añadir una máquina al dominio.

La cuenta que se ha de utilizar es la creada en
la sección de nombre *Añadiendo el usuario "root" a Samba*, es decir, la cuenta "root".

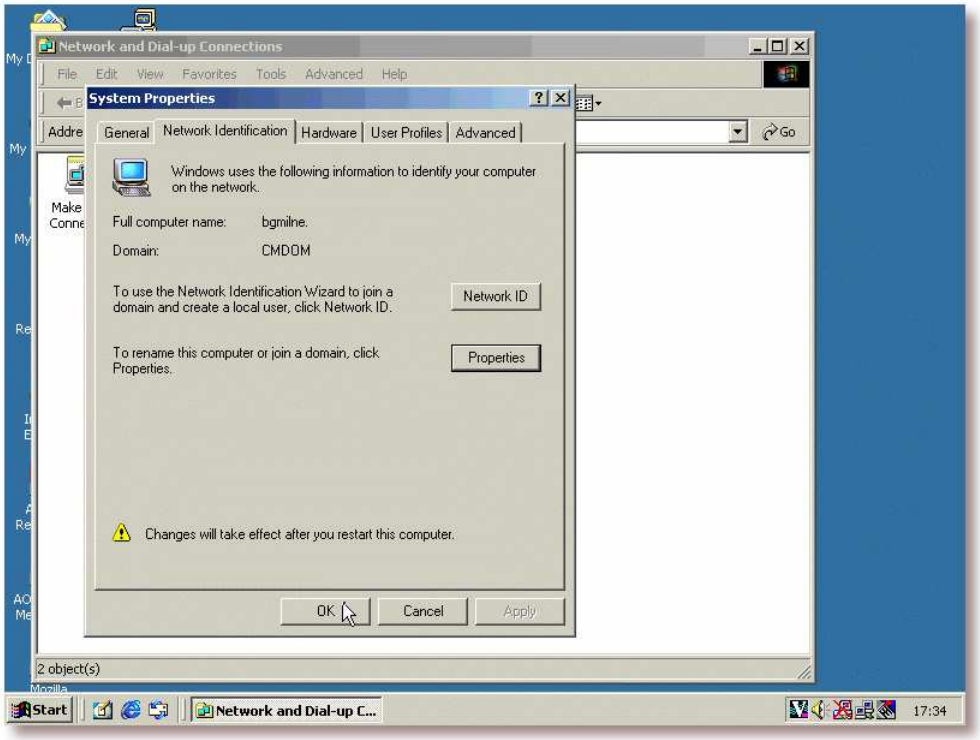
Pulse sobre el botón *Aceptar* una vez se han completado los datos necesarios.

Figura 12-26. Bienvenida al dominio



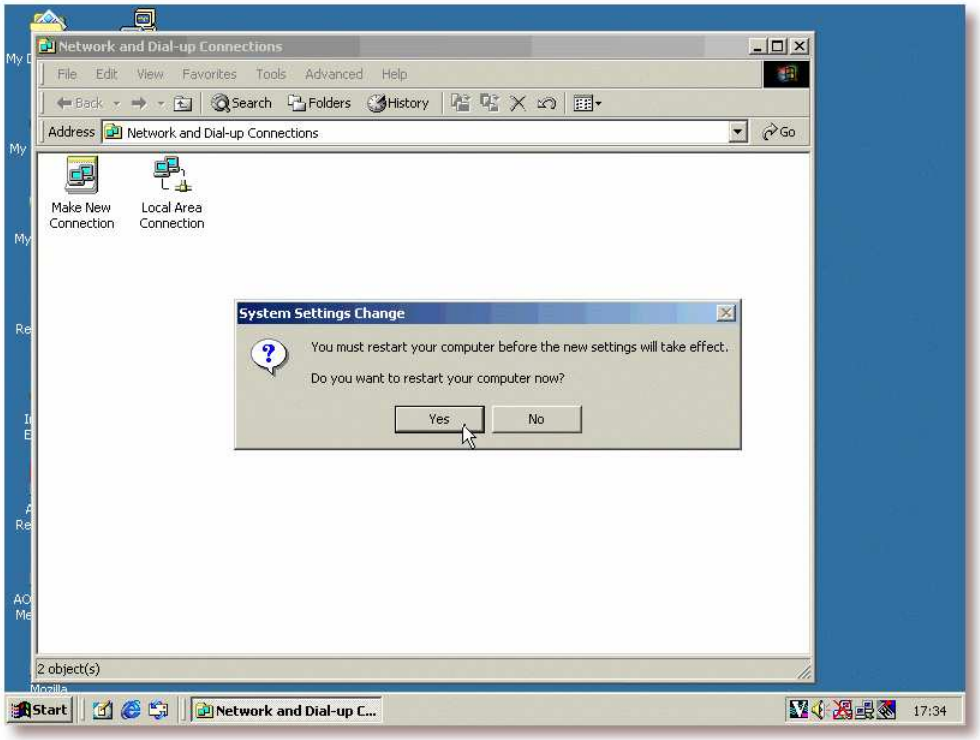
Una vez se ha añadido el cliente al dominio, se da la bienvenida al mismo. Pulse sobre el botón *Aceptar* para continuar.

Figura 12-27. Preparándose para el reinicio



Una vez recibida la bienvenida, se pulsa sobre el botón *Aceptar* del cuadro de diálogo *Propiedades del Sistema*.

Figura 12-28. Solicitud de reinicio



Para que los cambios tengan efecto, se ha de reiniciar el sistema. Pulse en el botón *Aceptar* para proceder con el reinicio.

Figura 12-29. Ctrl+Alt+Supr

Se pulsa la combinación de teclas: **Ctrl**+**Alt**+**Supr** para poder iniciar una nueva sesión en el sistema.

Figura 12-30. Selección del nuevo dominio

En el cuadro de diálogo de ingreso en el sistema, se selecciona el dominio al cual se acaba de añadir al cliente Windows 2000.

Figura 12-31. Cuenta de dominio

Se teclean un usuario y una clave válidos en el dominio y se pulsa sobre *Aceptar*.

Figura 12-32. Entrando en el sistema

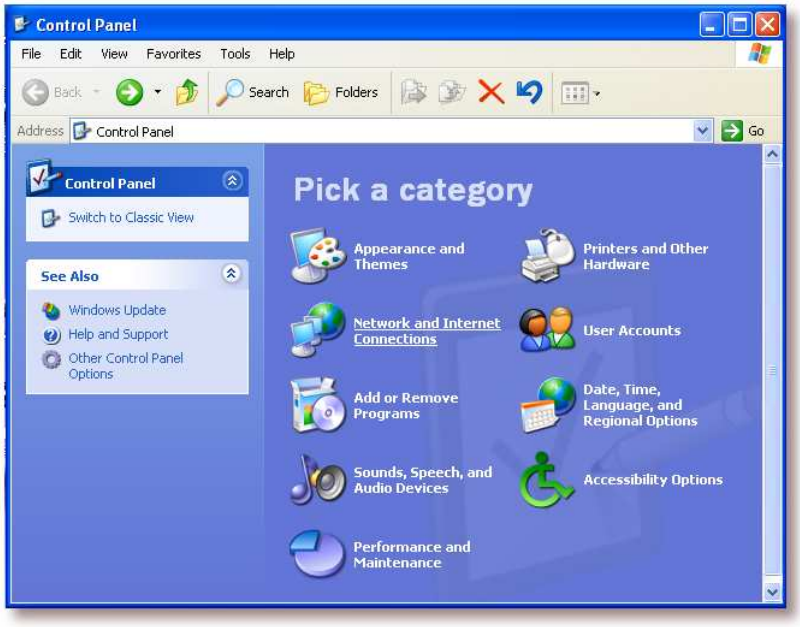
Si todo ha ido bien, el siguiente paso es la entrada al sistema.

Windows XP

Para poder añadir a un cliente Windows XP a un dominio manejado por Samba, se ha de realizar un cambio en el registro de Windows. En el Apéndice J se muestra el cambio a realizar.

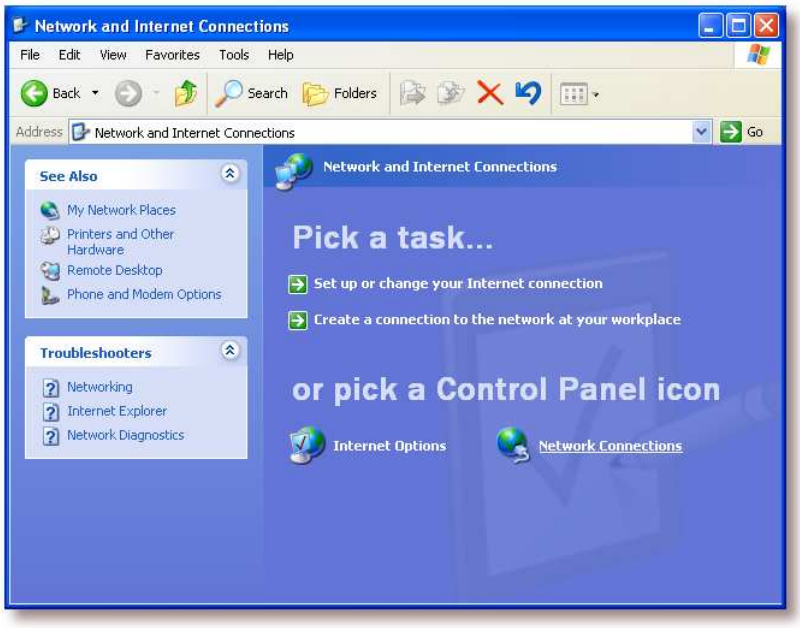
Una vez aplicado el cambio en el registro, siga los siguientes pasos para añadir al cliente Windows XP al dominio:

Figura 12-33. Conexiones de Red e Internet



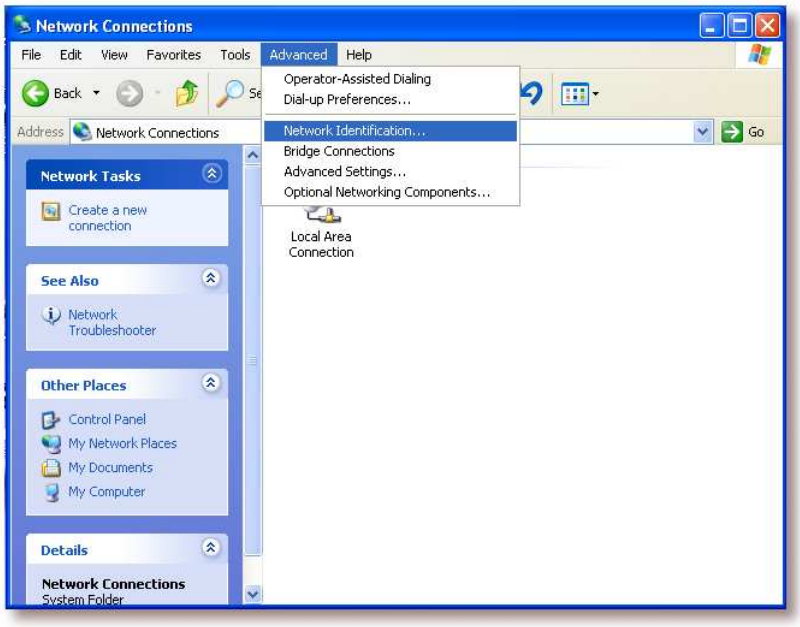
Acceda a la opción “Conexiones de Red e Internet” del *Panel de Control* (Inicio -> Configuración -> Panel de Control -> Conexiones de Red e Internet).

Figura 12-34. Conexiones de Red



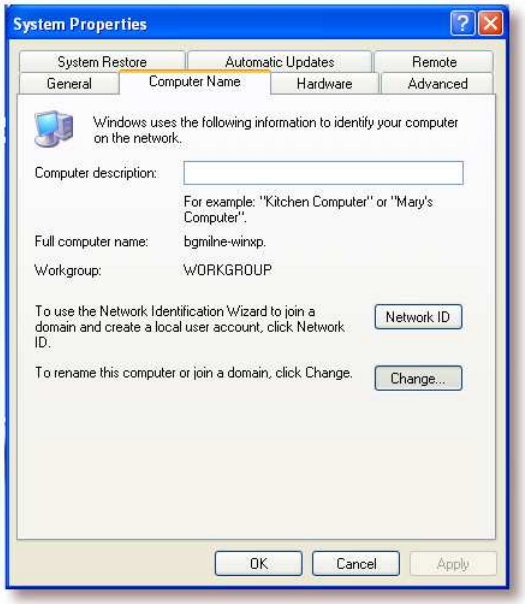
Pulse sobre “Conexiones de Red”.

Figura 12-35. Identificación de Red



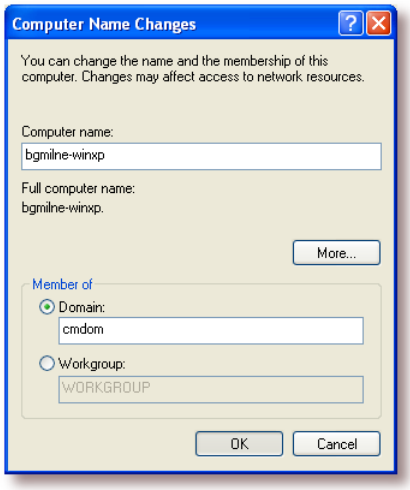
Pulse sobre el menú *Avanzado*, opción “Identificación de Red...”

Figura 12-36. Propiedades del Sistema



Pulse sobre el botón “Cambiar...”

Figura 12-37. Selección del Dominio



Seleccione la opción “Dominio”, teclee el dominio al cual se quiere añadir y, finalmente, pulse sobre el botón *Aceptar*.

Figura 12-38. Cuenta del dominio

Teclee la cuenta del usuario “root” de Samba (vea la
la sección de nombre *Añadiendo el usuario “root” a Samba* para más detalles) y pulse sobre el botón *Aceptar*.

Figura 12-39. Bienvenida al dominio

Si todo ha ido bien, se dará la bienvenida al dominio.

III. CUPS

Capítulo 13. Conceptos teóricos

Introducción

CUPS™, Common Unix Printing System™, es un sistema de impresión portable y extensible para Unix©. CUPS está siendo desarrollado por Easy Software Products (http://www.easysw.com/), una empresa de software emplazada en Hollywood, Maryland, que ha estado vendiendo software comercial para Unix desde 1993 a más de 40 distribuidores, que sirven sus productos en 80 países de todo el mundo.

La página principal de CUPS, desde donde se puede obtener más información, se encuentra localizada en http://www.cups.org (http://www.cups.org/).

Nota: Los conceptos teóricos se han basado en la la entrada bibliográfica Sweet01

Trasfondo histórico

La impresión en Unix históricamente se ha realizado con uno de estos dos sistemas de impresión: el demonio de impresión en línea de Berkeley (“LPD”) [RFC1179] y el sistema de impresión en línea de AT&T. Estos sistemas de impresión se diseñaron en la década de los setenta para imprimir texto en impresoras de línea; a partir de entonces, los vendedores han ido añadiendo diversos niveles de soporte para otro tipo de impresoras.

Algunos sustitutos a estos sistemas de impresión han aflorado [LPRng, Palladin, PLP], sin embargo, ninguno de ellos cambió las capacidades fundamentales de los sistemas primigenios.

A lo largo de los últimos años se han realizado muchos intentos de desarrollo para obtener una interfaz estándar de impresión, incluyendo el borrador de impresión estándar de POSIX, desarrollado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) [IEEE-1387.4], y el Protocolo de Impresión de Internet (IPP), desarrollado por IETF a través de PWG [IETF-IPP]. El protocolo de impresión estándar de POSIX define un conjunto común de herramientas para la consola así como una interfaz en C para la administración y los trabajos de impresión, pero fue abandonado por el IEEE.

El Protocolo de Impresión de Internet (IPP) define una serie de extensiones al Protocolo de Transferencia de HiperTexto 1.1 (HTTP) [RFC2616] que añaden soporte para los servicios de impresión remota. IPP/1.0 fue aceptado por el IETF, como un documento RFC experimental, en octubre de 1999. Desde entonces el PWG ha desarrollado y actualizado el conjunto de especificaciones para IPP/1.1, que ha sido aceptado por el IETF y está en espera para ser publicado como una propuesta de estándar. Al contrario que la Impresión POSIX, IPP ha gustado a las grandes empresas de soporte, y se ha posicionado para convertirse en la solución estándar para la impresión en red de todos los sistemas operativos.

CUPS hace uso de IPP/1.1 para proporcionar un sistema de impresión completo y moderno, destinado a sistemas Unix, que pueda ser ampliado para dar soporte a nuevas impresoras, dispositivos y protocolos, a la vez que garantice la compatibilidad con las aplicaciones Unix existentes. CUPS es Software Libre y se

distribuye bajo los términos de la Licencia Pública General (GPL) y la Licencia Pública General de Librerías (LGPL) del proyecto GNU.

Historia

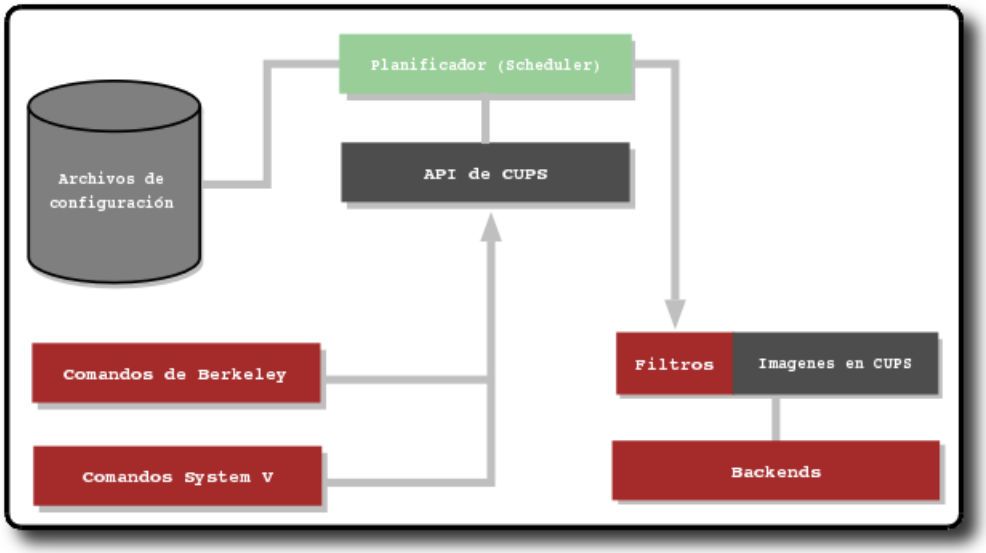
La primera versión de producción de CUPS (basada en IPP/1.0) fue liberada en octubre de 1999. Desde entonces, se han publicado bastantes actualizaciones para la versión 1.0, destinadas a corregir los errores encontrados, así como añadir seguridad y portabilidad a la versión existente; se ha de notar que no se han añadido nuevas funcionalidades para mejorar la estabilidad del código de CUPS.

CUPS 1.1 está basado en IPP/1.1 y se han añadido las funcionalidades pedidas por sus usuarios. Al igual que con la versión 1.0, CUPS 1.1 disfrutará de las actualizaciones necesarias para corregir cualquier problema encontrado en el software, pero no se añadirán nuevas características.

Una visión general sobre el diseño

Al igual que muchos otros sistemas de impresión, CUPS gira entorno a un proceso central de planeamiento (scheduling) de impresión, que cursa los trabajos de impresión, procesa las órdenes de administración y facilita la información de estado de la impresora a los programas locales y remotos, informado a los usuario que lo necesiten. La Figura 13-1 muestra la organización básica de CUPS.

Figura 13-1. Diagrama de la organización interna de CUPS[1]



Planificador

El planificador es un servidor HTTP/1.1 que maneja peticiones HTTP. A parte de ocuparse de las peticiones enviadas (*POST*) por la impresora a través del protocolo IPP, el planificador también actúa como un servidor web cuyas funciones son: mostrar la documentación, monitorizar el estado de la impresión y proveer de una interfaz para realizar tareas de administración.

El planificador también administra la lista de las impresoras disponibles en una LAN y reparte los trabajos de impresión como es preciso haciendo uso de los filtros y backends apropiados.

Archivos de configuración

Los archivos de configuración consisten en:

- Los archivos de configuración del servidor HTTP
- Los archivos de definición de las impresoras y las clases
- Los archivos de configuración de los tipos MIME y las reglas de conversión
- Los archivos PPD (*PostScript Printer Description*)

El archivo de configuración del servidor HTTP se ha creado similar al archivo de configuración del servidor Apache (http://www.apache.org/) a propósito, y define todas las propiedades de control de acceso del servidor.

Los archivos de definición de impresoras y clases, listan las colas y clases de impresión disponibles. Las clases de impresoras con una colección de impresoras. Los trabajos enviados a una clase, son reenviados a la primera impresora disponible en dicha clase, modelo *round-robin*.

Los archivos de tipos MIME listan los tipos MIME soportados (*text/plain*, *application/postscript*, etc.) y las reglas “mágicas” de la autodetección de los tipos de formato de un archivo. El servidor HTTP los utiliza para determinar el campo *Content-Type* (tipo de contenido) para las peticiones *GET* y *HEAD* así como por el *manejador de peticiones IPP* para determinar el tipo de archivo cuando se recibe un trabajo de impresión o una petición de envío de archivo con un formato de documento *application/octet-stream*.

Los archivos de las reglas de conversión MIME listan los filtros disponibles. Los filtros se utilizan cuando un trabajo es despachado, de forma que una aplicación pueda enviar un archivo convenientemente formateado al sistema de impresión, quien convertirá el documento en un formato imprimible, si es necesario. Cada filtro posee un coste relativo asociado, de forma que el algoritmo de elección de filtros pueda elegir el conjunto de filtros que convertirán el archivo al formato necesario con el menor “coste” total.

Los archivos PPD describen las capacidades de todas las impresoras, no sólo de las impresoras PostScript. Existe un archivo PPD por cada impresora. Los archivos PPD para las impresoras no PostScript definen un filtro adicional, a través del atributo *cupsFilter*, para soportar los controladores de la impresora.

API de CUPS

La API de CUPS contiene funciones de conveniencia específicas de CUPS para los trabajos de la cola de impresión, obtención de información sobre la impresora, acceso a los recursos a través de HTTP e IPP,

así como el manipulado de los archivos PPD. Al contrario que el resto de CUPS, la API de CUPS se distribuye bajo los términos de la licencia LGPL del proyecto GNU, para permitir su uso a las aplicaciones no GPL.

Órdenes de Berkeley y System V

CUPS provee las interfaces de las órdenes de consola de System V y Berkeley, que permiten el envío de trabajos y comprobación del estado de una impresora. Las órdenes **lpstat** y **lpcstatus** también muestran impresoras de rec ("impresora@servidor") cuando la búsqueda de impresoras está habilitada.

Las órdenes de administración de System V se suministran para manejar las impresoras y las clases. La herramienta de administración de Berkeley (**lpc**) sólo es soportada en un modo de solo lectura, para comprobar el estado actual de las colas de impresión y del planificador.

Filtros

El programa de filtrado lee desde la entrada estándar o desde un archivo, si se le pasa como parámetro. Todos los filtros han de soportar un conjunto común de opciones incluyendo el nombre de la impresora, el ID del trabajo, el número de copias y las opciones del trabajo. Todas las salidas son enviadas a la salida estándar.

Los filtros se suministran para múltiples formatos de archivo e incluye archivos de imágenes y filtros de búsqueda PostScript, que soportan impresoras no PostScript. Múltiples filtros se ejecutan en paralelo para producir el formato de salida requerido.

El filtro de búsqueda PostScript está basado en el núcleo GNU Ghostscript 5.50. En vez de utilizar los controladores de impresión y front-ends de Ghostscript, el filtro de CUPS utiliza un controlador de impresión genérico de búsqueda y un front-end compatible con CUPS para dar soporte a cualquier tipo de impresora "raster" desde cualquier filtro.

Imágenes en CUPS

La librería de imágenes de CUPS proporciona funciones de manipulado de grandes imágenes, haciendo una conversión del espacio de color y una administración del color, escalando las imágenes a imprimir y administrando los flujos de páginas "raster". Esta librería es utilizada por el archivo de filtros de imágenes de CUPS, por el RIP PostScript y todos los controladores de impresoras "raster".

Backends

Un programa backend es un filtro especial que envía datos a imprimir a un dispositivo o a una conexión de red. CUPS 1.1 provee backends para los puertos paralelo, serie, USB, protocolos como LPD, IPP y conexiones AppSocket (JetDirect).

La versión 2.0.6 y superior de Samba incluye un backend (**smbspool**(1)) que se puede utilizar con CUPS 1.0 o 1.1 para imprimir desde Windows.

Impresión en red

Tradicionalmente, la impresión en red ha sido una de las tareas más difíciles de llevar a cabo bajo Unix. Una de las razones es porque cada vendedor añade sus propias extensiones al protocolo LPD (el anterior estándar de la impresión en red), haciendo la impresión entre plataformas muy difícil, por no decir imposible.

Otra de las razones es que se tenía que administrar cada impresora de red en cada máquina cliente. En algunos casos se podía "clonar" la configuración de impresión desde un cliente "maestro" a los demás clientes, pero incluso así se consumía mucho tiempo y era propenso a errores. Se necesitaba algo mejor.

CUPS proporciona "búsqueda de impresoras", lo que permite a los clientes buscar y usar automáticamente las impresoras desde cualquier servidor de la red local. Esto significa que sólo se necesita configurar el servidor, y los clientes automáticamente ven las impresoras y sus clases.

Además de esto, CUPS puede asociar automáticamente impresoras en red idénticas en "clases implícitas". Esto permite a los clientes enviar trabajos a las clases implícitas y realizar la impresión en la primera impresora o servidor disponible. A mayores se pueden activar de manera sencilla funciones de control de errores y balanceo de carga, definiendo la misma impresora o múltiples servidores.

Nuevas características en CUPS 1.1

CUPS 1.1 incluye muchas características y funcionalidades nuevas, algunas de las cuales se presentarán en las siguientes secciones.

Backends

CUPS 1.1 implementa una nueva interfaz para los backends que le permite recuperar la lista de los dispositivos disponibles para los clientes CUPS. Esto permite poseer interfaces de administración que hagan peticiones al planificador de CUPS para obtener una lista de los dispositivos disponibles, configurar automáticamente las impresoras, siempre y cuando la información de identificación del dispositivo esté disponible, mostrando al usuario una lista de los dispositivos disponibles en vez de confiar que el usuario sepa que dispositivos están o no configurados en el sistema.

La nueva versión también incluye un backend para impresoras USB bajo *BSD y Linux. El soporte para USB en Solaris 8 se proveerá en subsecuentes liberaciones de parches.

Soporte de páginas de separación

CUPS 1.1 incluye soporte para páginas de separación al principio y al final de la impresión. Las páginas de separación pueden ser de cualquier formato y con soporte de sustitución dinámica para los títulos de los trabajos, nombres de usuario, etc. La página de separación por defecto están asociadas a cada impresora, pudiendo ser sobreescritas por el usuario.

Autentificación en modo *Digest*

La autentificación en modo *Digest* proporciona un método más seguro de autentificación para obtener acceso al sistema de impresión. Al contrario que la autentificación básica, la autentificación en modo *Digest* no envía las claves en "texto plano", lo que dificulta el acceso no autorizado al sistema.

La implementación de la autentificación en modo *Digest* de la versión 1.1 de CUPS se realiza gracias al uso de un archivo especial de claves MD5 en vez del archivo de claves de Unix. Este archivo se maneja con la nueva orden **lppasswd**.

Servicios de directorio

CUPS 1.1 añade un nuevo servicio de directorio ("búsqueda de impresoras"), característica que permite hacer uso de CUPS en LANs y WANs de gran dimensión fácilmente. Ahora se puede escanear un servidor remoto en busca de información de impresión y retransmitirla a la red local, así como clasificar el tipo de información a ser procesada (por ejemplo, ocultar los servidores, redes o dominios que no se quieran ver).

Cambios en la estructura de directorios

CUPS 1.1 utiliza una estructura de directorios que obedece a la versión 2.0 del estándar FHS (*Filesystem Hierarchy Standard*). Esto debería hacer la integración en sistemas Linux y *BSD existentes un poco más fácil.

Documentación

La documentación de CUPS 1.1 ha pasado varias revisiones, incluyendo una completa reescritura del manual de administración, un nuevo manual para programadores y un manual de referencia sobre la implementación IPP.

Controladores

CUPS 1.1 incluye controladores para las impresoras matriciales y de chorro de tinta de EPSON. Como ocurre con los controladores PCL de Hewlett-Packard, los controladores de EPSON no proveen necesariamente de la mejor calidad de impresión para todas las impresoras, de todas formas suelen imprimir con la calidad suficiente para el uso general del día a día.

Filtros

CUPS 1.1 incluye nuevos filtros para imágenes, PostScript, PDF y texto. El filtro de imágenes se ha actualizado para soportar archivos BMP de Windows y PIX de Alias.

El nuevo filtro para PostScript está basado en el programa Ghostscript 5.50 del proyecto GNU. Este filtro mejora el rendimiento con impresoras de gran resolución y soporta la mayoría de las características del nivel 3 del lenguaje PostScript.

El nuevo filtro para PDF está basado en el excelente software, Xpdf, de Derek Noonburg, soportando el escalado automático de páginas. El nuevo filtro es un reemplazo más rápido, pequeño y confiable que el filtro PDF del programa Ghostscript del proyecto GNU utilizado en la versión 1.0 de CUPS.

El nuevo filtro de texto soporta texto bidireccional y se le pueden incrustar fuentes si se desea.

Soporte IPP

Posiblemente la parte menos visible de CUPS es su soporte de IPP. CUPS 1.1 implementa todas las operaciones y atributos requeridos por IPP/1.1 y muchas de las opcionales. Las opciones opcionales “crear trabajo” y “enviar archivo” ya están implementadas, permitiendo una compatibilidad mejor con el sistema de impresión System V (un identificador de trabajo por cada orden **lp**), así como el soporte de páginas de separación.

Persistencia de trabajos

CUPS 1.1 tiene soporte para trabajos persistentes. Esto significa que los trabajos de impresión son preservados incluso después de un reinicio, característica que fue olvidada, desgraciadamente, en la versión 1.0 de CUPS.

A parte de esto, CUPS 1.1 permite mantener la información de cada impresión, una vez que el trabajo se ha impreso. El modo básico de persistencia post-trabajo provee un historial de impresiones (número de páginas impresas, tiempo de impresión que ha tomado un trabajo, etc.) pero no almacena el archivo del trabajo impreso. CUPS se puede configurar para que descarte toda la información una vez ha finalizado la impresión o para mantener los archivos de impresión una vez impresos, de forma que se pueda imprimir de nuevo el archivo más tarde.

Soporte para el cliente LPD

Por petición popular, CUPS 1.1 soporta los clientes basados en LPD, usando un pequeño demonio que maneja las peticiones LPD y las retransmite al servidor principal.

Definiciones de impresoras y opciones por parte del usuario

CUPS 1.1 incluye soporte para las definiciones de usuario de impresoras y opciones gracias a una nueva orden, **lpoptions**. Las impresoras definidas por el usuario son instancias especiales de las impresoras disponibles (por ejemplo “printer/instance” o “printer@server/instance”), que pueden tener sus propias opciones por defecto, como el tamaño del papel, la resolución y así en adelante. La orden **lpoptions** se puede utilizar también para establecer una cola de impresión diferente a la definida por defecto.

Interfaz de administración web

CUPS 1.0 poseía una interfaz, destinada a navegadores web, simple para las clases, trabajos y monitorización de impresión, CUPS 1.1 ha reemplazado esta interfaz con una interfaz de administración mejorada, que permite añadir, modificar, borrar, configurar y controlar las clases, los trabajos y las impresoras.

Información adicional sobre el proyecto

Página principal

El Proyecto CUPS dispone de una página principal, http://www.cups.org/, desde donde puede obtener mucha información sobre el proyecto. De hecho, para elaborar esta sección ha utilizado la información allí disponible.

Cómo obtener CUPS

Desde la siguiente dirección, podrá seleccionar la versión de CUPS en la que esté interesado y descargársela desde cualquiera de los mirrors disponibles: http://www.cups.org/software.php. Esto es posible ya que CUPS es Software Libre y se licencia bajo los términos de la licencia GPL y LGPL (vea los GNU General Public License, GNU LESSER GENERAL PUBLIC LICENSE y Apéndice AV para más información).

La mayoría de las distribuciones de GNU/Linux y muchos distribuidores de Unix disponen de paquetes binarios de CUPS. Infórmese de si su distribución posee este tipo de paquetes.

Documentación

La página principal del Proyecto CUPS dispone de una sección dedicada a la documentación, con un listado bastante amplio de documentación relativa al proyecto. Para más detalles, visite: http://www.cups.org/documentation.php

Información de soporte

La página dedicada al soporte de CUPS (http://www.cups.org/support.php), informa sobre los distintos métodos existentes para obtener ayuda en un determinado momento. Los métodos más importantes para obtener ayuda son los siguientes:

Grupos de noticias: El servidor de noticias de la empresa Easy Software Product, news.easysw.com (news://news.easysw.com), proporciona 5 grupos de noticias: cups.announce, cups.bugs, cups.cvs, cups.development y cups.general. Los mensajes que allí se publican, se redirigen a su vez a una serie de listas de correo, para obtener más información al respecto, visite el siguiente enlace: http://lists.easysw.com/mailman/listinfo

Chequeo de los archivos PPD: La siguiente URL nos proporciona un método de verificar que nuestros archivos PPD están correctos, haciendo uso de la herramienta cupstestppd: http://www.cups.org/testppd.php.

FAQs: La página principal de CUPS posee un listado de las preguntas más frecuentemente consultadas, este se encuentra en: http://www.cups.org/faq.php.

Reporte de bugs

CUPS dispone de un formulario de reporte de problemas (http://www.cups.org/str.php), desde donde se pueden enviar los errores y bugs relacionados con CUPS.

Cómo contactar

Para obtener más información sobre CUPS, puede contactar con la empresa *Easy Software Products* en la siguiente dirección:

```
Attn: CUPS Information
Easy Software Products
44141 Airport View Drive Suite 204
Hollywood, Maryland 20636-3111 USA

+1.301.373.9600

<cups-info@cups.org>
```

Notas

1. Si quiere obtener el código fuente de esta imagen realizada con Dia pulse aquí (./imagenes/cups-diagrama-organizacion-interna.dia)

Capítulo 14. Instalación

Introducción

Este capítulo comenzará haciendo un análisis de los paquetes necesarios para la instalación de un sistema completo de impresión con CUPS, para acabar con la instalación de los paquetes seleccionados.

El objetivo que perseguido con el sistema de impresión, es suministrar un mecanismos para que los clientes puedan imprimir, estén donde estén, y utilizando el sistema operativo que sea.

Los clientes tipo Unix tendrán el problema resuelto gracias al protocolo IPP, sobre el cual funciona CUPS. Por otro lado, los clientes con sistemas operativos de Microsoft podrán imprimir gracias a la integración de CUPS con Samba.

> **Nota:** La versión que se instalará de CUPS es la 1.1.20, que acompaña a la versión en desarrollo de Debian GNU/Linux (aka Sid).

Elección de los paquetes necesarios

La selección de los paquetes a instalar, para conseguir que el sistema de impresión CUPS funcione, se va a efectuar, en primer lugar, observando la descripción del paquete *cupsys*. A partir de las dependencias, sugerencias y recomendaciones de este paquete, se seleccionarán los paquetes más adecuados e importantes para conseguir los objetivos finales de este proyecto.

> **Nota:** Si su proyecto tiene otras necesidades, sería recomendable repasar la lista de paquetes, y ver cuales de ellos son realmente necesarios y cuales no.
>
> En este caso, como no se tienen impresoras definidas, se instalarán la mayoría de los paquetes de controladores para impresoras. Si ya se tuviese un conjunto de impresoras sobre las cuales actuar, se podría hacer una selección más fina de paquetes de controladores.

El siguiente ejemplo muestra la descripción del paquete *cupsys*:

Ejemplo 14-1. Descripción del paquete *cupsys*

```
$ /usr/bin/apt-cache show cupsys
Package: cupsys
Priority: optional
Section: net
Installed-Size: 10532
Maintainer: Kenshi Muto <kmuto@debian.org>
Architecture: i386
Version: 1.1.20final+rc1-9
Replaces: cupsys-pstoraster
```

```
Depends: libc6 (>= 2.3.2.ds1-4), libcupsimage2 (>= 1.1.19final-1),
libcupsys2-gnutls10 (>= 1.1.20final-1), libgcc1 (>= 1:3.4.1-3),
libgnutls11 (>= 1.0.16), libpam0g (>= 0.76), libpaper1, libslp1,
zlib1g (>= 1:1.2.1), gs-esp ❶, adduser (>= 3.12), debconf (>= 1.2.9), patch
Recommends: cupsys-client ❷, smbclient ❸, xpdf-common
Suggests: cupsys-bsd ❹, cupsys-driver-gimpprint ❺,
foomatic-bin | foomatic-filters-ppds ❻,
xpdf-korean | xpdf-japanese | xpdf-chinese-traditional | xpdf-chinese-simplified
Conflicts: cupsys-pstoraster (<< 2), lprng (>= 3.8.25)
Filename: pool/main/c/cupsys/cupsys_1.1.20final+rc1-9_i386.deb
Size: 3609096
MD5sum: 9a1db7a532df1477e7c572151d217030
Description: Common UNIX Printing System(tm) - server
 The Common UNIX Printing System (or CUPS(tm)) is a printing system and
 general replacement for lpd and the like.  It supports the Internet
 Printing Protocol (IPP), and has its own filtering driver model for
 handling various document types.
 .
 This package provides the CUPS scheduler/daemon and related files.
 .
 The terms "Common UNIX Printing System" and "CUPS" are trademarks of
 Easy Software Products (www.easysw.com), and refer to the original
 source packages from which these packages are made.
Task: print-server
```

❶ Paquete que provee la versión ESP del intérprete de PostScript *Ghostscript*. Este será utilizado por CUPS para renderizar archivos PostScript como gráficos, de forma que este tipo de archivos se puedan imprimir en impresoras sin soporte para PostScript.

Al ser una dependencia del paquete *cupsys*, no será necesario marcarlo para instalar, ya que se instalará automáticamente. De todas formas, se analizará para ver los paquetes que sugiere y recomienda.

❷ Herramientas para los clientes de CUPS.

❸ Como recomendación, *cupsys* propone el paquete *smbclient*. Este paquete ya se ha tratado en la la sección de nombre *Instalación de un cliente* en Capítulo 7, para más detalles diríjase a dicha sección.

Este paquete ya se supone instalado, por lo que no se marcará para instalar.

❹ Paquete que provee las órdenes de impresión BSD, de forma que puedan interactuar con CUPS.

❺ Controladores de impresión, con calidad de impresión fotográfica para CUPS, basados en Gimp-Print.

❻ Paquetes que proveen la base de datos de impresoras *Foomatic*, diseñada para facilitar la configuración de las impresoras más comunes. Más detalles en http://www.linuxprinting.org/

Del análisis anterior, se obtiene la siguiente lista de paquetes a instalar, a parte del paquete *cupsys*:

- *cupsys-client*

- *cupsys-bsd*
- *cupsys-driver-gimpprint*
- *foomatic-bin*
- *cupsomatic-ppd*

En las siguientes secciones se procederá al análisis de los paquetes de la lista anterior, de la misma forma que ya se hizo con el paquete *cupsys*.

Análisis del paquete *gs-esp*

En esta sección se analizará la lista de sugerencias y recomendaciones del paquete *gs-esp*; de esta lista se seleccionarán aquellos paquetes que se consideren interesantes para la consecución del proyecto.

Ejemplo 14-2. Descripción del paquete *gs-esp*

```
$ /usr/bin/apt-cache show gs-esp
Package: gs-esp
Priority: optional
Section: text
Installed-Size: 12008
Maintainer: Masayuki Hatta (mhatta) <mhatta@debian.org>
Architecture: i386
Version: 7.07.1-9
Replaces: gs-afpl (<< 8.14-3), gs-aladdin (<< 8.14-3),
gs-gpl (<< 8.01-3), gs (<< 8.01-3), gs-pdfencrypt (<< 7.00),
cupsys-pstoraster
Provides: gs, gs-pdfencrypt, postscript-viewer
Depends: libc6 (>= 2.3.2.ds1-4), libcupsimage2 (>= 1.1.19final-1),
libcupsys2-gnutls10 (>= 1.1.20final-1), libgimpprint1 (>= 4.2.6),
libglib2.0-0 (>= 2.4.1), libjpeg62, libpaper1,
libpng12-0 (>= 1.2.5.0-4), libstdc++5 (>= 1:3.3.4-1), libtiff4,
libx11-6 | xlibs (>> 4.1.0), libxext6 | xlibs (>> 4.1.0),
libxt6 | xlibs (>> 4.1.0), zlib1g (>= 1:1.2.1), gs-common (>= 0.2)
Recommends: gsfonts ❶ (>= 6.0-1), psfontmgr ❷
Conflicts: gs-afpl (<< 8.14-3), gs-aladdin (<< 8.14-3),
gs-gpl (<< 8.01-3), gs (<< 8.01-3), gs-pdfencrypt (<< 7.00),
cupsys-pstoraster
Filename: pool/main/g/gs-esp/gs-esp_7.07.1-9_i386.deb
Size: 2772000
MD5sum: 26559300a360d8aa1176512e4beab77e
Description: The Ghostscript PostScript interpreter - ESP version
 Ghostscript is used for PostScript preview and printing.  Usually as
 a back-end to a program such as ghostview, it can display postscript
 documents in an X11 environment.
 .
 Furthermore, it can render PostScript files as graphics to be printed
 on non-PostScript printers.  Supported printers include common
 dot-matrix, inkjet and laser models.
 .
 Package gsfonts contains a set of standard fonts for Ghostscript.
```

```
 .
 This version of gs is a fork of GNU Ghostscript with updated drivers
 and patches, intended mostly for use with the Common UNIX Printing
 System (CUPS) from Easy Software Products (www.easysw.com).  The
 ESP Ghostscript homepage is available at:
 .
 http://www.cups.org/ghostscript.php
```

❶ *gs-esp* recomienda la instalación de las fuentes para el intérprete Ghostscript, paquete que se instalará.

❷ *psfontmgr* es un administrador de fuentes PostScript que hace uso de la aplicación Defoma. Este paquete también se instalará, ya que puede facilitar, en un momento determinado, la administración de dichas fuentes.

Después de ver la descripción de este paquete, se añaden a la lista inicial (Primera lista de paquetes a instalar junto con cupsys), los siguientes:

- *gsfonts*
- *psfontmgr*

Paquetes *gsfonts* y *psfontmgr*

Esta sección no tiene más sentido que el mostrar la descripción de los paquetes que se van a instalar, para obtener una visión más amplia de las modificaciones que se van a introducir en el sistema.

Ejemplo 14-3. Descripción de los paquetes *gsfonts* y *psfontmgr*

```
$ /usr/bin/apt-cache show gsfonts psfontmgr
Package: gsfonts
Priority: optional
Section: text
Installed-Size: 5080
Maintainer: Masayuki Hatta (mhatta) <mhatta@debian.org>
Architecture: all
Version: 8.14+v8.11-0.1
Depends: defoma
Conflicts: gs (<< 5.50-5), gs-aladdin (<< 6.50-4), gsfonts-x11 (<< 0.13)
Filename: pool/main/g/gsfonts/gsfonts_8.14+v8.11-0.1_all.deb
Size: 3726818
MD5sum: b383e6b56330d231fbd0dfee8797aaec
Description: Fonts for the Ghostscript interpreter(s)
 These are free look-alike fonts of the Adobe PostScript fonts.
 Recommended for all flavors of Ghostscript (gs-gpl, gs-afpl and gs-esp).

Package: psfontmgr
Priority: optional
Section: admin
Installed-Size: 172
```

```
Maintainer: Angus Lees <gus@debian.org>
Architecture: all
Source: defoma
Version: 0.11.8-0.1
Depends: defoma (>= 0.9.1), whiptail | dialog, perl
Conflicts: defoma-ps, scigraphica-common (<= 0.7.1-3)
Filename: pool/main/d/defoma/psfontmgr_0.11.8-0.1_all.deb
Size: 21220
MD5sum: 82d87f3940cc0270fdff58568ca3c5ee
Description: PostScript font manager -- part of Defoma, Debian Font Manager
 psfontmgr manages PostScript fonts through the Defoma framework. It
 registers the name of available PostScript fonts to Defoma in
 postscript category, so applications which output a postscript file
 have all the available PostScript fonts in their font-choosing menus.
 .
 It also provides a tool named defoma-psfont-installer, which registers
 PostScript fonts installed in a PostScript printer. This tool benefits
 those who want to print a PostScript file with the printer fonts and
 have the printer fonts appear in a font-choosing menu.
Task: chinese-s, chinese-t
```

Análisis del paquete *cupsys-client*

Esta sección está dedicada al análisis del paquete *cupsys-client*, de este análisis se obtendrá otra lista de paquetes a instalar, que se añadirán a las ya existentes
(Primera lista de paquetes a instalar junto con cupsys y
Segunda lista de paquetes a instalar junto con cupsys)

Ejemplo 14-4. Descripción del paquete *cupsys-client*

```
$ /usr/bin/apt-cache show cupsys-client
Package: cupsys-client
Priority: optional
Section: net
Installed-Size: 308
Maintainer: Kenshi Muto <kmuto@debian.org>
Architecture: i386
Source: cupsys
Version: 1.1.20final+rc1-9
Replaces: cupsys (<= 1.1.18-3)
Depends: libc6 (>= 2.3.2.ds1-4),
libcupsys2-gnutls10 (>= 1.1.20final-1), zlib1g (>= 1:1.2.1)
Recommends: cupsys-bsd ❶
Suggests: cupsys, kdeprint ❷, gtklp, cupsys-pt, xpp
Conflicts: lprng
Filename: pool/main/c/cupsys/cupsys-client_1.1.20final+rc1-9_i386.deb
Size: 87964
MD5sum: 100897320ff2fc8296d8c7192d11e313
Description: Common UNIX Printing System(tm) - client programs (SysV)
```

```
 The Common UNIX Printing System (or CUPS(tm)) is a printing system and
 general replacement for lpd and the like.  It supports the Internet
 Printing Protocol (IPP), and has its own filtering driver model for
 handling various document types.
 .
 This package provides the System V style print client programs.
 .
 The terms "Common UNIX Printing System" and "CUPS" are trademarks of
 Easy Software Products (www.easysw.com), and refer to the original
 source packages from which these packages are made.
Task: print-server
```

❶ Paquete sugerido por *cupsys*, que ya estaba en la
Primera lista de paquetes a instalar junto con cupsys. La
la sección de nombre *Análisis del paquete cupsys-bsd* analizará este paquete, en busca de paquetes interesantes para el proyecto.

❷ Subsistema de impresión de KDE. Se hará uso de este subsistema para mostrar, en algunas ocasiones, la forma de configurar CUPS.

La elección de este frontend sobre los demás existentes, ha sido por la facilidad de uso que presenta y la potencia a la hora de la administración.

Se suma el paquete *kdeprint* a la lista de paquetes a instalar para obtener el sistema de impresión CUPS:

- *kdeprint*

Descripción del paquete *kdeprint*

Esta sección no tiene más sentido que el mostrar la descripción del paquete que se va a instalar, para obtener una visión más amplia de las modificaciones que se van a introducir en el sistema.

Ejemplo 14-5. Descripción del paquete *kdeprint*

```
$ /usr/bin/apt-cache show kdeprint
Package: kdeprint
Priority: optional
Section: utils
Installed-Size: 1828
Maintainer: Debian Qt/KDE Maintainers <debian-qt-kde@lists.debian.org>
Architecture: i386
Source: kdebase
Version: 4:3.3.0a-1
Replaces: kdebase (<< 4:3.0.0), kdebase-doc (<< 4:3.0.0)
Depends: kdelibs4 (>= 4:3.3.0), libart-2.0-2 (>= 2.3.16),
libc6 (>= 2.3.2.ds1-4), libfam0c102, libgcc1 (>= 1:3.4.1-3),
libice6 | xlibs (>> 4.1.0), libidn11 (>= 0.5.2),
libpng12-0 (>= 1.2.5.0-4), libqt3c102-mt (>= 3:3.3.3),
libsm6 | xlibs (>> 4.1.0), libstdc++5 (>= 1:3.3.4-1),
libx11-6 | xlibs (>> 4.1.0), libxext6 | xlibs (>> 4.1.0),
```

```
libxrender1, zlib1g (>= 1:1.2.1), enscript, gv, poster, psutils
Suggests: khelpcenter, efax | hylafax-client | mgetty-fax
Filename: pool/main/k/kdebase/kdeprint_3.3.0a-1_i386.deb
Size: 1061246
MD5sum: b865d5a1909d34c910a5eba77617b3fc
Description: KDE Print
 KDE is a powerful Open Source graphical desktop environment
 for Unix workstations. It combines ease of use, contemporary
 functionality, and outstanding graphical design with the
 technological superiority of the Unix operating system.
 .
 This package contains the KDE printing subsystem. It can use Cups,
 lpd-ng or the traditional lpd. It also includes support for fax and pdf
 printing.
 .
 This package is part of the official KDE base module.
```

Análisis del paquete *cupsys-bsd*

La descripción de este paquete no desvela ningún otro paquete a instalar. A continuación se muestra su descripción:

Ejemplo 14-6. Descripción del paquete *cupsys-bsd*

```
$ /usr/bin/apt-cache show cupsys-bsd
Package: cupsys-bsd
Priority: extra
Section: net
Installed-Size: 192
Maintainer: Kenshi Muto <kmuto@debian.org>
Architecture: i386
Source: cupsys
Version: 1.1.20final+rc1-9
Replaces: lpr, cupsys (<= 1.1.15-2), manpages-fr (<< 0.9.5-1)
Provides: lpr
Depends: libc6 (>= 2.3.2.ds1-4), libcupsys2-gnutls10 (>= 1.1.20final-1),
cupsys-client (= 1.1.20final+rc1-9), debconf, netbase
Conflicts: lpr, lprng, manpages-fr (<< 0.9.5-1)
Filename: pool/main/c/cupsys/cupsys-bsd_1.1.20final+rc1-9_i386.deb
Size: 40272
MD5sum: cfc6bc7f6a73e414752f297e3949f382
Description: Common UNIX Printing System(tm) - BSD commands
 The Common UNIX Printing System (or CUPS(tm)) is a printing system and
 general replacement for lpd and the like.  It supports the Internet
 Printing Protocol (IPP), and has its own filtering driver model for
 handling various document types.
 .
 This package provides the BSD commands for interacting with CUPS.  It
 is provides separately to allow CUPS to coexist with other printing
```

```
 systems (to a small degree).
 .
 The terms "Common UNIX Printing System" and "CUPS" are trademarks of
 Easy Software Products (www.easysw.com), and refer to the original
 source packages from which these packages are made.
Task: print-server
```

Análisis del paquete *cupsys-driver-gimpprint*

Sección que analizará el paquete de los controladores para CUPS basados en *Gimp-Print*. A partir de este paquete se seleccionarán otros; vea el siguiente ejemplo para más detalles:

Ejemplo 14-7. Descripción del paquete *cupsys-driver-gimpprint*

```
$ /usr/bin/apt-cache show cupsys-driver-gimpprint
Package: cupsys-driver-gimpprint
Priority: optional
Section: graphics
Installed-Size: 1192
Maintainer: Roger Leigh <rleigh@debian.org>
Architecture: i386
Source: gimp-print
Version: 4.2.7-4
Depends: libc6 (>= 2.3.2.ds1-4), libcupsimage2 (>= 1.1.19final-1),
libcupsys2-gnutls10 (>= 1.1.20final-1), libgimpprint1 (>= 4.2.7),
zlib1g (>= 1:1.2.1), perl, cupsys-driver-gimpprint-data ❶ (= 4.2.7-4),
cupsys (>= 1.1.4) | cups (>= 1.1.4)
Recommends: gs-esp (>= 7.05.2-1) | gs-gpl (>= 8.01-1) | postscript-viewer
Suggests: gimpprint-doc (>= 4.2.7-4), gimpprint-locales ❷ (>= 4.2.7-4)
Filename: pool/main/g/gimp-print/cupsys-driver-gimpprint_4.2.7-4_i386.deb
Size: 952450
MD5sum: 0b6224bdd85be3a35b56af4d22d0de82
Description: Gimp-Print printer drivers for CUPS
 This package includes a CUPS driver based on Gimp-Print.
 .
 The CUPS drivers contain all of the files needed to support
 photo-quality printing on any printer supported by Gimp-Print.  You
 can find out more about the Common UNIX Printing System ("CUPS"), an
 IPP-based printing system for UNIX/Linux, at:
 .
   http://www.cups.org
 .
 This is Gimp-Print version 4.2.7, a stable release in
 the 4.2 line.
 .
 Gimp-Print is the print facility for the Gimp, and in addition a
 suite of drivers that may be used with common UNIX spooling systems
 using GhostScript or CUPS.  These drivers provide printing quality
 for UNIX/Linux on a par with proprietary vendor-supplied drivers in
 many cases, and can be used for many of the most demanding printing
```

```
 tasks.
Task: print-server
```

❶ Este paquete es una dependencia, por lo que se va a instalar cuando se instale el paquete *cupsys-driver-gimpprint*. Su contenido son los archivos PPDs, del proyecto Gimp-Print, para CUPS.

❷ Paquete que provee los datos de internacionalización para *Gimp-Print*.

El paquete que se lista a continuación se suma a los ya seleccionados anteriormente para instalar:

- *gimpprint-locales*

Paquetes *gimpprint-locales* y *cupsys-driver-gimpprint-data*

Esta sección no tiene más sentido que el mostrar la descripción de los paquetes que se van a instalar, para obtener una visión más amplia de las modificaciones que se van a introducir en el sistema.

Ejemplo 14-8. Descripción de los paquetes *gimpprint-locales* y *cupsys-driver-gimpprint-data*

```
$ /usr/bin/apt-cache show gimpprint-locales \
                          cupsys-driver-gimpprint-data
Package: gimpprint-locales
Priority: optional
Section: libs
Installed-Size: 1152
Maintainer: Roger Leigh <rleigh@debian.org>
Architecture: all
Source: gimp-print
Version: 4.2.7-4
Replaces: libgimpprint1 (<= 4.2.0-1)
Filename: pool/main/g/gimp-print/gimpprint-locales_4.2.7-4_all.deb
Size: 309592
MD5sum: a32bf289f46ea3a6ce6ed915b3d6b647
Description: Locale data files for Gimp-Print
 This package contains the i18n files of Gimp-Print, used by
 libgimpprint1, cupsys-driver-gimpprint and escputil.  It is also
 used by the Gimp Print plugin.
 It will be used by any programs which link with libgimpprint.
 .
 They are needed when you want the programs in Gimp-Print to print
 their messages in other languages than US English.
 .
 This is Gimp-Print version 4.2.7, a stable release in
 the 4.2 line.
 .
 Gimp-Print is the print facility for the Gimp, and in addition a
 suite of drivers that may be used with common UNIX spooling systems
 using GhostScript or CUPS.  These drivers provide printing quality
 for UNIX/Linux on a par with proprietary vendor-supplied drivers in
 many cases, and can be used for many of the most demanding printing
```

```
 tasks.

Package: cupsys-driver-gimpprint-data
Priority: optional
Section: graphics
Installed-Size: 1984
Maintainer: Roger Leigh <rleigh@debian.org>
Architecture: all
Source: gimp-print
Version: 4.2.7-4
Replaces: cupsys-driver-gimpprint (<< 4.2.6-4)
Depends: cupsys-driver-gimpprint (= 4.2.7-4)
Filename: pool/main/g/gimp-print/cupsys-driver-gimpprint-data_4.2.7-4_all.deb
Size: 1368570
MD5sum: 988e7ee0a060ebaed149c9d91dd9c5b8
Description: Gimp-Print printer drivers for CUPS
 This package includes Gimp-Print PPDs for CUPS.
 .
 The CUPS drivers contain all of the files needed to support
 photo-quality printing on any printer supported by Gimp-Print.  You
 can find out more about the Common UNIX Printing System ("CUPS"), an
 IPP-based printing system for UNIX/Linux, at:
 .
   http://www.cups.org
 .
 This is Gimp-Print version 4.2.7, a stable release in
 the 4.2 line.
 .
 Gimp-Print is the print facility for the Gimp, and in addition a
 suite of drivers that may be used with common UNIX spooling systems
 using GhostScript or CUPS.  These drivers provide printing quality
 for UNIX/Linux on a par with proprietary vendor-supplied drivers in
 many cases, and can be used for many of the most demanding printing
 tasks.
```

Análisis del paquete *foomatic-bin*

Desde la página linuxprinting.org (http://www.linuxprinting.org/) se distribuyen una serie de controladores para distintas impresoras, cuyo objetivo es facilitar la instalación y configuración de las mismas.

En esta sección se verán los paquetes necesarios para obtener dichos controladores:

Ejemplo 14-9. Descripción del paquete *foomatic-bin*

```
$ /usr/bin/apt-cache show foomatic-bin
Package: foomatic-bin
Priority: optional
Section: text
```

```
Installed-Size: 60
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: all
Source: foomatic-db-engine
Version: 3.0.2-2
Depends: foomatic-db ❶ (>> 2.9), foomatic-db-hpijs ❷, foomatic-db-engine ❸,
foomatic-filters ❹
Filename: pool/main/f/foomatic-db-engine/foomatic-bin_3.0.2-2_all.deb
Size: 47592
MD5sum: f147f54037ca6c8c9a4a1128f3f6adfa
Description: linuxprinting.org printer support - transition package
 Release 3.0 of foomatic has reorganized the foomatic printing system.
 This package is provided to facilitate a smooth upgrade from Foomatic
 2.0 or earlier.
 .
 Once you have installed the dependencies of this package, this
 package can be safely purged from your system.
 .
 Home Page: http://www.linuxprinting.org/
```

❶ Paquete que contiene la base de datos de las impresoras más comunes que se distribuye desde linuxprinting.org (http://www.linuxprinting.org/). Estos controladores hacen uso de Ghostscript para la parte del procesado de la impresión.

❷ Paquete que incluye el soporte necesario para las impresoras que hacen uso de los controladores HPIJS, particularmente las impresoras de inyección de tinta de Hewlett-Packard.

❸ Programas dependientes de la arquitectura necesarios para configurar y mantener el sistema *foomatic*.

❹ Scripts de filtrado utilizados por las colas de impresión para convertir los datos PostScript entrantes en el formato nativo de las impresoras que hacen uso de un archivo PPD específico de la impresora, pero independiente de la cola de impresión.

El paquete *foomatic-bin*, no es más que un metapaquete de dependencias. Con la instalación de este paquete, se instalarán a su vez la siguiente lista de paquetes, por lo que no será necesario marcarlos para la instalación:

- *foomatic-db*
- *foomatic-db-hpijs*
- *foomatic-db-engine*
- *foomatic-filters*

Análisis del paquete *foomatic-db*

A continuación se muestra la descripción del paquete *foomatic-db*, la cual se analizará en busca de nuevos paquetes para instalar, en caso de ser necesario:

Ejemplo 14-10. Descripción de los paquetes *foomatic-db*

```
$ /usr/bin/apt-cache show foomatic-db
Package: foomatic-db
Priority: optional
Section: text
Installed-Size: 10064
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: all
Version: 20041013-1
Depends: foomatic-filters
Recommends: foomatic-db-engine
Suggests: foomatic-db-hpijs, foomatic-db-gimp-print ❶, foo2zjs ❷
Conflicts: foomatic-bin (<< 2.9)
Filename: pool/main/f/foomatic-db/foomatic-db_20041013-1_all.deb
Size: 494012
MD5sum: 84891b80ef692464897e8ceb4bc8724a
Description: linuxprinting.org printer support - database
 Foomatic is a printing system designed to make it easier to set up
 common printers for use with Debian (and other operating systems).
 It provides the "glue" between a print spooler (like CUPS or lpr) and
 your actual printer, by telling your computer how to process files
 sent to the printer.
 .
 This package contains the printer database distributed by
 linuxprinting.org for most common drivers.  You will probably need
 the foomatic-db-engine package for this package to be useful.
 .
 The foomatic-db-hpijs package adds additional printers supported by
 the HPIJS printer driver backend, particularly consumer inkjet
 printers from Hewlett-Packard.
 .
 The foomatic-db-gimp-print package adds additional printers supported
 by the GIMP-Print printer driver backend, most commonly used for
 color photo printing on consumer inkjets.
 .
 The foo2zjs package adds backend support for a number of printers
 from HP and Minolta/QMS that use the Zenographics ZjStream protocol.
 .
 Home Page: http://www.linuxprinting.org/
```

❶ Paquete que provee soporte para las impresoras, haciendo uso de la suite de controladores de impresoras Gimp-Print.

❷ Controladores de impresión para aquellas impresoras que utilizan el protocolo *Zenographics ZjStream* para la transmisión de los datos de impresión.

Este paquete no se instalará, de todas formas, ha de analizar si posee alguna impresora de este tipo.

A partir del paquete *foomatic-db*, se ha encontrado otro paquete más para la lista de paquetes de instalación. El paquete en cuestión es:

- *foomatic-db-gimp-print*

Paquetes foomatic-db-gimp-print y foo2zjs

Esta sección no tiene más sentido que el mostrar la descripción de los paquetes que se van a instalar, para obtener una visión más amplia de las modificaciones que se van a introducir en el sistema.

> **Nota:** En esta ocasión se muestra la descripción del paquete *foo2zjs*, que no va a ser instalado. El motivo de mostrar su descripción, es proveer la información necesaria para aquellas personas que tengan una impresora del tipo que soporta el paquete *foo2zjs*.

Ejemplo 14-11. Descripción de los paquetes *foomatic-db-gimp-print* y *foo2zjs*

```
$ /usr/bin/apt-cache show foomatic-db-gimp-print \
                          foo2zjs
Package: foomatic-db-gimp-print
Priority: optional
Section: text
Installed-Size: 11948
Maintainer: Roger Leigh <rleigh@debian.org>
Architecture: all
Source: gimp-print
Version: 4.2.7-4
Depends: foomatic-db, ijsgimpprint (>= 4.2.7-4)
Conflicts: foomatic-bin (<< 2.9), foomatic-db (<< 2.9)
Filename: pool/main/g/gimp-print/foomatic-db-gimp-print_4.2.7-4_all.deb
Size: 544364
MD5sum: ef504aba3492142f5174aaeecd4af05f
Description: linuxprinting.org printer support - database for Gimp-Print printer drivers
 Foomatic is a printing system designed to make it easier to set up
 common printers for use with Debian (and other operating systems).
 It provides the "glue" between a print spooler (like CUPS or lpr) and
 your actual printer, by telling your computer how to process files
 sent to the printer.
 .
 This package includes support for printers using the Gimp-Print
 printer driver suite.
 .
 Home Page: http://www.linuxprinting.org/
 .
 This is Gimp-Print version 4.2.7, an unstable
 development release in the 4.3 line.
 .
 Gimp-Print is the print facility for the Gimp, and in addition a
 suite of drivers that may be used with common UNIX spooling systems
 using GhostScript or CUPS.  These drivers provide printing quality
 for UNIX/Linux on a par with proprietary vendor-supplied drivers in
 many cases, and can be used for many of the most demanding printing
 tasks.
```

```
Package: foo2zjs
Priority: optional
Section: text
Installed-Size: 400
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: i386
Version: 20040210-2
Depends: libc6 (>= 2.3.2.ds1-4)
Recommends: foomatic-db-engine
Suggests: psutils
Filename: pool/main/f/foo2zjs/foo2zjs_20040210-2_i386.deb
Size: 187138
MD5sum: e7ab1d8f6ea4e32fa6cd59fdee505ce8
Description: Support for printing to ZjStream-based printers
 foo2zjs is an open source printer driver for printers that use the
 Zenographics ZjStream wire protocol for their print data, such as the
 Minolta/QMS magicolor 2200 DL/2300 DL and HP LaserJet 1000/1005.
 These printers are often erroneously referred to as "winprinters" or
 "GDI printers".
 .
 The foomatic-db-engine package is recommended to simplify configuring
 this printer driver.  The psutils package is needed to enable n-up
 printing support.
 .
 Home Page: http://foo2zjs.rkkda.com/
```

Paquete *foomatic-db-hpijs*

A continuación se muestra la descripción del paquete *foomatic-db-hpijs*. De esta no se obtiene ningún nuevo paquete para instalar.

Ejemplo 14-12. Descripción del paquete *foomatic-db-hpijs*

```
$ /usr/bin/apt-cache show foomatic-db-hpijs
Package: foomatic-db-hpijs
Priority: optional
Section: text
Installed-Size: 4712
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: all
Version: 1.5-20041013-1
Depends: foomatic-filters, foomatic-db, hpijs (>> 1.3)
Conflicts: foomatic-bin (<< 2.9), foomatic-db (<< 2.9)
Filename: pool/main/f/foomatic-db-hpijs/foomatic-db-hpijs_1.5-20041013-1_all.deb
Size: 214228
MD5sum: 161b737f47bca70174237efae2d63ee8
Description: linuxprinting.org printer support - database for HPIJS printers
 Foomatic is a printing system designed to make it easier to set up
 common printers for use with Debian (and other operating systems).
```

```
 It provides the "glue" between a print spooler (like CUPS or lpr) and
 your actual printer, by telling your computer how to process files
 sent to the printer.
 .
 This package includes support for printers using the HPIJS printer
 driver backend, particularly consumer inkjet printers from
 Hewlett-Packard.
 .
 Home Page: http://www.linuxprinting.org/
Task: print-server
```

Análisis de los paquetes *foomatic-db-engine*

Aunque este paquete sugiere y recomienda la instalación de nuevos paquetes, se ha decidido no instalarlos, sólo se mostrará su descripción a modo de información.

Ejemplo 14-13. Descripción de los paquetes *foomatic-db-engine*

```
$ /usr/bin/apt-cache show foomatic-db-engine
Package: foomatic-db-engine
Priority: optional
Section: text
Installed-Size: 704
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: i386
Version: 3.0.2-2
Replaces: foomatic-bin (<< 2.9)
Depends: perl (>= 5.6.0-16), libc6 (>= 2.3.2.ds1-4),
libxml2 (>= 2.6.11), zlib1g (>= 1:1.2.1), foomatic-db, foomatic-filters,
wget | curl
Pre-Depends: bash (>= 2.05)
Recommends: netcat ❶
Suggests: foomatic-db-hpijs, foomatic-db-gimp-print, foomatic-gui ❷
Conflicts: foomatic-bin (<< 2.9), foomatic-db (<< 2.9)
Filename: pool/main/f/foomatic-db-engine/foomatic-db-engine_3.0.2-2_i386.deb
Size: 252714
MD5sum: aed29832cb990e97d859fb9066a06617
Description: linuxprinting.org printer support - programs
 Foomatic is a printing system designed to make it easier to set up
 common printers for use with Debian (and other operating systems).
 It provides the "glue" between a print spooler (like CUPS or lpr) and
 your actual printer, by telling your computer how to process files
 sent to the printer.
 .
 This package contains the architecture-dependent programs needed to
 set up and maintain the foomatic system.  You will also need one or
 more database packages.  The foomatic-db package includes drivers for
 most common printers using Ghostscript as the print processor, as
 well as some common glue code used in other filter systems.
 .
```

```
 foomatic-db-hpijs includes support for photo-quality printing with
 Hewlett-Packard and some other consumer inkjets using the HPIJS
 backend developed by HP.
 .
 foomatic-db-gimp-print includes support for photo-quality printing
 with many consumer inkjets (including those from HP and Epson).
 .
 foomatic-gui provides a GNOME-based setup tool for Foomatic printer
 queues using the command-line tools provided in this package.
 .
 Home Page: http://www.linuxprinting.org/
Task: print-server
```

❶ La navaja suiza del protocolo TCP/IP.

❷ Interfaz gráfica de configuración del sistema de filtrado Foomatic.

Paquetes netcat y foomatic-gui

Ejemplo 14-14. Descripción de los paquetes *netcat* y *foomatic-gui*

```
$ /usr/bin/apt-cache show netcat \
                         foomatic-gui
Package: netcat
Priority: optional
Section: net
Installed-Size: 176
Maintainer: Decklin Foster <decklin@red-bean.com>
Architecture: i386
Version: 1.10-26
Depends: libc6 (>= 2.3.2.ds1-4)
Filename: pool/main/n/netcat/netcat_1.10-26_i386.deb
Size: 66302
MD5sum: 3273445ba7953c3c827872d6c474053b
Description: TCP/IP swiss army knife
 A simple Unix utility which reads and writes data across network
 connections using TCP or UDP protocol.  It is designed to be a reliable
 "back-end" tool that can be used directly or easily driven by other
 programs and scripts. At the same time it is a feature-rich network
 debugging and exploration tool, since it can create almost any kind of
 connection you would need and has several interesting built-in
 capabilities.

Package: foomatic-gui
Priority: optional
Section: gnome
Installed-Size: 248
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: all
Version: 0.6.7
Depends: python (>> 2.3), python (<< 2.4), foomatic-db-engine, python-gnome2,
```

```
python-glade2, netcat, pconf-detect, nmap, smbclient, gksu
Filename: pool/main/f/foomatic-gui/foomatic-gui_0.6.7_all.deb
Size: 58252
MD5sum: 3720f90cb004a41a24b19f07ca8bdf23
Description: GNOME interface for configuring the Foomatic printer filter system
 Foomatic is a printing system designed to make it easier to set up
 common printers for use with Debian (and other operating systems).
 It provides the "glue" between a print spooler (like CUPS or lpr) and
 your actual printer, by telling your computer how to process files
 sent to the printer.
 .
 This package includes a GNOME-based graphical user interface to simplify
 configuring printers that use Foomatic.
 .
 Project Home: http://savannah.nongnu.org/projects/foomatic-gui/
 Development weblog: http://blog.lordsutch.com/?topic=13
Task: print-server
```

Análisis del paquete *foomatic-filters*

A partir de la descripción de este paquete no se obtiene ningún otro para la instalación. Los motivos son que los posibles paquetes sujetos a la instalación, ya se han seleccionado en secciones anteriores o ya se encuentran instalados en el sistema.

> **Importante:** Se da por supuesto que ya tiene instalado en el sistema las herramientas de conversión de archivos de texto a archivos PostScript (vea el siguiente ejemplo para más detalles), si no posee ninguna de estas herramientas instaladas, sería recomendable que lo hiciese.

Ejemplo 14-15. Descripción del paquete *foomatic-filters*

```
$ /usr/bin/apt-cache show foomatic-filters
Package: foomatic-filters
Priority: optional
Section: text
Installed-Size: 324
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: all
Version: 3.0.2-1
Replaces: foomatic-bin (<< 2.9), cupsomatic-ppd
Depends: perl, debconf (>= 0.5) | debconf-2.0, ucf (>= 0.30)
Pre-Depends: bash (>= 2.05)
Recommends: cupsys-client | lpr | lprng | pdq | rlpr, gs-esp | gs,
cupsys | enscript ❶ | a2ps ❷ | mpage ❸, foomatic-db-engine
Conflicts: foomatic-bin (<< 2.9), cupsomatic-ppd (<< 20030507)
Filename: pool/main/f/foomatic-filters/foomatic-filters_3.0.2-1_all.deb
Size: 123842
MD5sum: ba5f0f7710be13d2a131c5d16cd8cec5
```

```
Description: linuxprinting.org printer support - filters
 Foomatic is a printer database designed to make it easier to set up
 common printers for use with Debian (and other operating systems).
 It provides the "glue" between a print spooler (like CUPS or lpr) and
 your actual printer, by telling your computer how to process files
 sent to the printer.
 .
 This package consists of filter scripts used by the printer spoolers
 to convert the incoming PostScript data into the printer's native
 format using a printer-specific, but spooler-independent PPD file.
 You will need to install the foomatic-db-engine package and its
 dependencies for this package to be useful.
 .
 For use with CUPS, you will need both the cupsys and cupsys-client
 packages installed on your system.
 .
 Home Page: http://www.linuxprinting.org/
```

❶❷❸Estos tres paquetes proveen una serie de herramientas para convertir archivos, normalmente de texto, en formato PostScript.

Es imprescindible tener al menos uno de estos paquetes instalados en el sistema. Será labor del administrador elegir cual se instala.

Análisis del paquete *cupsomatic-ppd*

Ejemplo 14-16. Descripción del paquete *cupsomatic-ppd*

```
$ /usr/bin/apt-cache show cupsomatic-ppd
Package: cupsomatic-ppd
Priority: optional
Section: text
Installed-Size: 12
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: all
Source: foomatic-filters-ppds
Version: 20041013-1
Depends: foomatic-filters-ppds ❶
Filename: pool/main/f/foomatic-filters-ppds/cupsomatic-ppd_20041013-1_all.deb
Size: 2588
MD5sum: 6474bf484cd5a424134e301b1dd928a3
Description: linuxprinting.org printer support - transition package
 Foomatic is a printer database designed to make it easier to set up
 common printers for use with Debian (and other operating systems).
 It provides the "glue" between a print spooler (like CUPS or lpr) and
 your actual printer, by telling your computer how to process files
 sent to the printer.
```

```
 .
 This package depends on the foomatic-filters-ppds package, which
 replaces the functionality of this package.  This package can be
 safely removed once you have installed foomatic-filters-ppds.
 .
 Home Page: http://www.linuxprinting.org/
```

❶ Archivos PPD que se adaptan a la especificación de Adobe.

Un nuevo paquete para la lista de instalación:

- *foomatic-filters-ppds*

Paquete *foomatic-filters-ppds*

Esta sección no tiene más sentido que el mostrar la descripción del paquete que se va a instalar, para obtener una visión más amplia de las modificaciones que se van a introducir en el sistema.

Ejemplo 14-17. Descripción del paquete *foomatic-filters-ppds*

```
$ /usr/bin/apt-cache show foomatic-filters-ppds
Package: foomatic-filters-ppds
Priority: extra
Section: text
Installed-Size: 10616
Maintainer: Chris Lawrence <lawrencc@debian.org>
Architecture: all
Version: 20041013-1
Replaces: cupsomatic-ppd (<< 20030507)
Depends: foomatic-db-engine
Recommends: cupsys
Suggests: foomatic-db-hpijs, foomatic-db-gimp-print, foo2zjs
Conflicts: cupsomatic-ppd (<< 20030507)
Filename: pool/main/f/foomatic-filters-ppds/foomatic-filters-ppds_20041013-1_all.deb
Size: 6145132
MD5sum: 249f8685a14a4b7b05a8a74cb4621134
Description: linuxprinting.org printer support - prebuilt PPD files
 Foomatic is a printer database designed to make it easier to set up
 common printers for use with Debian (and other operating systems).
 It provides the "glue" between a print spooler (like CUPS or lpr) and
 your actual printer, by telling your computer how to process files
 sent to the printer.
 .
 This package provides Adobe-compliant PPD files for *every single
 printer* supported by Foomatic.  Unless you want to be able to select
 your printer from the web interface of CUPS or PPR, you almost
 certainly don't want this package.  Instead, you can use the
 "foomatic-configure" script in foomatic-db-engine, the "foomatic-gui"
 package, or the web interface for getting a particular PPD file at
 http://www.linuxprinting.org/printer_list.cgi
```

```
 .
 Again, you probably don’t want this package unless you have a lot of
 disk space to spare and/or using the CUPS or PPR web interface to set
 up your printer queue is important to you.
 .
 Home Page: http://www.linuxprinting.org/
Task: print-server
```

Lista completa de paquetes a instalar

Juntando todos los paquetes que se han ido seleccionando para la instalación, el conjunto de los mismos queda como sigue:

- *cupsys*
- *cupsys-client*
- *cupsys-bsd*
- *cupsys-driver-gimpprint*
- *foomatic-bin*
- *cupsomatic-ppd*
- *gsfonts*
- *psfontmgr*
- *kdeprint*
- *gimpprint-locales*
- *foomatic-db-gimp-print*
- *foomatic-filters-ppds*

A la lista anterior se ha de sumar un paquete más, que se instalará posteriormente. El paquete en cuestión es *cups-pdf*, que no es más que una impresora PDF virtual: todo el trabajo de impresión que procese lo convierte a un archivo PDF. Esta impresora será la impresora utilizada para la realización de las pruebas, al no disponer de una impresora real.

> **Nota:** Para completar el análisis de paquetes relacionados con CUPS, habría que hacer una búsqueda en la base de datos de paquetes disponibles y seleccionar aquellos que se consideren necesarios.
>
> La búsqueda se puede realizar con la siguiente orden: **/usr/bin/apt-cache search cups**. Esta orden devolverá una lista con aquellos paquetes cuya descripción posea la palabra *cups*. De la lista devuelta, los paquetes más interesantes son:
>
> - *bluez-cups*
> - *cups-pdf*
> - *escputil*

- *hpoj*

De la lista anterior, el único paquete que se va a instalar es el *cups-pdf*, como ya se ha dicho.

Instalando los paquetes

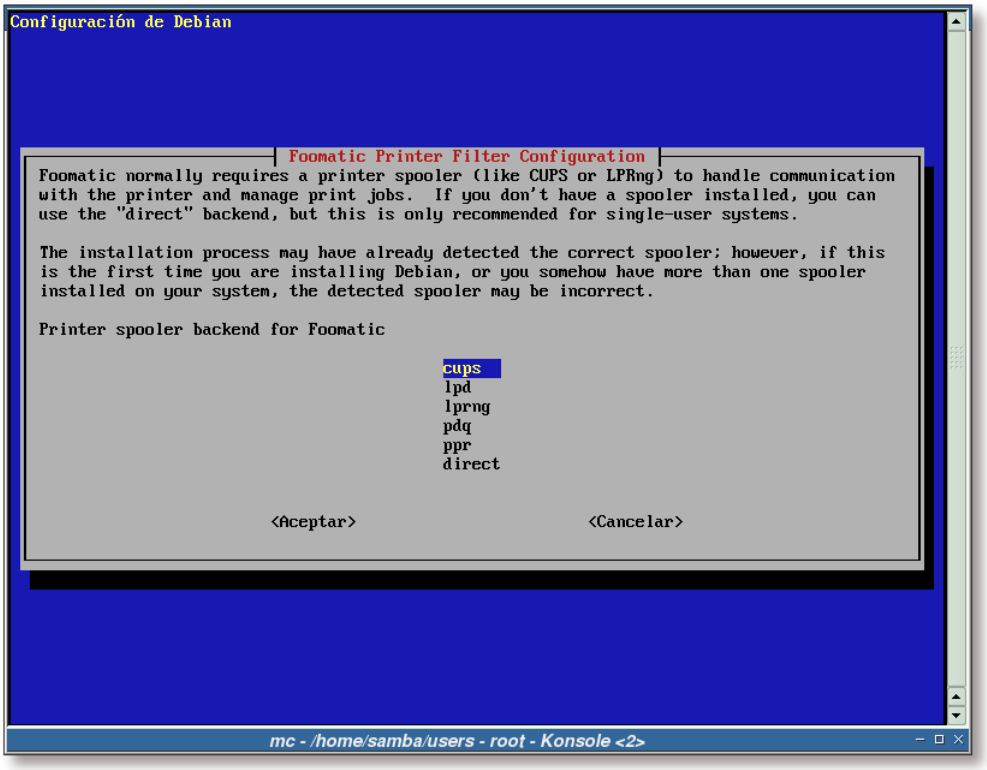
En esta se mostrará el proceso de instalación de los paquetes seleccionados en la sección anterior, la sección de nombre *Elección de los paquetes necesarios.* La lista completa de paquetes necesarios se encuentra en la la sección de nombre *Lista completa de paquetes a instalar*. El siguiente ejemplo muestra el proceso de instalación de dichos paquetes:

Ejemplo 14-18. Instalación del sistema de impresión CUPS (primera parte)

```
# /usr/bin/apt-get install cupsys cupsys-client cupsys-bsd \
                           cupsys-driver-gimpprint foomatic-bin \
                           cupsomatic-ppd gsfonts psfontmgr \
                           kdeprint gimpprint-locales \
                           foomatic-db-gimp-print \
                           foomatic-filters-ppds
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
gsfonts ya está en su versión más reciente. ❶
psfontmgr ya está en su versión más reciente. ❷
kdeprint ya está en su versión más reciente. ❸
Se instalarán los siguientes paquetes extras:
  cupsys-driver-gimpprint-data foomatic-db foomatic-db-engine foomatic-db-hpijs
  foomatic-filters gs-esp hpijs ijsgimpprint libcupsimage2 libijs-0.35
Paquetes sugeridos:
  xpdf-korean xpdf-japanese xpdf-chinese-traditional xpdf-chinese-simplified gtklp cupsys-pt
  xpp gimpprint-doc foo2zjs foomatic-gui hpoj
Paquetes recomendados
  xpdf-common
Se instalarán los siguientes paquetes NUEVOS:
  cupsomatic-ppd cupsys cupsys-bsd cupsys-client cupsys-driver-gimpprint
  cupsys-driver-gimpprint-data foomatic-bin foomatic-db foomatic-db-engine
  foomatic-db-gimp-print foomatic-db-hpijs foomatic-filters foomatic-filters-ppds
  gimpprint-locales gs-esp hpijs ijsgimpprint libcupsimage2 libijs-0.35
0 actualizados, 19 se instalarán, 0 para eliminar y 0 no actualizados.
0 actualizados, 19 se instalarán, 0 para eliminar y 2 no actualizados.
Se necesita descargar 0B/17,1MB de archivos.
Se utilizarán 67,8MB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n] S
Preconfiguring packages ...
```

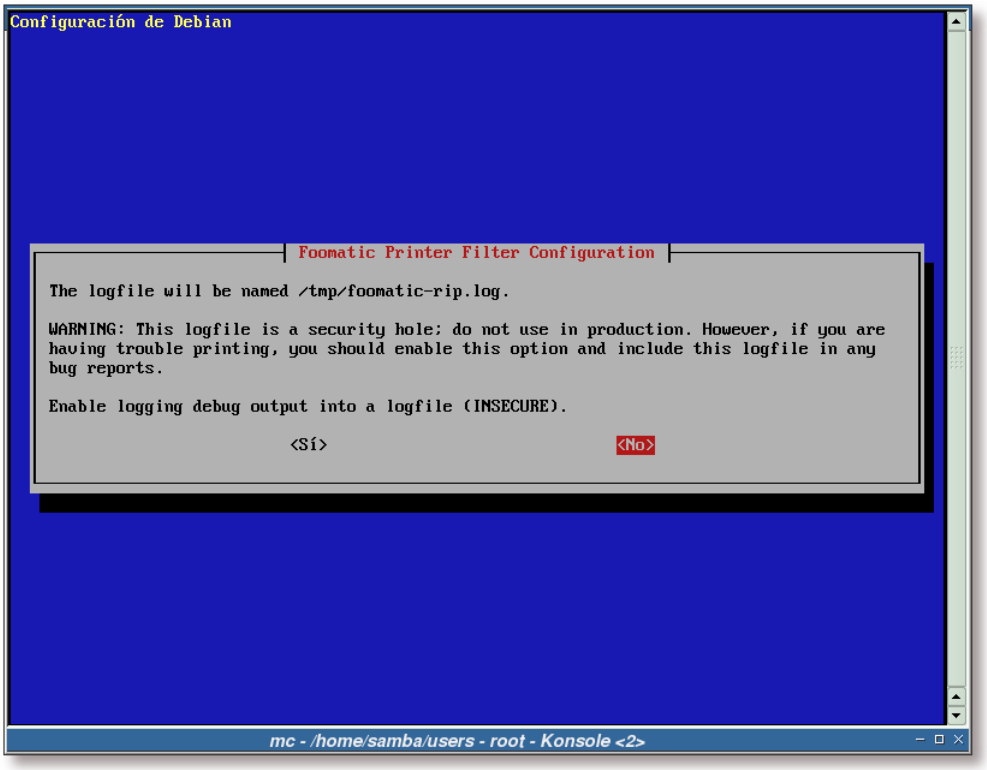
❶❷❸En el sistema donde se han realizado las pruebas ya se encontraban instalados estos paquetes.

Figura 14-1. *Backend* de impresión para Foomatic



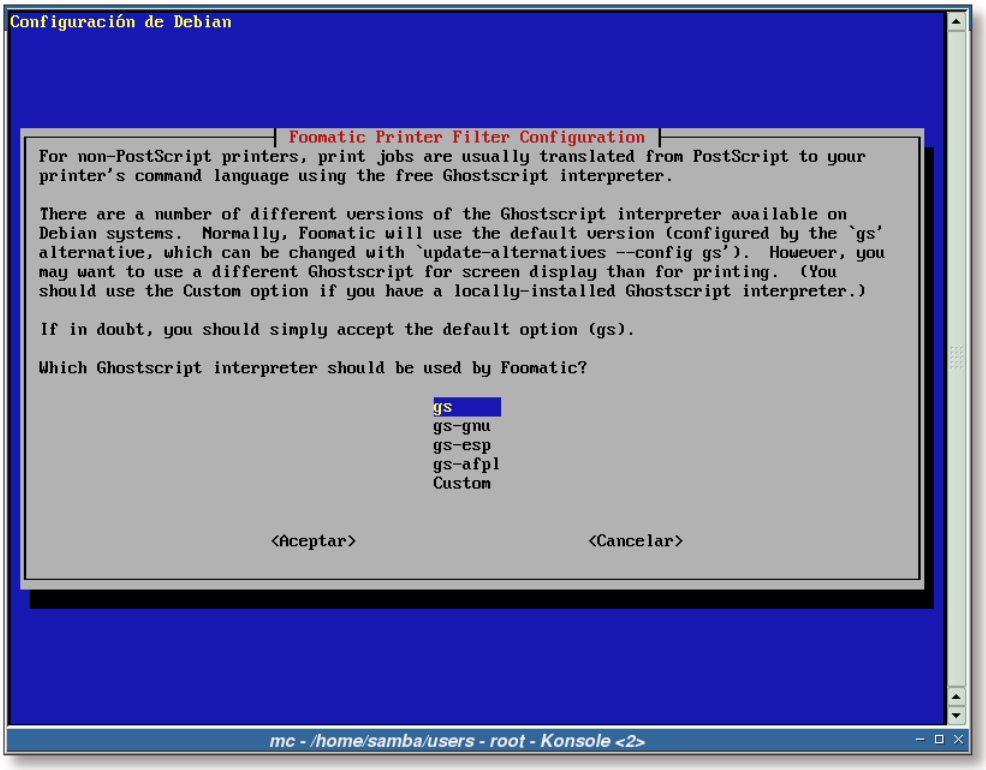
Seleccione la cola de impresión que desea que utilice *Foomatic* para los trabajos de impresión. Como en esta documentación se va a emplear CUPS, se ha elegido esta opción.

Figura 14-2. Configuración del filtro de impresión Foomatic



Foomatic permite la creación de un archivo de log, sobre el que volcará los informes de depuración. La creación de este archivo supone un riesgo de seguridad en el sistema, por lo que se recomienda no instalarlo, a no ser que lo necesite para analizar su comportamiento.

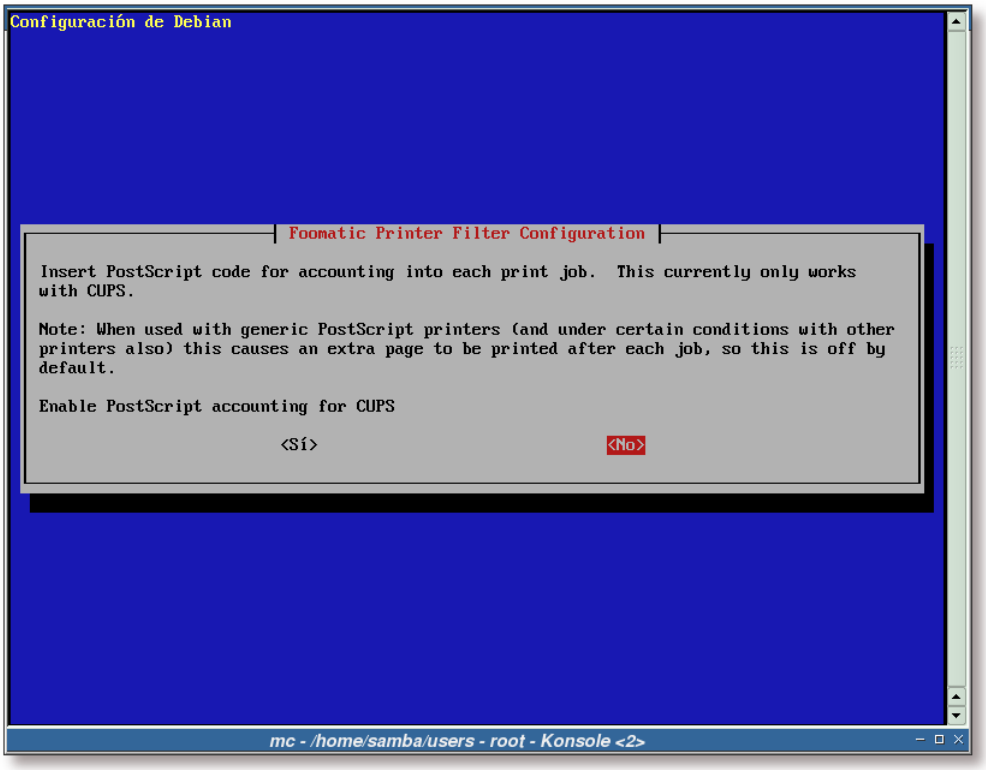
Figura 14-3. Selección del intérprete Ghostscript



Se recomienda seleccionar la opción *gs*, de forma que se elegirá el intérprete de Ghostscript seleccionado en las *alternativas* de Debian.

Si en un determinado momento quiere cambiar el intérprete de Ghostscript predeterminado, sólo ha de ejecutar: **/usr/sbin/update-alternatives --config gs** y seleccionar aquel que desee.

Figura 14-4. Insertar información de contabilidad en cada trabajo

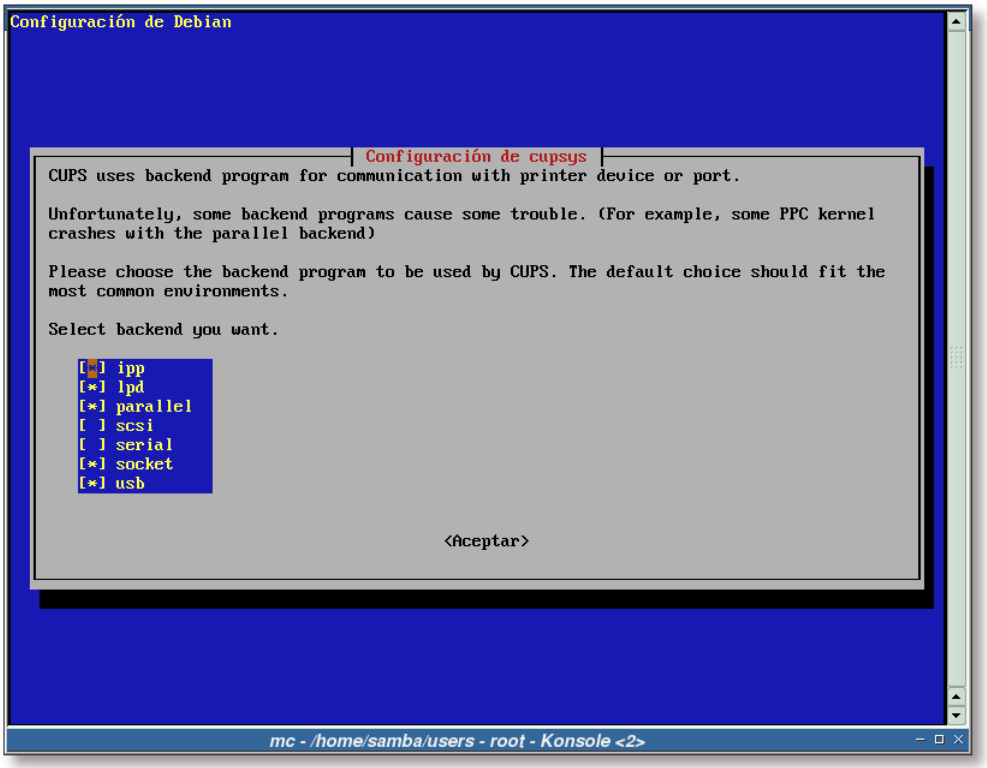


Respondemos negativamente a esta pregunta, debido a que se utilizará un programa externo, PyKota, para la gestión de quotas de impresión.

Figura 14-5. Trabajos sin tipo MIME

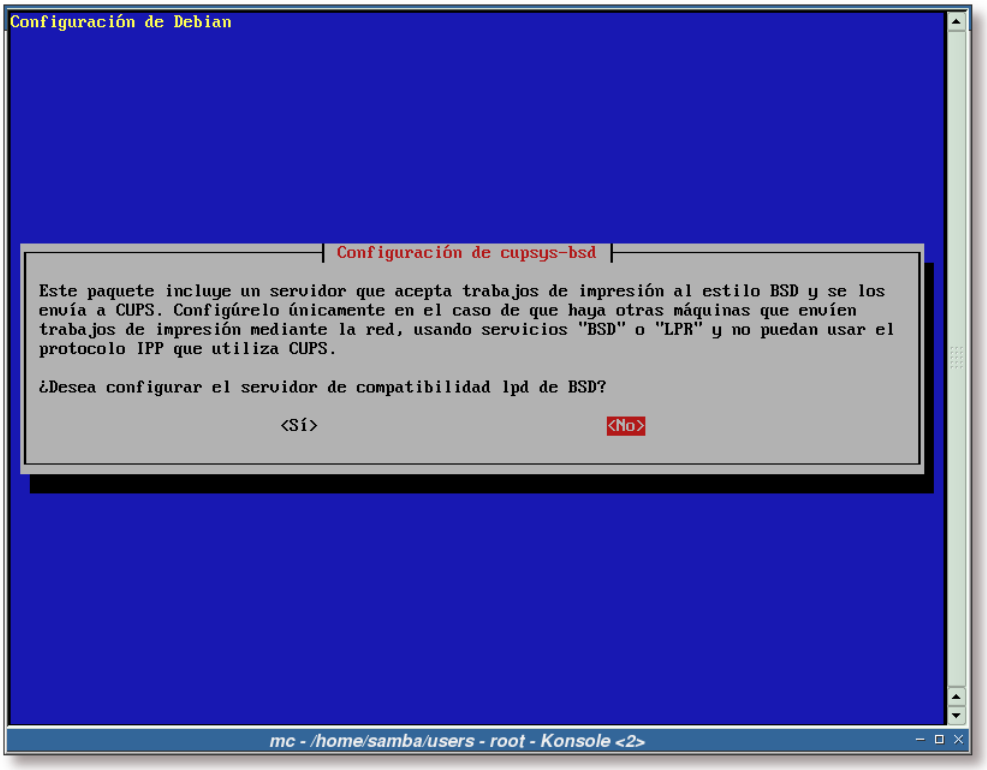
Aquellos trabajos que no lleven adjunto un tipo MIME, serán enviados a la impresora tal cual, sin ningún tipo de preprocesado.

Figura 14-6. Selección de *backends* para CUPS



En esta pantalla se seleccionarán los *backends* que utilizará CUPS a la hora de imprimir.

Figura 14-7. Compatibilidad lpd de BSD



No se activa la compatibilidad lpd de BSD en este caso, por no ser necesaria. Puede que en su caso esta situación sea distinta...

Ejemplo 14-19. Instalación del sistema de impresión CUPS (segunda parte)

```
Seleccionando el paquete foomatic-filters previamente no seleccionado.
(Leyendo la base de datos ...
135345 ficheros y directorios instalados actualmente.)
Desempaquetando foomatic-filters (de .../foomatic-filters_3.0.2-1_all.deb) ...
Seleccionando el paquete foomatic-db previamente no seleccionado.
Desempaquetando foomatic-db (de .../foomatic-db_20041013-1-1_all.deb) ...
Seleccionando el paquete foomatic-db-engine previamente no seleccionado.
Desempaquetando foomatic-db-engine (de .../foomatic-db-engine_3.0.2-2_i386.deb) ...
Seleccionando el paquete foomatic-filters-ppds previamente no seleccionado.
Desempaquetando foomatic-filters-ppds (de .../foomatic-filters-ppds_20041013-1_all.deb) ...
Seleccionando el paquete cupsomatic-ppd previamente no seleccionado.
Desempaquetando cupsomatic-ppd (de .../cupsomatic-ppd_20041013-1_all.deb) ...
Seleccionando el paquete libcupsimage2 previamente no seleccionado.
Desempaquetando libcupsimage2 (de .../libcupsimage2_1.1.20final+rc1-9_i386.deb) ...
Seleccionando el paquete gs-esp previamente no seleccionado.
Desempaquetando gs-esp (de .../gs-esp_7.07.1-9_i386.deb) ...
Seleccionando el paquete cupsys previamente no seleccionado.
```

```
Desempaquetando cupsys (de .../cupsys_1.1.20final+rc1-9_i386.deb) ...
Seleccionando el paquete cupsys-client previamente no seleccionado.
Desempaquetando cupsys-client (de .../cupsys-client_1.1.20final+rc1-9_i386.deb) ...
Seleccionando el paquete cupsys-driver-gimpprint-data previamente no seleccionado.
Desempaquetando cupsys-driver-gimpprint-data (de .../cupsys-driver-gimpprint-data_4.2.7-4_all.deb)
Seleccionando el paquete cupsys-driver-gimpprint previamente no seleccionado.
Desempaquetando cupsys-driver-gimpprint (de .../cupsys-driver-gimpprint_4.2.7-4_i386.deb) ...
Seleccionando el paquete hpijs previamente no seleccionado.
Desempaquetando hpijs (de .../hpijs_1.6.2-1_i386.deb) ...
Seleccionando el paquete foomatic-db-hpijs previamente no seleccionado.
Desempaquetando foomatic-db-hpijs (de .../foomatic-db-hpijs_1.5-20041013-1_all.deb) ...
Seleccionando el paquete foomatic-bin previamente no seleccionado.
Desempaquetando foomatic-bin (de .../foomatic-bin_3.0.2-2_all.deb) ...
Seleccionando el paquete libijs-0.35 previamente no seleccionado.
Desempaquetando libijs-0.35 (de .../libijs-0.35_0.35-1_i386.deb) ...
Seleccionando el paquete ijsgimpprint previamente no seleccionado.
Desempaquetando ijsgimpprint (de .../ijsgimpprint_4.2.7-4_i386.deb) ...
Seleccionando el paquete foomatic-db-gimp-print previamente no seleccionado.
Desempaquetando foomatic-db-gimp-print (de .../foomatic-db-gimp-print_4.2.7-4_all.deb) ...
Seleccionando el paquete gimpprint-locales previamente no seleccionado.
Desempaquetando gimpprint-locales (de .../gimpprint-locales_4.2.7-4_all.deb) ...
Seleccionando el paquete cupsys-bsd previamente no seleccionado.
Desempaquetando cupsys-bsd (de .../cupsys-bsd_1.1.20final+rc1-9_i386.deb) ...
Configurando foomatic-filters (3.0.2-1) ...

Creating config file /etc/foomatic/filter.conf with new version

Configurando foomatic-db (20041013-1) ...
Configurando foomatic-db-engine (3.0.2-2) ...
Configurando foomatic-filters-ppds (20041013-1) ...
invoke-rc.d: unknown initscript, /etc/init.d/cupsys not found.

Configurando cupsomatic-ppd (20041013-1) ...
Configurando libcupsimage2 (1.1.20final+rc1-9) ...

Configurando gs-esp (7.07.1-9) ...

Configurando cupsys (1.1.20final+rc1-9) ...
Adding group ‘lpadmin’ (116)...
Hecho.
Starting printing system service: cupsd.

Configurando cupsys-client (1.1.20final+rc1-9) ...
Configurando hpijs (1.6.2-1) ...
Configurando foomatic-db-hpijs (1.5-20041013-1) ...
Configurando foomatic-bin (3.0.2-2) ...
Configurando libijs-0.35 (0.35-1) ...

Configurando ijsgimpprint (4.2.7-4) ...
Configurando foomatic-db-gimp-print (4.2.7-4) ...
Configurando gimpprint-locales (4.2.7-4) ...
Configurando cupsys-bsd (1.1.20final+rc1-9) ...
```

```
Configurando cupsys-driver-gimpprint-data (4.2.7-4) ...
Configurando cupsys-driver-gimpprint (4.2.7-4) ...
No Gimp-Print PPD files to update.
Reloading printing system service: cupsd.
```

Instalación del paquete *cups-pdf*

Esta sección está dedicada a la instalación de lo que será la impresora del proyecto.

Como ya se ha comentado anteriormente (la sección de nombre *Lista completa de paquetes a instalar*), el paquete *cups-pdf* añadirá un nuevo *backend* al servidor CUPS, desde el cual se podrán crear impresoras virtuales. Estas impresoras convertirán los trabajos de impresión a archivos PDF.

El siguiente ejemplo muestra el proceso de instalación de este paquete:

Ejemplo 14-20. Instalación del paquete *cups-pdf*

```
# /usr/bin/apt-get install cups-pdf
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Paquetes sugeridos:
  gnome-cups-manager
Se instalarán los siguientes paquetes NUEVOS:
  cups-pdf
0 actualizados, 1 se instalarán, 0 para eliminar y 2 no actualizados.
Se necesita descargar 0B/15,4kB de archivos.
Se utilizarán 106kB de espacio de disco adicional después de desempaquetar.
Seleccionando el paquete cups-pdf previamente no seleccionado.
(Leyendo la base de datos ...
140777 ficheros y directorios instalados actualmente.)
Desempaquetando cups-pdf (de .../cups-pdf_1.6.3-1_i386.deb) ...
Configurando cups-pdf (1.6.3-1) ...
Restarting printing system service: cupsd.
```

Los documentos PDF generados por las impresoras virtuales se almacenarán en el directorio: `$HOME/cups-pdf`. (Más datos en `/usr/share/doc/cups-pdf/README.Debian`).

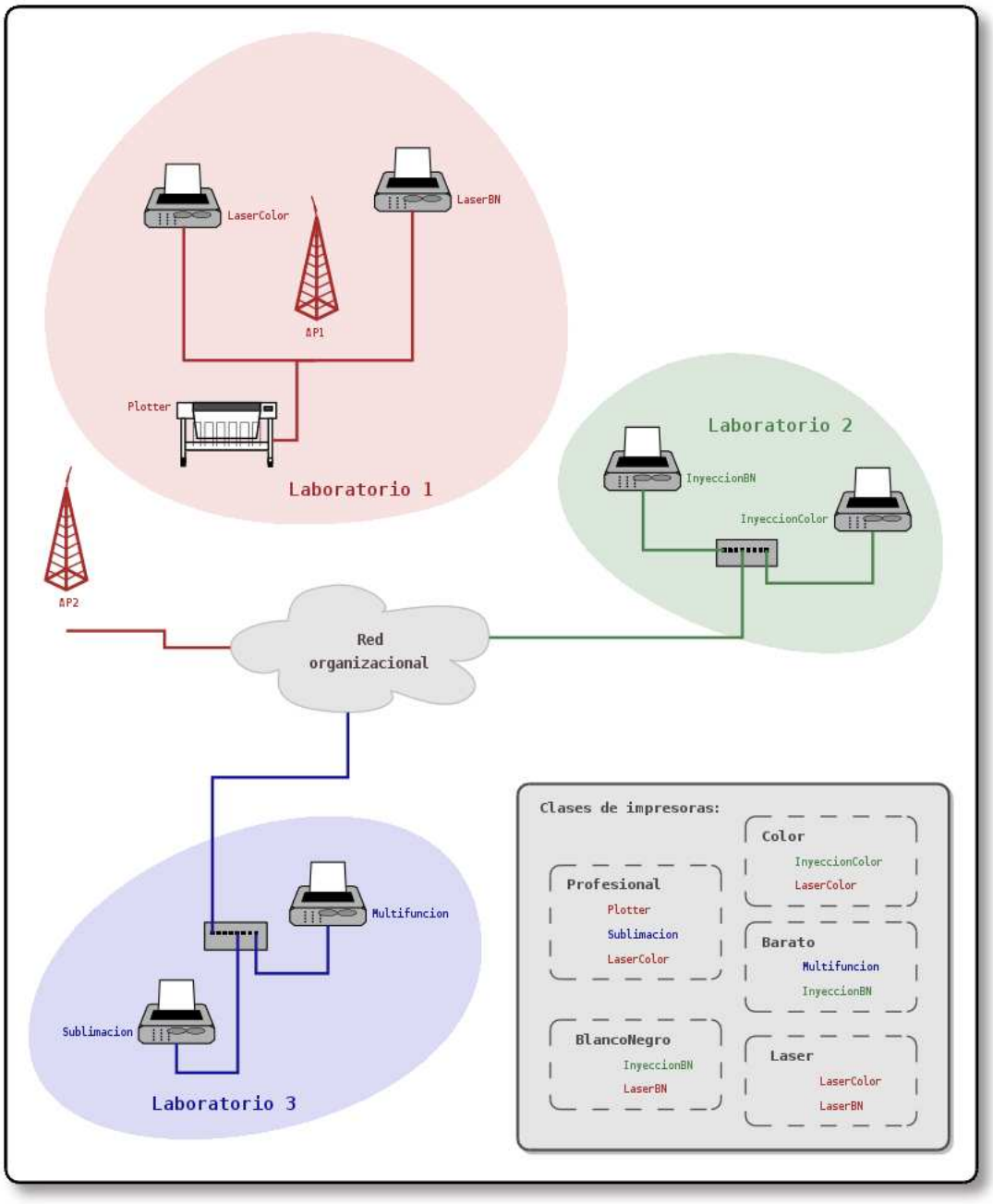
Con este paquete finalizaría la parte de instalación de CUPS, en las siguientes secciones se verán las modificaciones y configuración que se han de realizar al sistema.

Capítulo 15. Configuración

Introducción

Este capítulo comienza con la realización de unas comprobaciones en el sistema relacionadas con Samba. Luego se configurarán algunos aspectos necesarios para la integración de CUPS en LDAP, la interactuación con los clientes MS Windows, etc. Y finalmente, se simulará la siguiente red de impresión:

Figura 15-1. Estructura de la red de impresión



Red de impresión que se simulará en CUPS. Esta red está formada por tres laboratorios, en los cuales hay una serie de impresoras. La interconexión de los laboratorios se ha realizado mediante cable y red inalámbrica.

Las impresoras se han agrupado en 5 clases, como se puede observar en la imagen. Las clases de impresoras definidas en este ejemplo no serían muy útiles en un entorno real por diversos motivos; pero sirvan para ilustrar su funcionamiento.

Si quiere obtener el código fuente de esta imagen, generado con el programa de diagramas Dia, pulse aquí (./imagenes/cups-red-impresoras.dia).

Nota: La bibliografía consultada, mayoritariamente, para la realización de este capítulo ha sido: el capítulo 18 de la entrada bibliográfica VernooijTerpstraCarter01 y la entrada bibliográfica CUPS02.

Comprobaciones iniciales

Antes de proceder con la configuración de CUPS, se va a comprobar que el servidor Samba está preparado para funcionar junto con CUPS. Esta comprobación se realizará con la orden **ldd**, que nos mostrará las librerías compartidas que utiliza el demonio **smbd**, en este caso. Si entre estas librerías se encuentra la de CUPS, es que Samba ha sido compilado con soporte para este sistema de impresión:

Ejemplo 15-1. Verificando que Samba se ha compilado con soporte para CUPS

```
$ /usr/bin/ldd ‘which smbd‘ | /bin/grep "cups"
        libcups.so.2 => /usr/lib/libcups.so.2 (0x40109000)
```

Con el ejemplo anterior se comprueba que Samba ha sido compilado con soporte para CUPS. El siguiente paso va a ser el reinicio de Samba, para comprobar que ya no da error al no encontrar un servidor CUPS en el sistema (vea Samba no puede contactar con el servidor CUPS para más detalles).

El procedimiento para reiniciar Samba está descrito en el Ejemplo 11-3. Una vez se ha reiniciado el servidor Samba, se analiza el archivo de log `/var/log/samba/log.smbd` para ver si se produce algún error relacionado con CUPS, como ocurría en: Samba no puede contactar con el servidor CUPS:

```
[2004/10/09 20:13:22, 0] smbd/server.c:main(760)
  smbd version 3.0.7-Debian started.
  Copyright Andrew Tridgell and the Samba Team 1992-2004
```

Se puede comprobar, que ahora ya no se produce ningún error en el arranque del demonio **smbd** al disponer el sistema de un servidor de impresión CUPS.

Modificaciones en la configuración del sistema

Para conseguir integrar CUPS en el sistema, tal y como se ha configurado hasta el momento, es necesario realizar algunas modificaciones, que se muestran en las siguientes secciones.

Modificaciones de PAM

Se ha de añadir al sistema de autentificación de CUPS, la posibilidad de utilizar usuarios almacenados en la base de datos de LDAP. Esto se realiza en el archivo `/etc/pam.d/cupsys`. Si se echa un vistazo a su

contenido, se comprobará que no es necesario realizar ninguna modificación al mismo, ya que en la la sección de nombre *Configuración de PAM* en Capítulo 5 se han realizado todas las modificaciones necesarias.

```
@include common-auth
@include common-account
@include common-session
```

Modificaciones en Samba

Es necesario realizar una pequeña revisión en la configuración de Samba, los cambios se muestran a continuación:

Ejemplo 15-2. Diferencia entre la configuración de Samba antes y después de instalar CUPS

```
$ /usr/bin/diff -u /etc/samba/smb.conf-antes /etc/samba/smb.conf
--- /etc/samba/smb.conf-antes     2004-06-15 16:17:19.000000000 +0100
+++ /etc/samba/smb.conf    2004-06-15 16:15:48.000000000 +0100
@@ -188,7 +188,7 @@
 # When using [print$], root is implicitly a 'printer admin', but you can
 # also give this right to other users to add drivers and set printer
 # properties
-   printer admin = @domainadmins
+   printer admin = @domainprintoperator ❶


 ######## File sharing ########
@@ -327,13 +327,15 @@

 [printers]
    comment = All Printers
-   path = /tmp
+   path = /var/spool/samba ❷
    browseable = no
    public = yes
    guest ok = no
    writable = no
    printable = yes
    create mask = 0700
+   use client driver = no ❸
+   printer admin = root, @domainprintoperator ❹

 # Windows clients look for this share name as a source of downloadable
 # printer drivers
@@ -343,7 +345,7 @@
    browseable = yes
    guest ok = no
    read only = yes
-   write list = root, @domainadmins
+   write list = root, @domainprintoperator ❺
```

```
[tmp]
   comment = Temporal
```

❷ Se modifica la ruta de la cola de impresión de Samba. Este es un cambio puramente *estético*.

Si no existe el directorio de la cola de impresión para Samba, se tendrá que crear en este momento.

> **Aviso**
>
> Tenga especial cuidado con los permisos que le asigna al directorio `/var/spool/samba`; tenga en cuenta, que todo usuario que quiera imprimir en una impresora compartida por Samba, ha de tener permisos de escritura en dicho directorio.
>
> En este caso, el directorio tiene los siguientes permisos:
>
> ```
> $ /bin/ls -ld /var/spool/samba
> drwxrws---  2 root domainpoweruser 48 \
>                         2004-10-09 20:28 /var/spool/samba
> ```
>
> Note que se ha utilizado el grupo *domainpoweruser*, grupo al que han de pertenecer aquellos usuarios que quieran imprimir vía Samba.

❸ Para saber más acerca de esta opción, se recomienda la lectura de la sección “Raw Print Serving Vendor Drivers on Windows Clients” y “How to Recognize If cupsaddsmb Completed Successfully” del capítulo 18 (*CUPS Printing Support*) de la entrada bibliográfica VernooijTerpstraCarter01; así como la página del manual smb.conf(5).

El valor de esta opción dependerá del comportamiento de su sistema.

❶❹❺En el Grupos adicionales para Samba se propone la opción de añadir los grupos de usuarios listados en el archivo `template_config.php` de la aplicación phpLDAPadmin. Esos grupos ya existen en el sistema empleado para la elaboración de esta documentación, por lo que se hará uso de ellos.

Se selecciona el grupo más adecuado, “domainprintoperator”, para la administración de las impresoras.

Una vez modificada la configuración de Samba, este servidor ha de releer su configuración. En el Ejemplo 11-2 se muestra como hacerlo.

Modificaciones relativas a CUPS

Nota: Para realizar esta sección se ha consultado, principalmente, la entrada bibliográfica CUPS02.

Archivo `/etc/cups/client.conf`

En este archivo se descomentarán dos líneas, la primera hace referencia al servidor donde está instalado CUPS y la segunda al uso o no de cifrado:

```
ServerName gsr.pt ❶
```

```
Encryption Required ❷
```

❶ Se especifica donde está alojado el servidor CUPS.

❷ Se hace uso del cifrado TLS en las comunicaciones.

Nota: En el Apéndice AE tiene un ejemplo completo de este archivo de configuración.

Archivo `/etc/cups/cupsd.conf`

El archivo de configuración `cupsd.conf` está estructurado en secciones, por este motivo, las opciones de configuración más importantes se irán mostrando en sucesivas secciones, que se corresponderán con las secciones del archivo tratado.

Nota: En el Apéndice AF tiene un ejemplo completo de este archivo de configuración.

Server Identity

```
ServerName gsr.pt ❶
ServerAdmin sergio@gsr.pt ❷
```

❶ Nombre del servidor donde está alojado CUPS.

❷ Dirección de correo del administrador de impresión.

Encryption Support

Se han utilizado los mismos certificados creados en la
la sección de nombre *Certificado emitido por una CA* en Capítulo 4, por este motivo se ha copiado el directorio `/etc/ldap/ssl/` a `/etc/cups`.

Ejemplo 15-3. Copiando el contenido del directorio `/etc/ldap/ssl/` a `/etc/cups`

```
# /bin/cp -va /etc/ldap/ssl/ /etc/cups/
«/etc/ldap/ssl/» -> «/etc/cups/ssl»
«/etc/ldap/ssl/crl» -> «/etc/cups/ssl/crl»
«/etc/ldap/ssl/certs» -> «/etc/cups/ssl/certs»
«/etc/ldap/ssl/certs/servidorcert.pem» -> «/etc/cups/ssl/certs/servidorcert.pem»
«/etc/ldap/ssl/index.txt.old» -> «/etc/cups/ssl/index.txt.old»
«/etc/ldap/ssl/index.txt» -> «/etc/cups/ssl/index.txt»
«/etc/ldap/ssl/serial.old» -> «/etc/cups/ssl/serial.old»
«/etc/ldap/ssl/serial» -> «/etc/cups/ssl/serial»
«/etc/ldap/ssl/newcerts» -> «/etc/cups/ssl/newcerts»
«/etc/ldap/ssl/newcerts/01.pem» -> «/etc/cups/ssl/newcerts/01.pem»
«/etc/ldap/ssl/cacert.pem» -> «/etc/cups/ssl/cacert.pem»
```

```
«/etc/ldap/ssl/index.txt.attr» -> «/etc/cups/ssl/index.txt.attr»
«/etc/ldap/ssl/private» -> «/etc/cups/ssl/private»
«/etc/ldap/ssl/private/cakey.pem» -> «/etc/cups/ssl/private/cakey.pem»
«/etc/ldap/ssl/private/servidorkey.pem» -> «/etc/cups/ssl/private/servidorkey.pem»
# /bin/chown root.lpadmin -vR /etc/cups/ssl
cambiado el propietario de «/etc/cups/ssl» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/crl» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/certs» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/certs/servidorcert.pem» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/index.txt.old» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/index.txt» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/serial.old» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/serial» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/newcerts» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/newcerts/01.pem» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/cacert.pem» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/index.txt.attr» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/private» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/private/cakey.pem» a root:lpadmin
cambiado el propietario de «/etc/cups/ssl/private/servidorkey.pem» a root:lpadmin
```

Las opciones de configuración, por tanto, quedarían de la siguiente forma:

```
ServerCertificate /etc/cups/ssl/certs/servidorcert.pem
ServerKey /etc/cups/ssl/private/servidorkey.pem
```

Network Options

Se especifica donde ha de escuchar el servidor CUPS y en que puertos:

```
Listen gsr.pt:631 ❶
SSLListen gsr.pt:6443 ❷
```

❶ Puerto por defecto, destinado a las conexiones sin cifrado.

❷ Puerto destinado a las conexiones con cifrado. Si su sistema no posee el puerto 443 ocupado, sería recomendable utilizarlo.

Security Options

La única modificación que se realizará en esta sección, será obligar a aquellos directorios que precisan autentificación para su acceso, a hacer uso de cifrado. Para ello se utilizará la directiva *Encryption Required*.

```
<Location /jobs>

    AuthType Basic
    AuthClass User

    Encryption Required
```

```
</Location>

<Location /admin>

    AuthType Basic
    AuthClass System

    Order Deny,Allow
    Deny From All
    Allow From 127.0.0.1

    Encryption Required

</Location>
```

Reinicio del servidor CUPS

Una vez se ha finalizado la configuración de CUPS, se ha de reiniciar el servidor, para que relea su configuración:

Ejemplo 15-4. Reinicio del servidor CUPS

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

Creación de la estructura de impresión

En la introducción de este capítulo (la sección de nombre *Introducción*) se mostró la estructura de la red de impresión que se va a simular en esta documentación. De forma simplificada, se crearán siete impresoras[1] y cinco clases.

En las dos siguientes secciones se mostrará la forma de hacer esto, respectivamente.

Creación de las impresoras

Las impresoras que se van a crear a continuación son todas del mismo tipo: impresoras PDF virtuales; el único elemento diferenciador entre ellas será su nombre.

Los nombres de las impresoras serán:

- LaserColor
- LaserBN
- Plotter

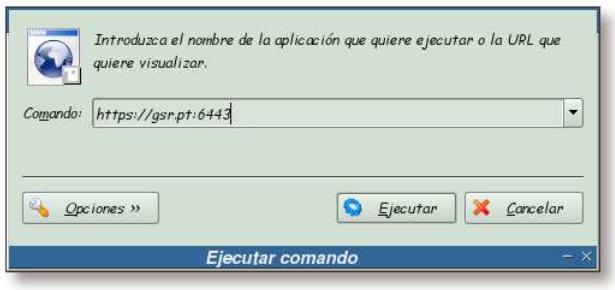
- InyeccionColor
- InyeccionBN
- Sublimacion
- Multifuncion

Las dos secciones siguientes mostrarán como añadir una impresora desde la interfaz de administración web de CUPS y desde el frontend que provee el escritorio KDE para la administración de impresoras.

Añadiendo una impresora desde la interfaz de administración web de CUPS

En esta sección se mostrará el proceso seguido para añadir una impresora desde la interfaz de administración web de CUPS.

Figura 15-2. Accediendo a la interfaz de administración web de CUPS



Si se encuentra en un entorno de escritorio KDE, teclee **Alt**+**F2** e introduzca la dirección donde se encuentre instalado CUPS seguido del puerto donde está escuchando. En este caso: *https://gsr.pt:6443*.

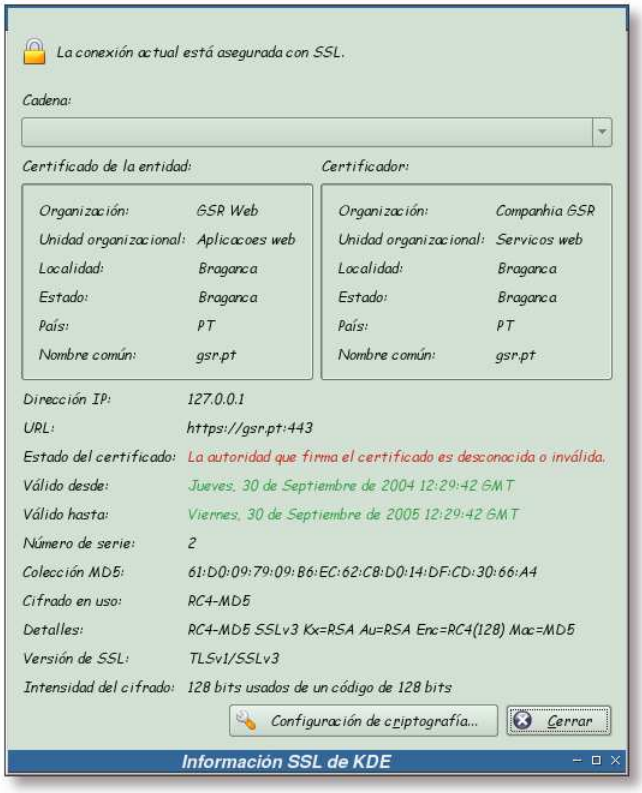
Nota: Si se fija en la URL que se ha tecleado, se ha especificado el protocolo *https* y el puerto de conexión segura de CUPS. Esto es necesario si se quiere hacer uso de cifrado en las comunicaciones con CUPS.

Si no accede de esta forma a la interfaz web de CUPS, no podrá realizar labores de administración, ya que se ha obligado en los archivos de configuración de CUPS, al uso de cifrado en las secciones de administración.

Figura 15-3. Aviso acerca del certificado del servidor web I

Como se ha accedido a la interfaz web de CUPS vía el puerto seguro y debido a que la entidad certificadora que se ha creado para las conexiones SSL/TLS es desconocida, sale este aviso. Pulse sobre el botón *Detalles* para obtener más información.

Figura 15-4. Información SSL



En esta pantalla se muestra la información del certificado y la entidad certificadora que ha creado dicho certificado. Pulse sobre el botón *Cerrar* para continuar.

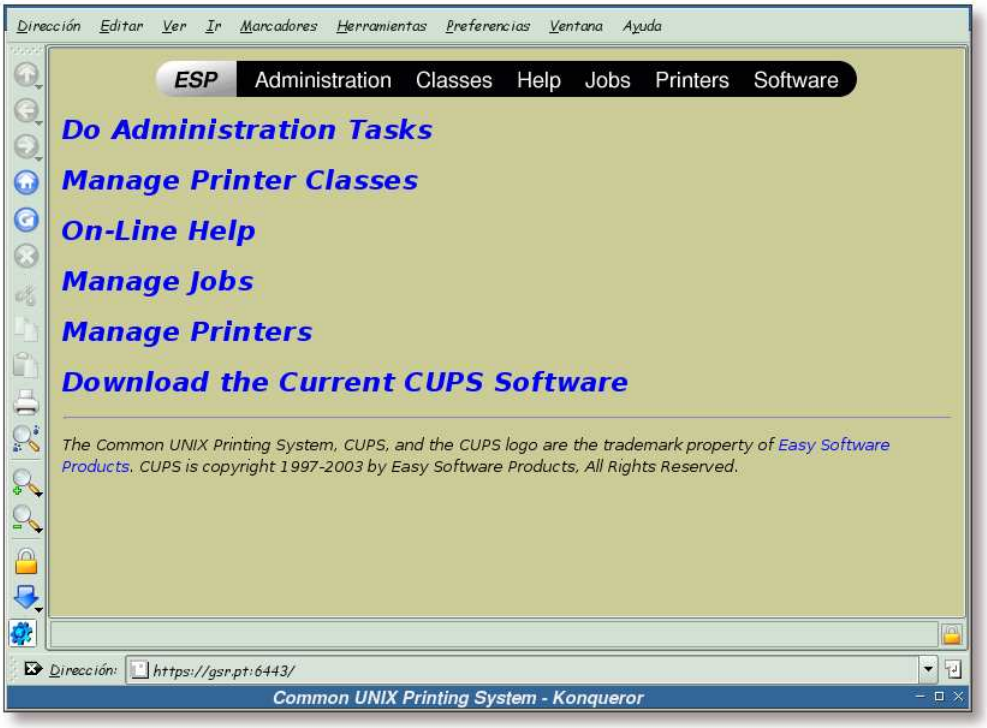
Figura 15-5. Aviso acerca del certificado del servidor web II

Pulse ahora sobre el botón *Continuar* para seguir con la carga de la página.

Figura 15-6. Período de aceptación del certificado

Seleccione la opción deseada y pulse sobre ella.

Figura 15-7. Administrando impresoras

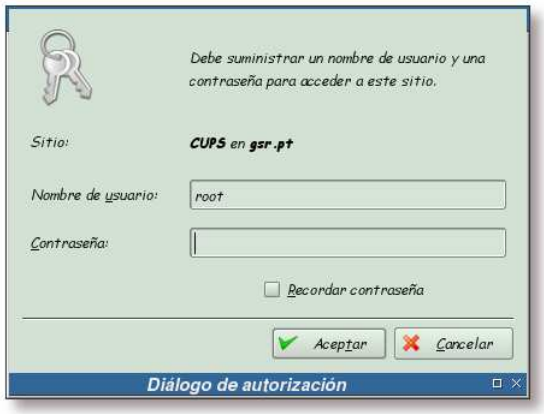


Una vez se tenga acceso al interfaz de administración web de CUPS, pulse sobre el enlace “Manage Printers”.

Figura 15-8. Añadir nueva impresora

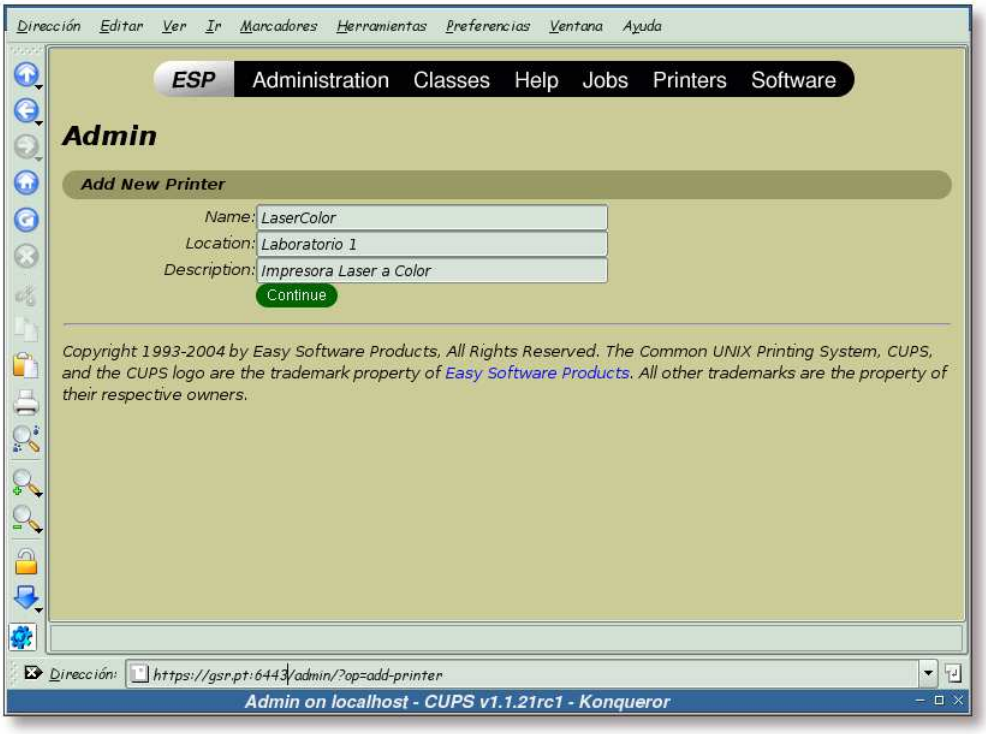
Pulse sobre el botón “Add Printer” para comenzar el proceso de adición de una impresora al sistema.

Figura 15-9. Clave del administrador



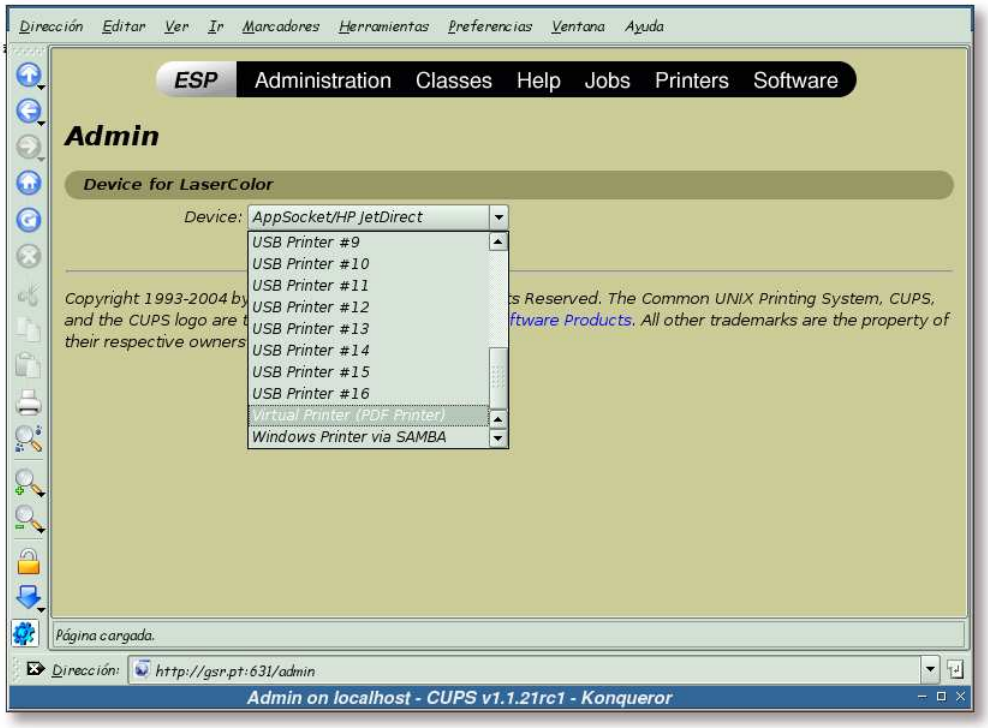
Introduzca un usuario con permisos de administración para el sistema de impresión, así como su clave.

Figura 15-10. Información sobre la impresora



Teclee el nombre, la localización y una breve descripción de la nueva impresora. Procure no introducir caracteres especiales ni espacios en el nombre de la impresora.

Figura 15-11. Dispositivo de impresión I



Seleccione el tipo *Virtual Printer (PDF Printer)* como dispositivo de impresión...

Aviso

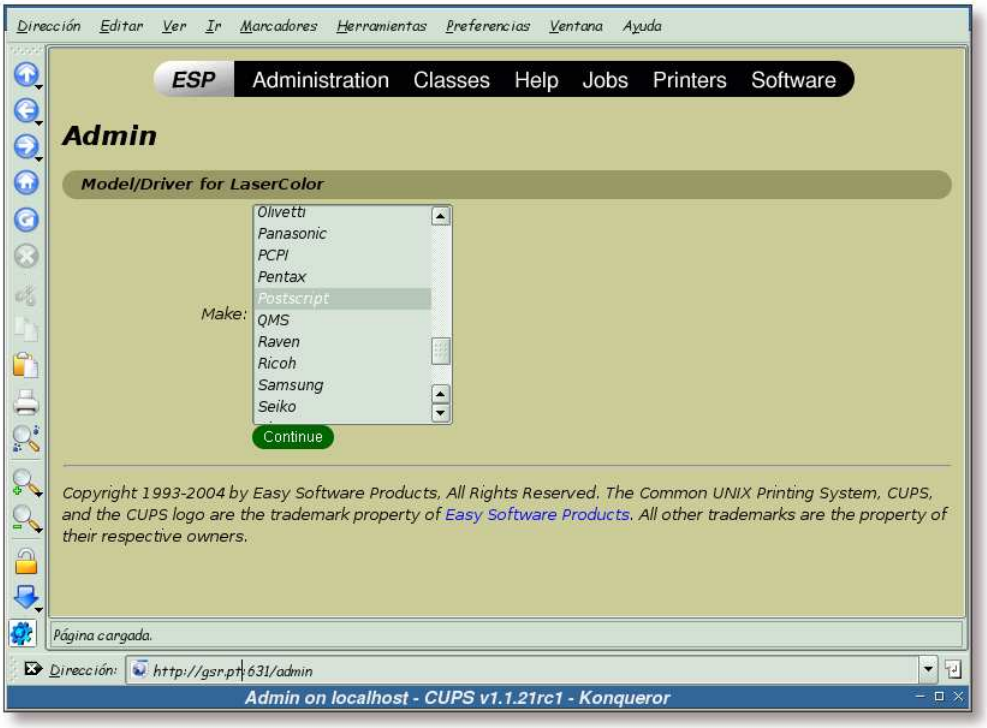
En las pruebas realizadas desde la interfaz web de CUPS por el puerto seguro *6443*, no se ha conseguido que se muestren los dispositivos de impresión disponibles en el sistema. Por este motivo se ha seguido, a partir de este punto, la configuración por el puerto estándar: el 631.

Para conseguir esto, se han de comentar (o cambiar al valor adecuado) las directivas *Encryption* de los directorios `/admin` y `/jobs` del archivo de configuración `/etc/cups/cupsd.conf` (más datos sobre estas directivas en la la sección de nombre *Security Options*).

Figura 15-12. Dispositivo de impresión II

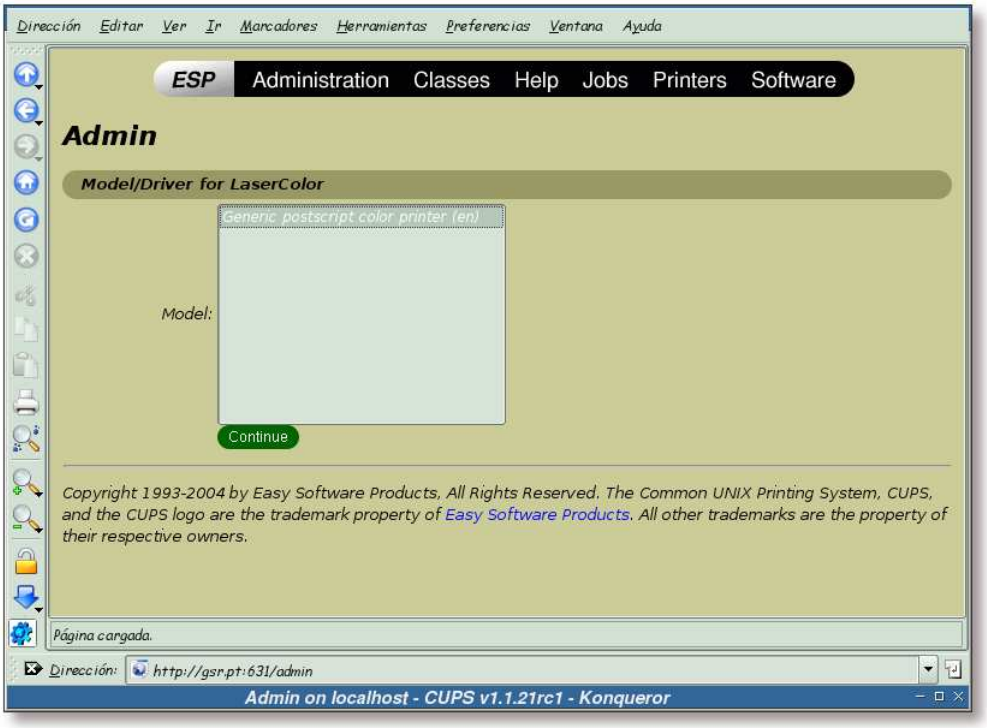
... y pulse sobre el botón “Continue”.

Figura 15-13. Modelo



Seleccione el modelo “Postsript” y pulse sobre el botón “Continue”.

Figura 15-14. Controlador

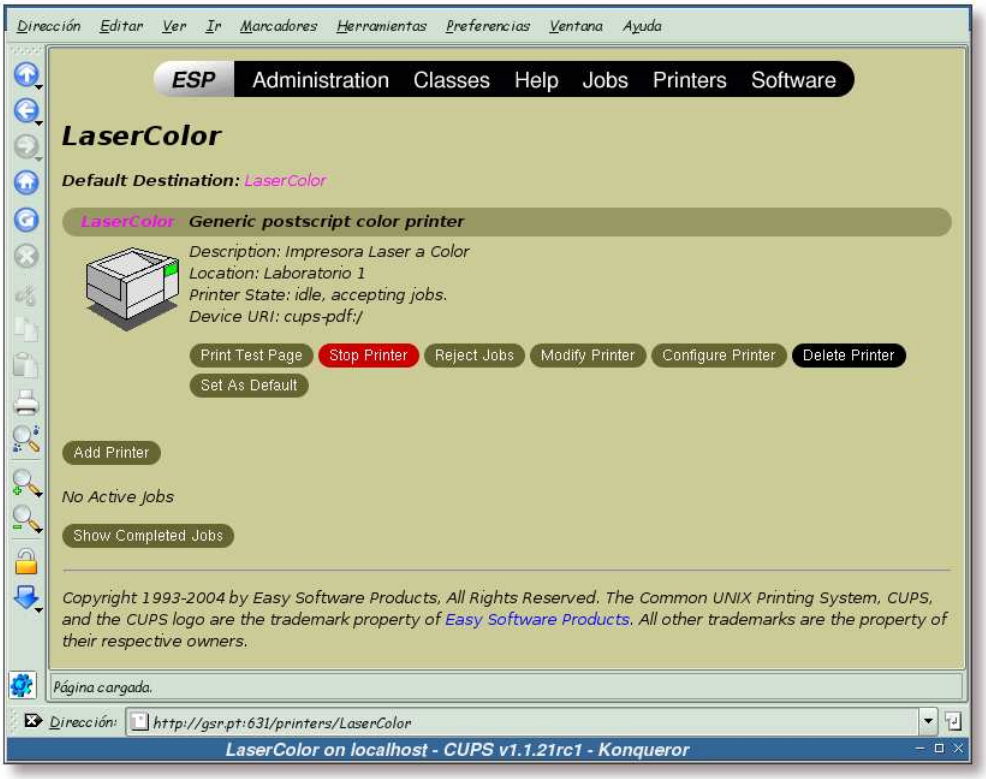


Seleccione el controlador “Generic postscript color printer (en)” como controlador para la nueva impresora.

Figura 15-15. Nueva impresora lista

Esta pantalla informa que se acaba de crear satisfactoriamente la nueva impresora. Para ver los detalles de la misma, pulse sobre el enlace “LaserColor”.

Figura 15-16. Información sobre la impresora LaserColor

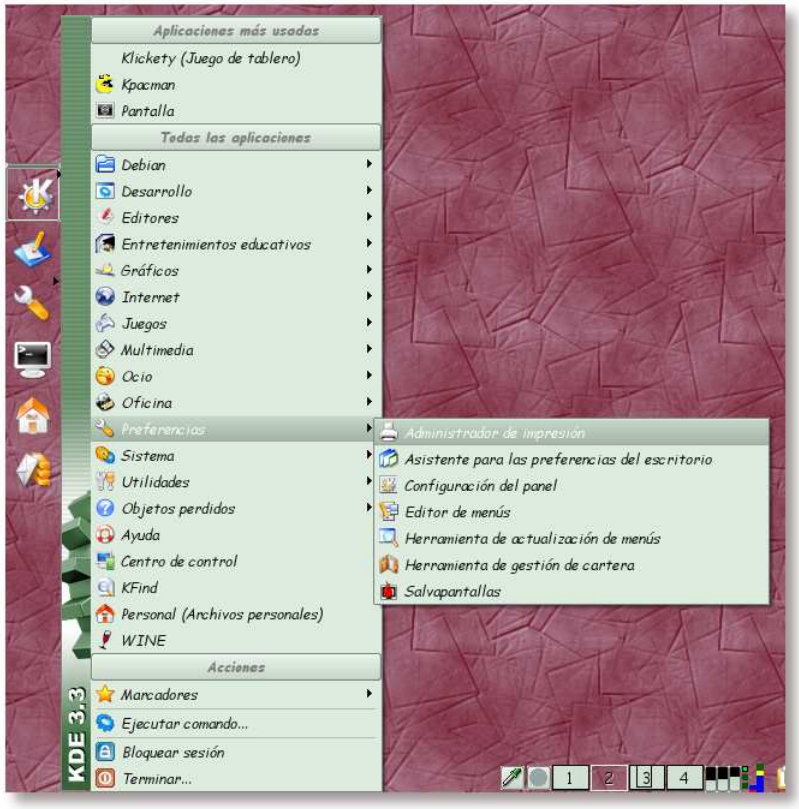


Desde esta ventana se puede realizar la administración de la impresora *LaserColor*, así como observar el estado de la misma en un momento determinado.

Añadiendo una impresora desde KDE

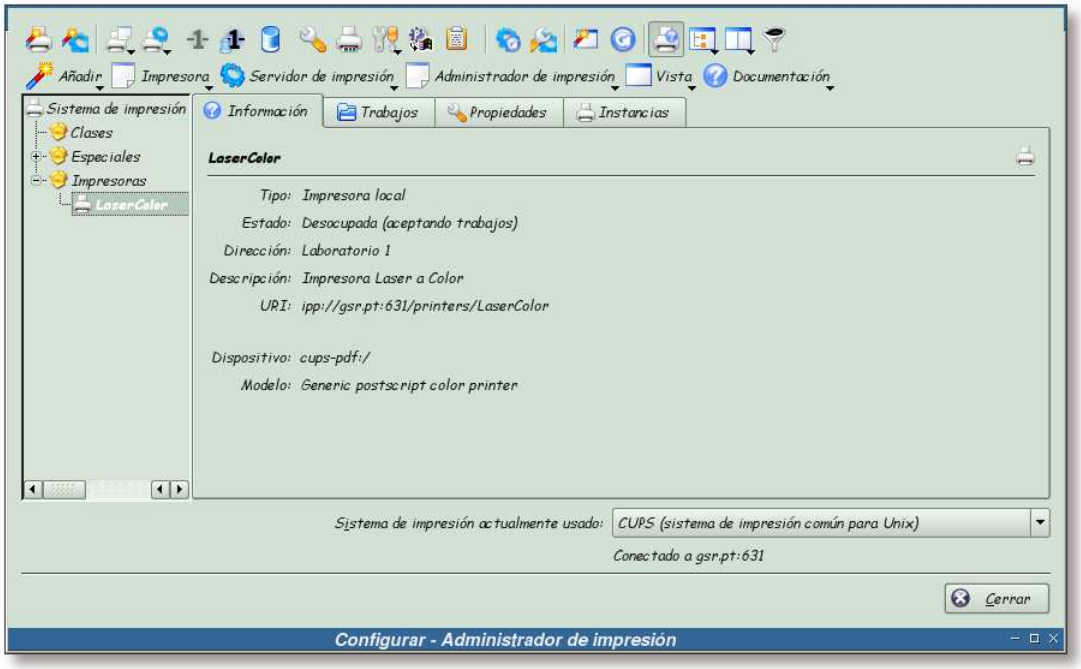
En esta sección se mostrará el proceso seguido para añadir una impresora desde el administrador de impresión de KDE.

Figura 15-17. Arrancando el administrador de impresión



Acceda al menú de KDE, y seleccione la herramienta *Administrador de impresión* desde el mismo; o bien teclee la orden **/usr/bin/kcmshell printers**.

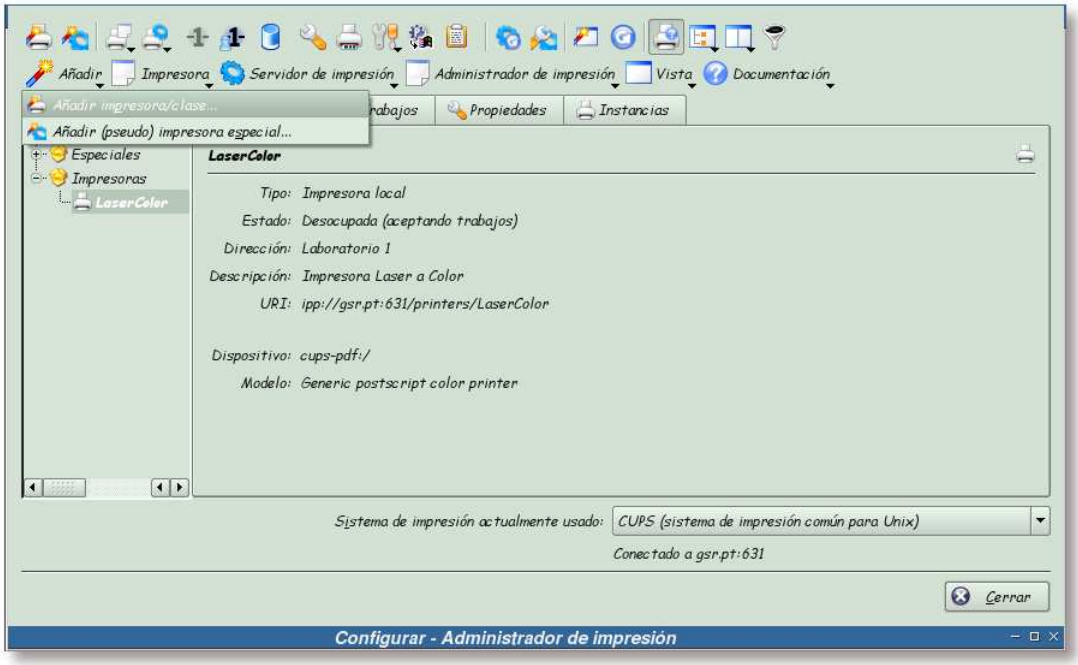
Figura 15-18. Administrador de impresión



Una vez arrancado el administrador de impresión de KDE, ha de asegurarse que la opción del campo: *Sistema de impresión actualmente usado* es el sistema de impresión CUPS.

Si se fija en la imagen, bajo el directorio `impresoras` aparece la impresora *LaserColor*, que se añadió en la sección anterior
(la sección de nombre *Añadiendo una impresora desde la interfaz de administración web de CUPS*).

Figura 15-19. Nueva impresora



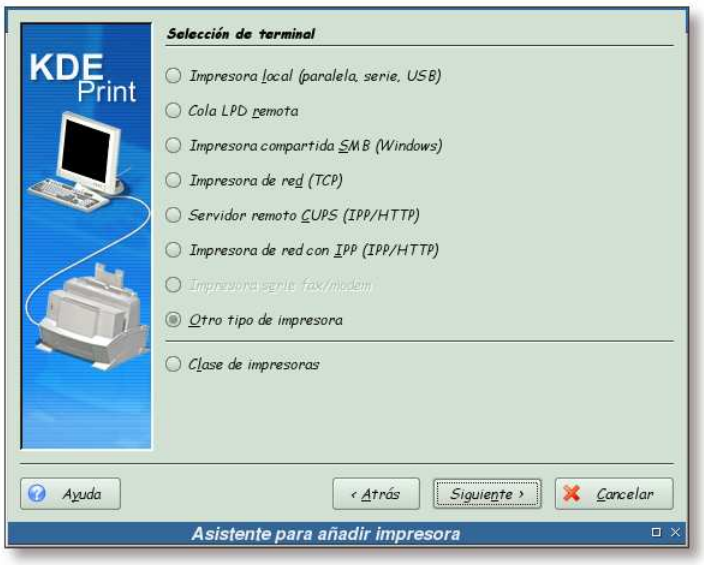
Para añadir una nueva impresora, pulse sobre el botón “Añadir” y seguidamente sobre la opción *Añadir impresora/clase...*

Figura 15-20. Bienvenida al asistente de impresión de KDE

Esta pantalla nos da la bienvenida al asistente que guiará el proceso de adición de una nueva impresora al

sistema. Pulse sobre el botón “Siguiente” para continuar.

Figura 15-21. Selección del tipo de impresora



En esta pantalla se selecciona el tipo de impresora que se va a añadir al sistema. En este caso, se va a añadir una impresora virtual, por lo que se selecciona la opción *Otro tipo de impresora* y se pulsa sobre el botón “Siguiente”.

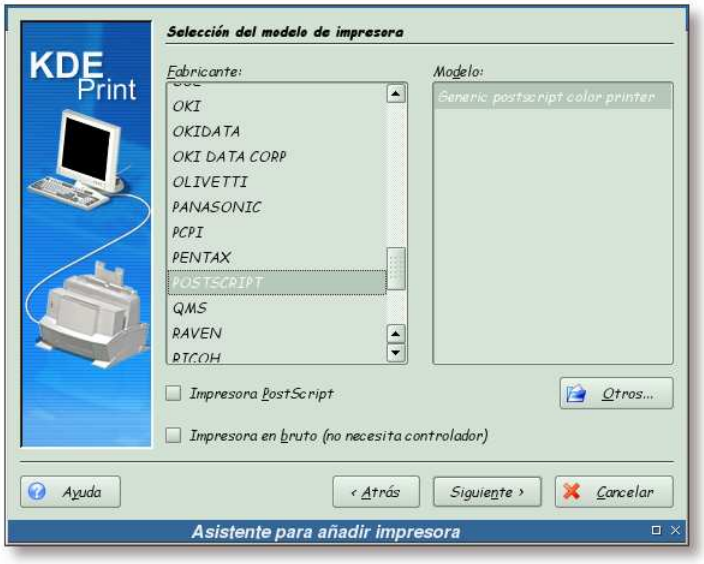
Figura 15-22. URI de la impresora

Seleccione el tipo *Virtual Printer (PDF Printer)* y pulse sobre el botón “Siguiente”.

Figura 15-23. Reconstruyendo la base de datos de controladores

Espere a que se finalice la reconstrucción de la base de datos de controladores de impresión.

Figura 15-24. Modelo de la impresora



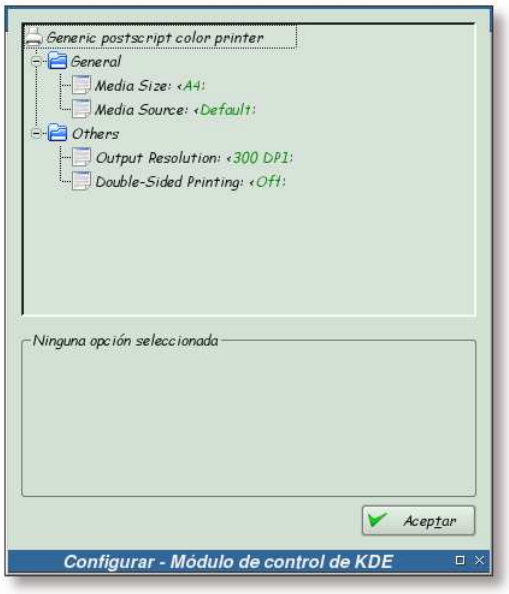
Seleccione el fabricante “POSTSCRIPT” y el modelo “Generic postscript color printer” y pulse sobre el botón “Siguiente” para continuar.

Figura 15-25. Probando la impresora I

Desde esta pantalla se permite realizar pruebas con la configuración de la impresora que se está añadiendo, antes de añadirla definitivamente al sistema.

Pulse sobre el botón “Preferencias...”

Figura 15-26. Opciones de configuración del controlador de impresión



Dependiendo del controlador de impresión elegido, en esta pantalla aparecerán unas opciones u otras. En el caso de la impresora virtual, esta pantalla muestra las opciones que soporta el controlador, pudiendo variar dichas opciones para adaptarlas a las necesidades del sistema.

Una vez cambiadas las opciones, pulse sobre el botón “Aceptar” para continuar.

Figura 15-27. Probando la impresora II

Pulse ahora sobre el botón “Probar”

Figura 15-28. Usuario con privilegios de administración de impresión

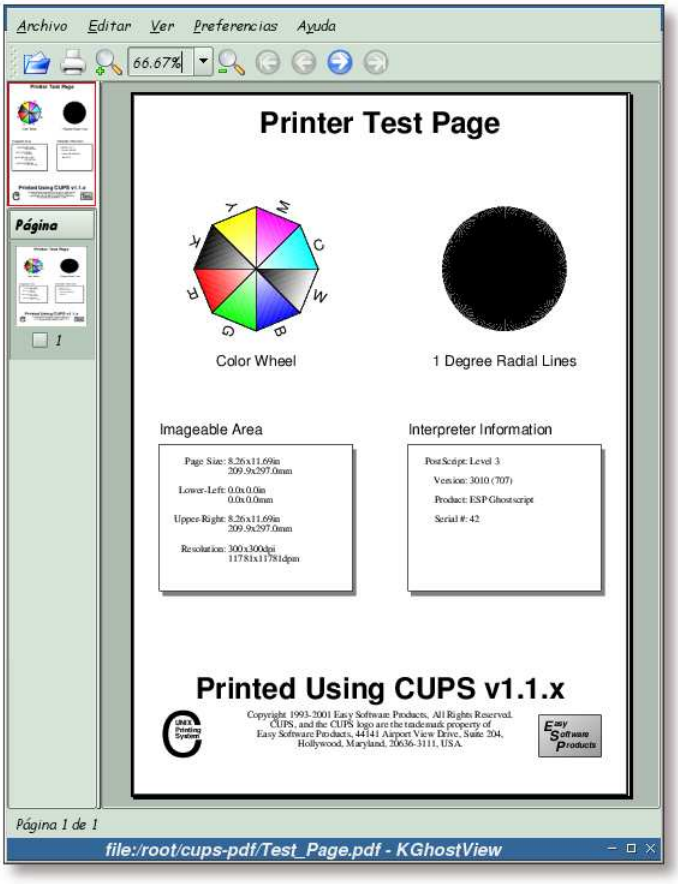
Teclee los datos de un usuario con privilegios de administración de impresión y pulse sobe el botón “Aceptar”.

Figura 15-29. Prueba enviada a la impresora

Esta pantalla nos informa de que se ha enviado la prueba de impresión a la impresora. Pulse sobre el botón “Aceptar” para continuar.

Si todo ha ido bien, en el home del usuario que se ha tecleado, aparecerá un nuevo directorio, `$HOME/cups-pdf` y dentro de este un archivo similar a `Test_Page.pdf`. Si se abre este archivo con un visualizador de archivos PDF, se podrá comprobar que es una prueba de impresión de CUPS.

Figura 15-30. Prueba de impresión



En esta pantalla se puede observar la prueba de impresión que se ha realizado en la imagen anterior.

Figura 15-31. Selección de rótulos

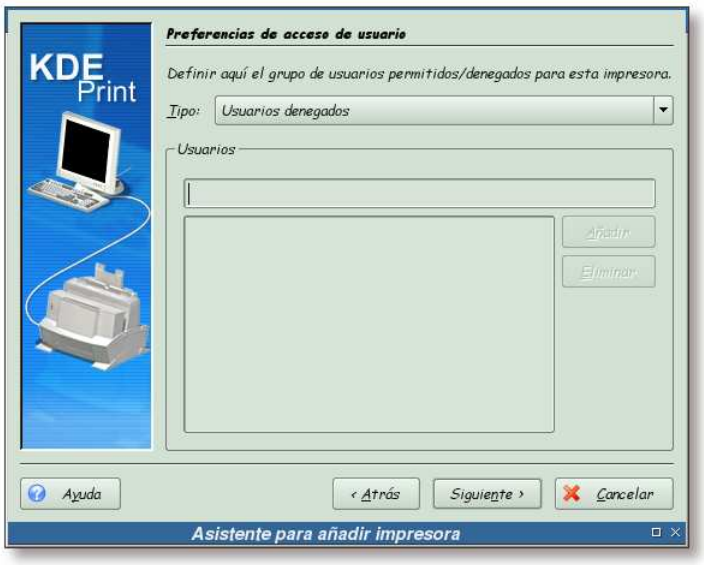
CUPS permite imprimir páginas separadoras para los trabajos de impresión. Si desea hacer uso de esta característica, seleccione los rótulos que desee en esta pantalla, en caso contrario, pulse directamente sobre el botón “Siguiente”.

Figura 15-32. Cuotas de impresión

CUPS implemente un *rudimentario* sistema de cuotas de impresión. Como se va a hacer uso de PyKota

para la administración de cuotas, esta opción no se utilizará. Pulse el botón “Siguiente” para continuar.

Figura 15-33. Permisos de acceso a la impresora

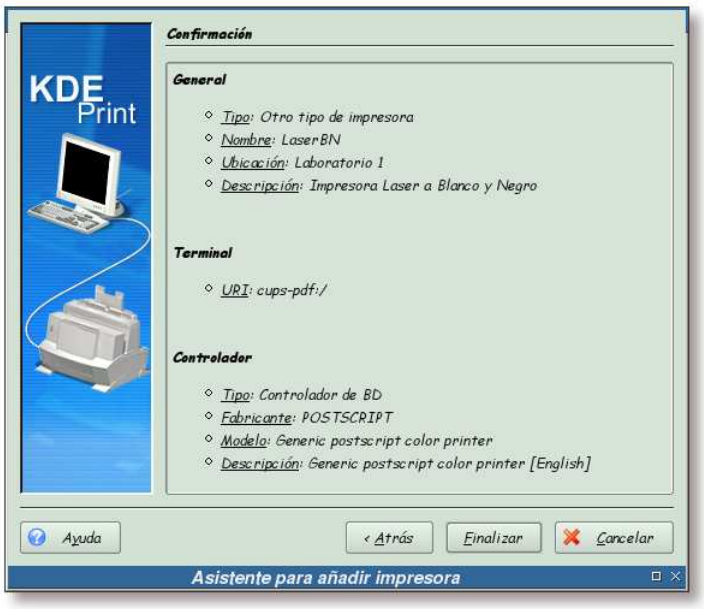


En esta pantalla se seleccionan los usuarios a los que se les permite, o no, imprimir. Como este control se realizará con la herramienta PyKota, pulse sobre el botón “Siguiente” directamente.

Figura 15-34. Información sobre la impresora

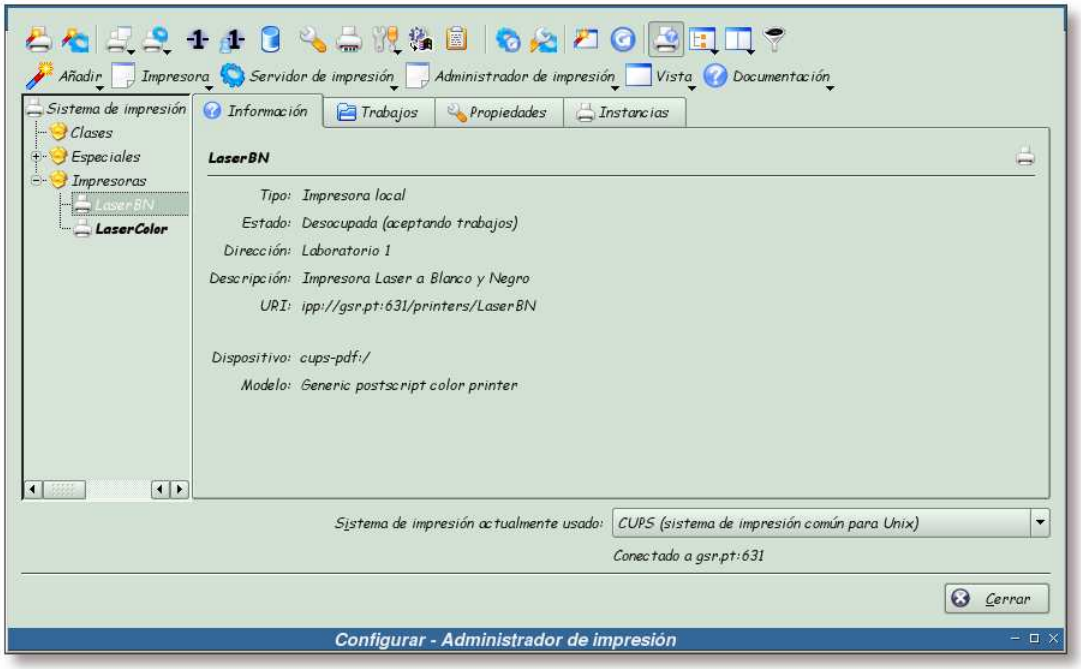
Complete los campos con el nombre, ubicación y descripción para la impresora que se está añadiendo. Pulse sobre el botón “Siguiente” para continuar.

Figura 15-35. Confirmación



Esta es la última pantalla antes de crear la nueva impresora. Revise la información sobre la misma, y si todo está correcto, pulse sobre el botón “Finalizar” para crear la impresora.

Figura 15-36. Nueva impresora *LaserBN*

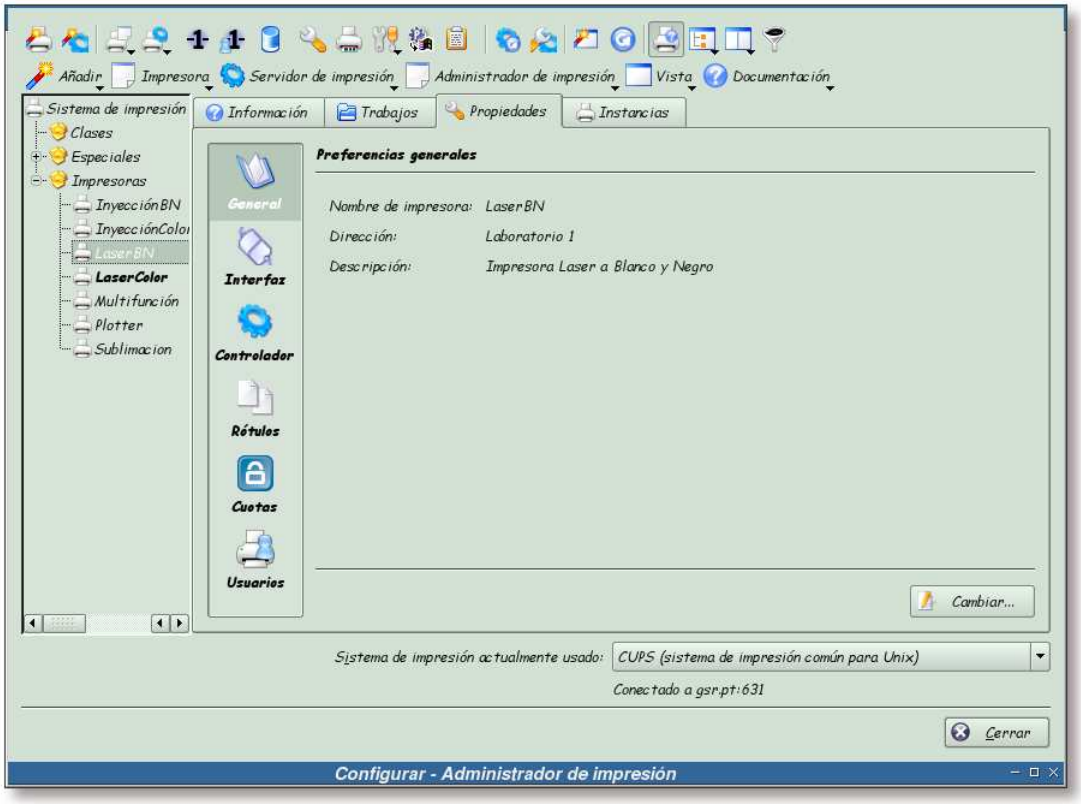


Se puede apreciar en el directorio de impresoras la aparición de una nueva entrada, en este caso la impresora *LaserBN*.

Añadiendo el resto de impresoras

El proceso de creación de nuevas impresoras se ha realizado para cada una de las impresoras que se muestran en el esquema de la la sección de nombre *Introducción,* obteniendo finalmente:

Figura 15-37. Listado de impresoras



Impresoras que conforman la red organizacional del esquema mostrado en la la sección de nombre *Introducción.*

Creación de las clases

Al igual que ya se hizo en la la sección de nombre *Creación de las impresoras* con las impresoras, en esta sección se añadirán las clases.

Los nombres y el contenido de las clases será:

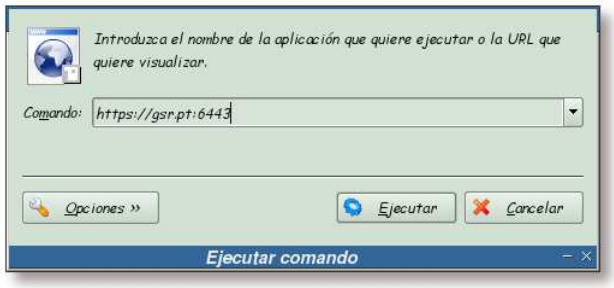
- *Profesional:* Plotter, Sublimacion, LaserColor
- *Color:* LaserColor, InyeccionColor
- *BlancoNegro:* LaserBN, InyeccionBN
- *Barato:* Multifuncion, InyeccionBN
- *Laser:* LaserColor, LaserBN

Las dos siguientes secciones mostrarán como añadir una clase desde la interfaz de administración web de CUPS y desde el frontend que provee el escritorio KDE para la administración de impresoras.

Añadiendo una clase desde la interfaz de administración web de CUPS

En esta sección se mostrará el proceso seguido para añadir una clase desde la interfaz de administración web de CUPS.

Figura 15-38. Accediendo a la interfaz de administración web de CUPS



Si se encuentra en un entorno de escritorio KDE, teclee **Alt**+**F2** e introduzca la dirección donde se encuentre instalado CUPS seguido del puerto donde está escuchando. En este caso: *https://gsr.pt:6443*.

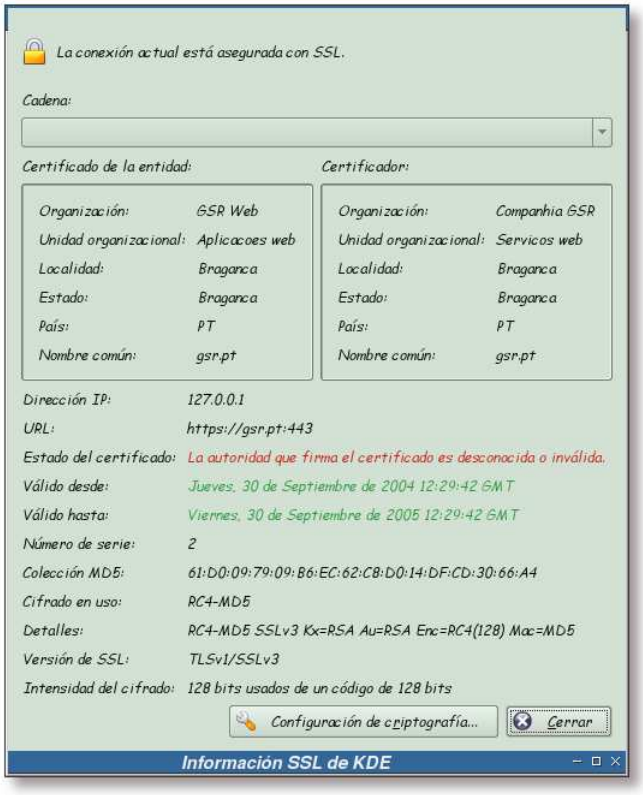
Nota: Si se fija en la URL que se ha tecleado, se ha especificado el protocolo *https* y el puerto de conexión segura de CUPS. Esto es necesario si se quiere hacer uso de cifrado en las comunicaciones con CUPS.

Si no accede de esta forma a la interfaz web de CUPS, no podrá realizar labores de administración, ya que se ha obligado en los archivos de configuración de CUPS, al uso de cifrado en las secciones de administración.

Figura 15-39. Aviso acerca del certificado del servidor web I

Como se ha accedido a la interfaz web de CUPS vía el puerto seguro y debido a que la entidad certificadora que se ha creado para las conexiones SSL/TLS es desconocida, sale este aviso. Pulse sobre el botón *Detalles* para obtener más información.

Figura 15-40. Información SSL



En esta pantalla se muestra la información del certificado y la entidad certificadora que ha creado dicho certificado. Pulse sobre el botón *Cerrar* para continuar.

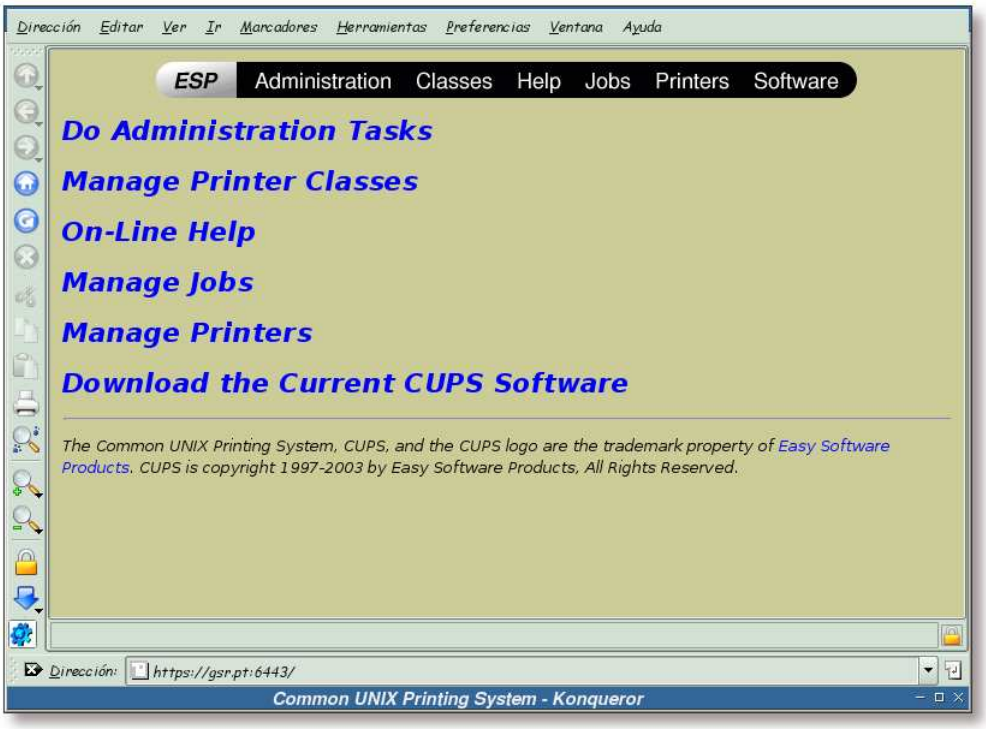
Figura 15-41. Aviso acerca del certificado del servidor web II

Pulse ahora sobre el botón *Continuar* para seguir con la carga de la página.

Figura 15-42. Período de aceptación del certificado

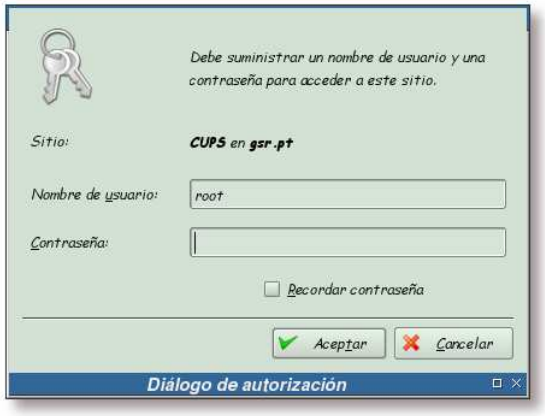
Seleccione la opción deseada y pulse sobre ella.

Figura 15-43. Administrando clases



Una vez se tenga acceso al interfaz de administración web de CUPS, pulse sobre el enlace “Do Administration Tasks”.

Figura 15-44. Clave del administrador

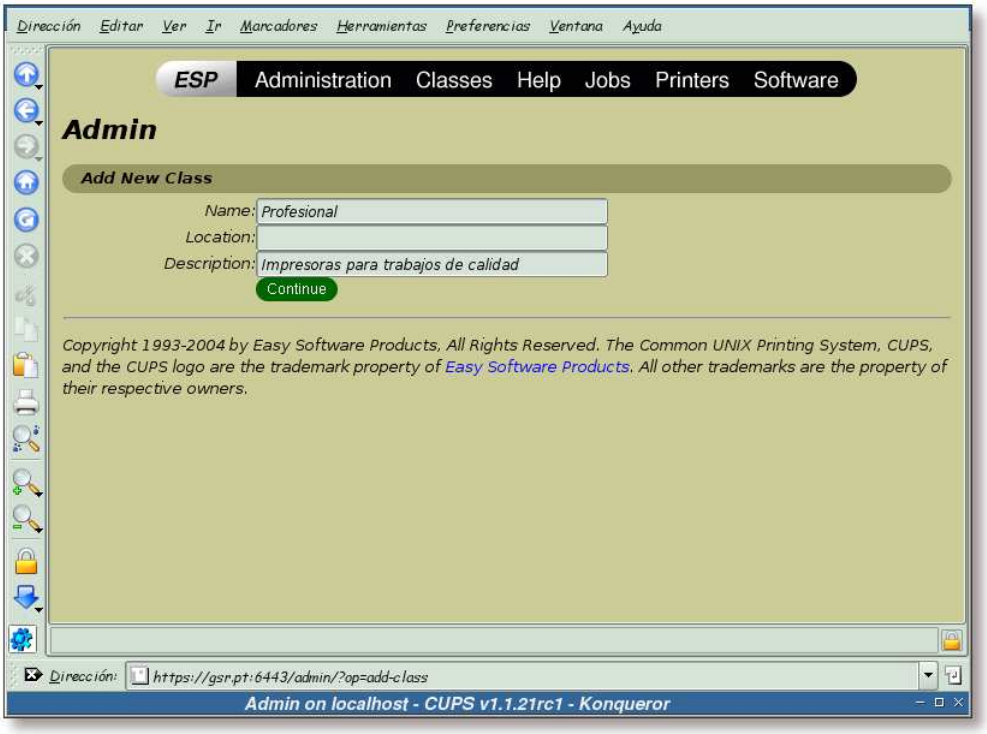


Introduzca un usuario con permisos de administración para el sistema de impresión, así como su clave.

Figura 15-45. Añadiendo una clase

Para comenzar el proceso de adición de una clase, pulse sobre el botón “Add Class”.

Figura 15-46. Información sobre la clase



Teclee la información relativa a la clase y pulse sobre el botón “Continue”.

Figura 15-47. Miembros de la clase

Seleccione las impresoras que van a pertenecer a la clase y pulse sobre el botón “Continue”.

Aviso

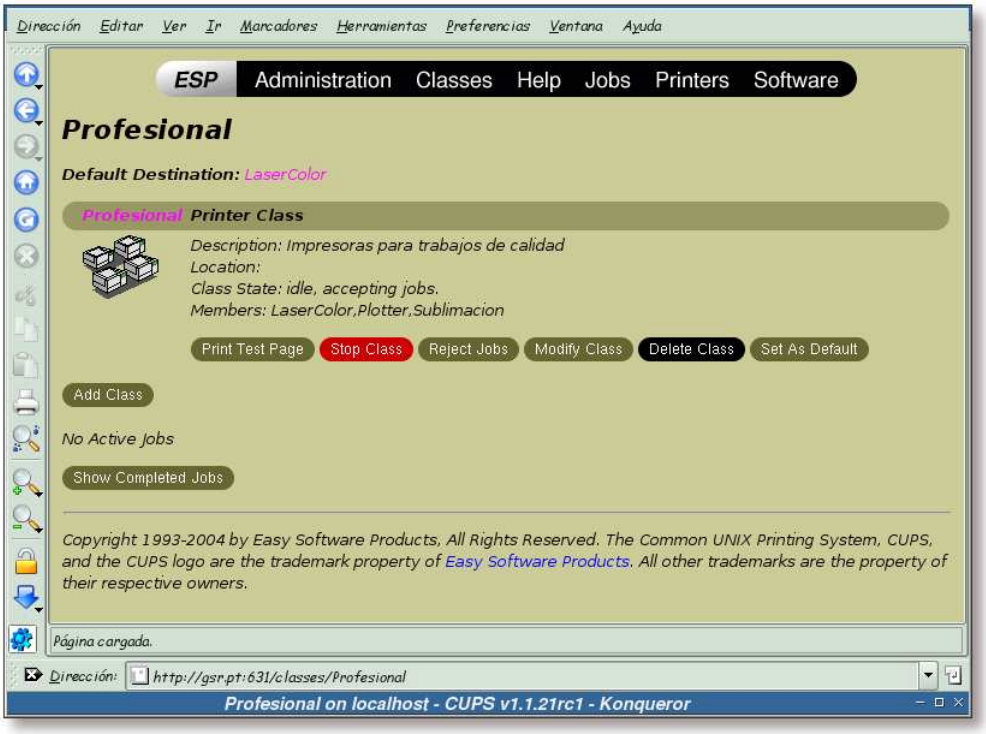
En las pruebas realizadas desde la interfaz web de CUPS por el puerto seguro *6443*, no se ha conseguido que se muestren las impresoras existentes. Por este motivo se ha seguido, a partir de este punto, la configuración por el puerto estandar: el 631.

Para conseguir esto, se han de comentar (o cambiar al valor adecuado) las directivas *Encryption* de los directorios `/admin` y `/jobs` del archivo de configuración `/etc/cups/cupsd.conf` (más datos sobre estas directivas en la la sección de nombre *Security Options*).

Figura 15-48. Nueva clase lista

Esta pantalla informa que se acaba de crear satisfactoriamente la nueva clase. Para ver los detalles de la misma, pulse sobre el enlace “Profesional”.

Figura 15-49. Información sobre la clase *Profesional*

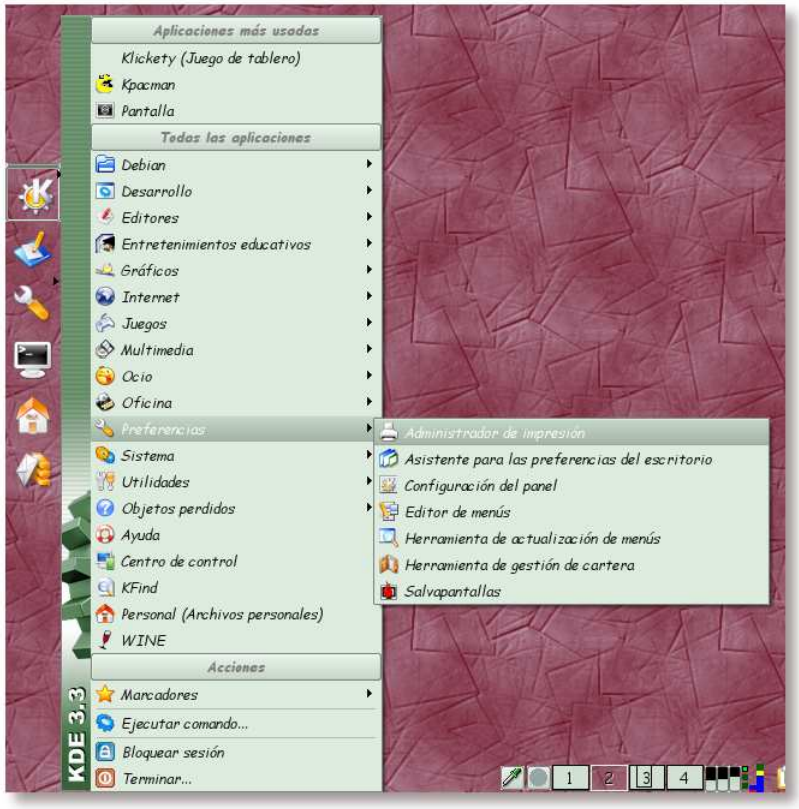


Desde esta ventana se puede realizar la administración de la clase *Profesional*.

Añadiendo una clase desde KDE

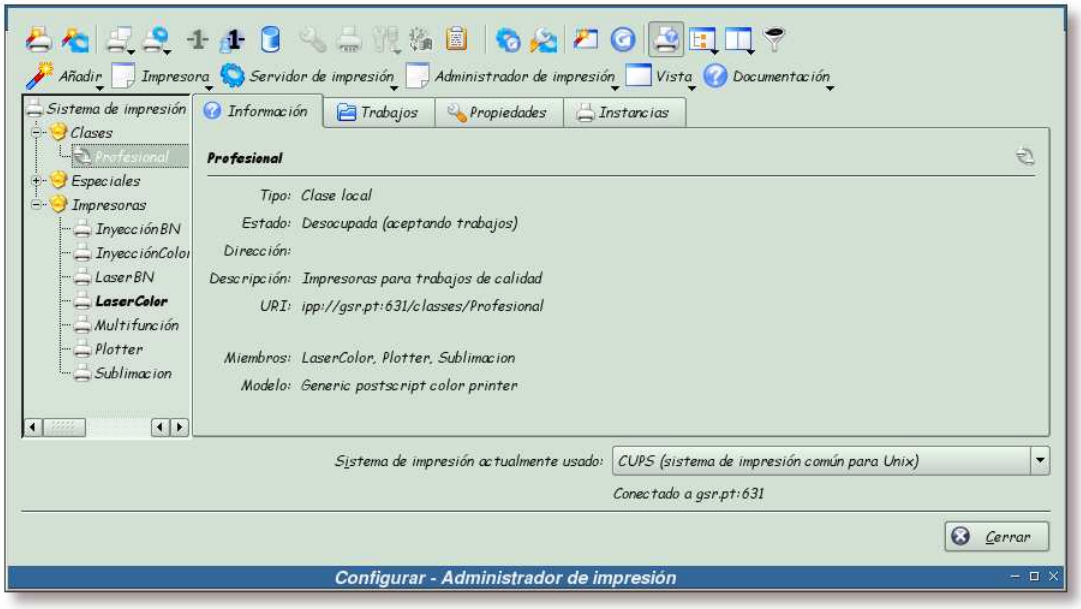
En esta sección se mostrará el proceso seguido para añadir una clase desde la el administrador de impresión de KDE.

Figura 15-50. Arrancando el administrador de impresión



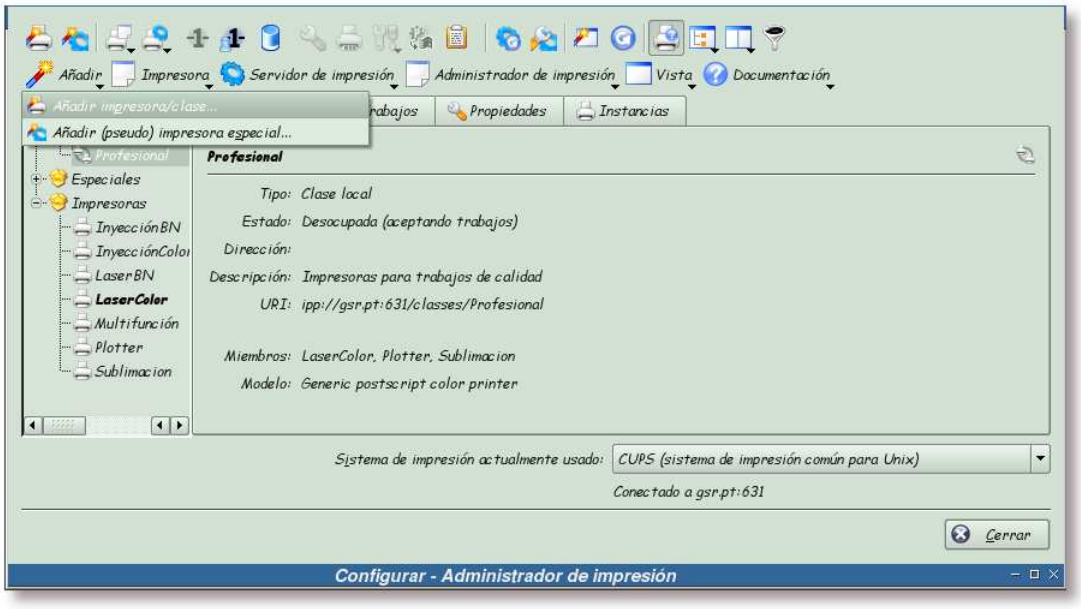
Acceda al menú de KDE, y seleccione la herramienta *Administrador de impresión* desde el mismo; o bien teclee la orden **/usr/bin/kcmshell printers**.

Figura 15-51. Administrador de impresión



En esta pantalla se puede observar el estado actual del sistema de impresión. A parte de las impresoras que se han añadido anteriormente aparece también la nueva clase que se acaba de añadir.

Figura 15-52. Nueva clase



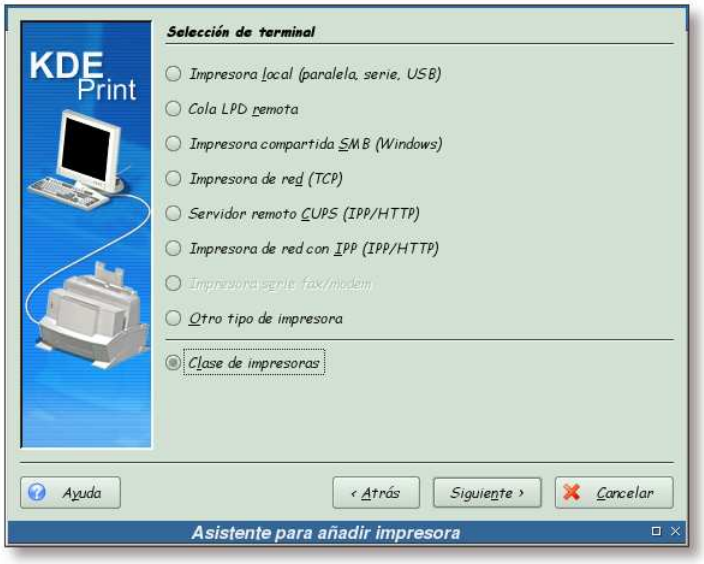
Para añadir una nueva clase, pulse sobre el botón “Añadir” y seguidamente sobre la opción *Añadir*

impresora/clase...

Figura 15-53. Bienvenida al asistente de impresión de KDE

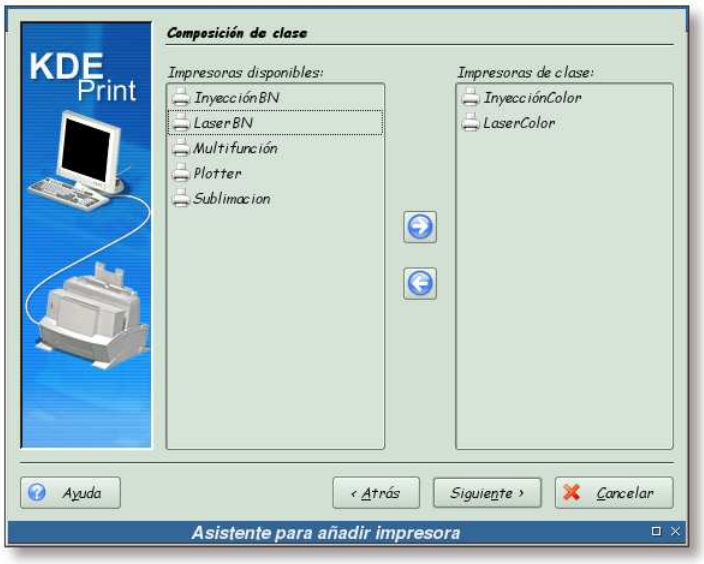
Esta pantalla nos da la bienvenida al asistente que guiará el proceso de adición de una nueva clase al sistema. Pulse sobre el botón “Siguiente” para continuar.

Figura 15-54. Selección de la clase impresora



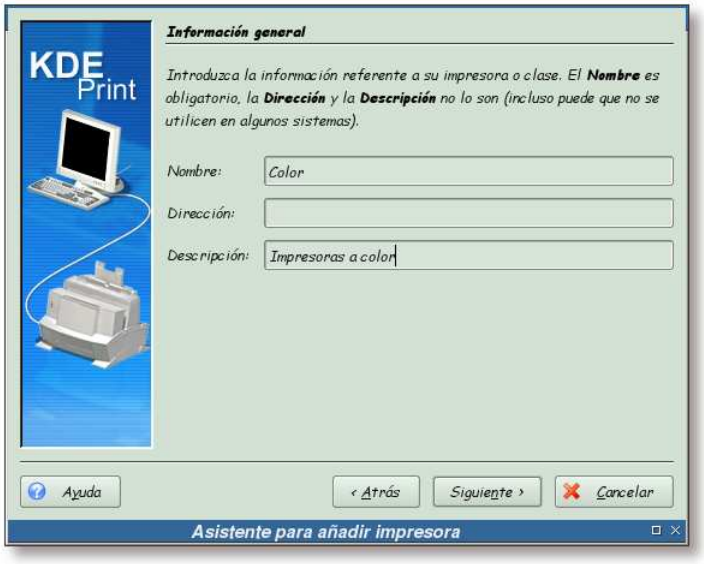
En esta pantalla se selecciona el tipo de impresora que se va a añadir al sistema. En este caso, se va a añadir una clase de impresora, por lo que se selecciona la opción *Clase de impresora* y se pulsa sobre el botón “Siguiente”.

Figura 15-55. Composición de la clase



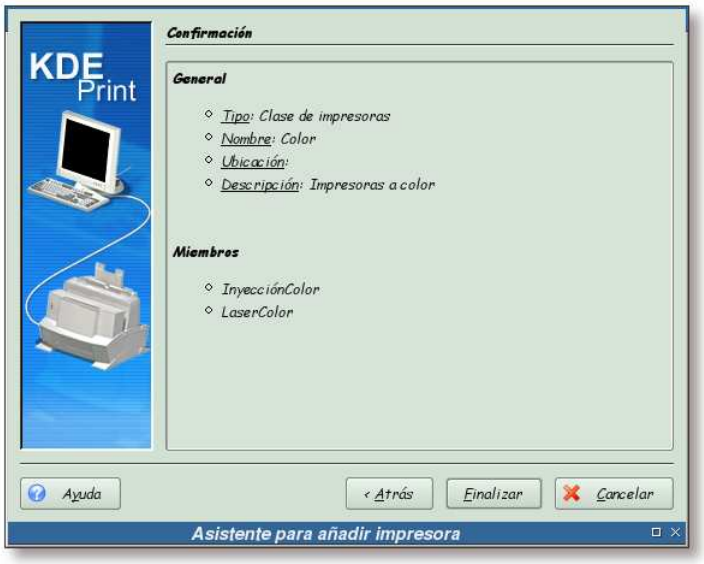
Seleccione las impresoras que formarán parte de la clase que se está creando. Una vez seleccionadas, pulse sobre el botón “Siguiente” para continuar.

Figura 15-56. Información sobre la clase



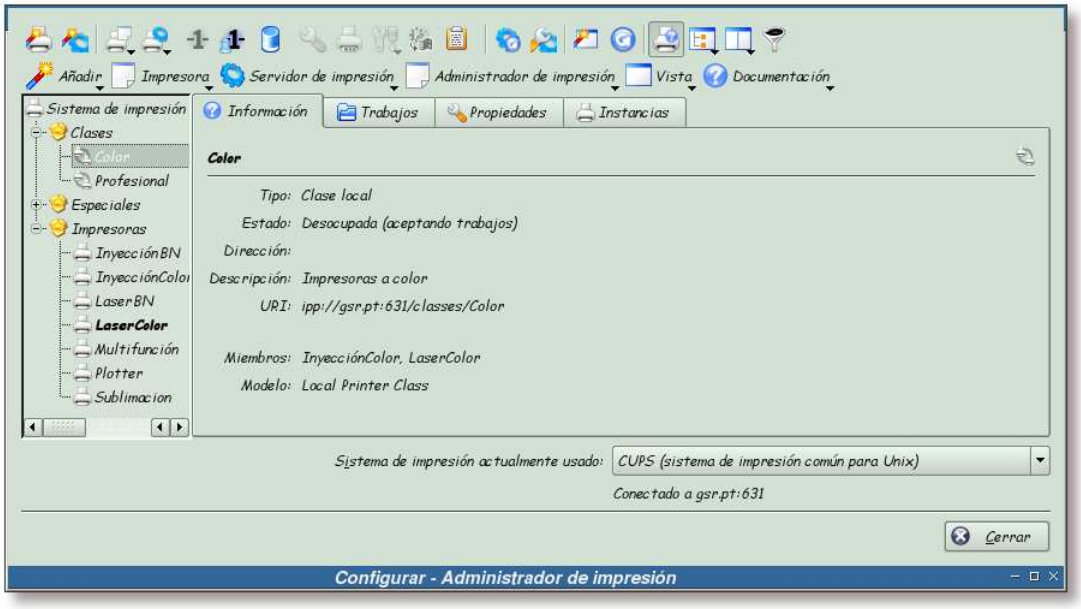
Complete la información relativa a la nueva clase, y pulse sobre el botón “Siguiente” para continuar.

Figura 15-57. Confirmación de la creación de la nueva clase



Antes de añadir la nueva clase al sistema, revise los datos de la misma, y una vez esté seguro de que todo está correcto, pulse sobre el botón “Finalizar”, lo que creará la nueva clase en el sistema.

Figura 15-58. Nueva clase *Color*

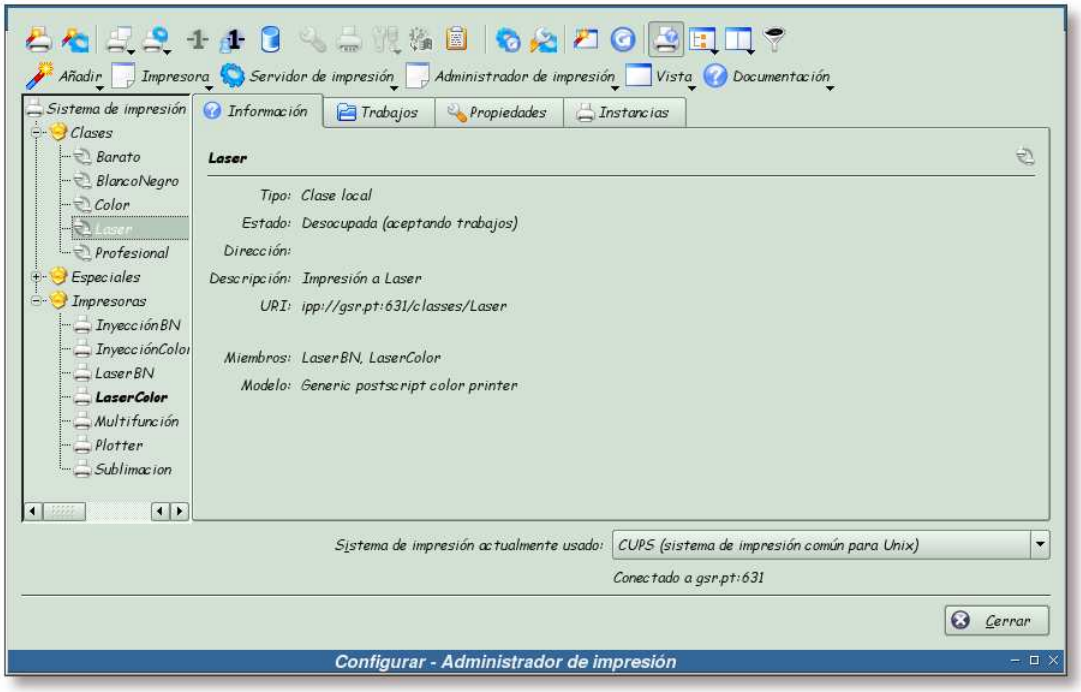


Se puede apreciar en el directorio de clases la aparición de una nueva entrada, en este caso la clase *Color*.

Añadiendo el resto de clases

El proceso de creación de nuevas clases se ha realizado para cada una de las clases que se muestran en el esquema de la la sección de nombre *Introducción*, obteniéndose finalmente:

Figura 15-59. Listado de clases

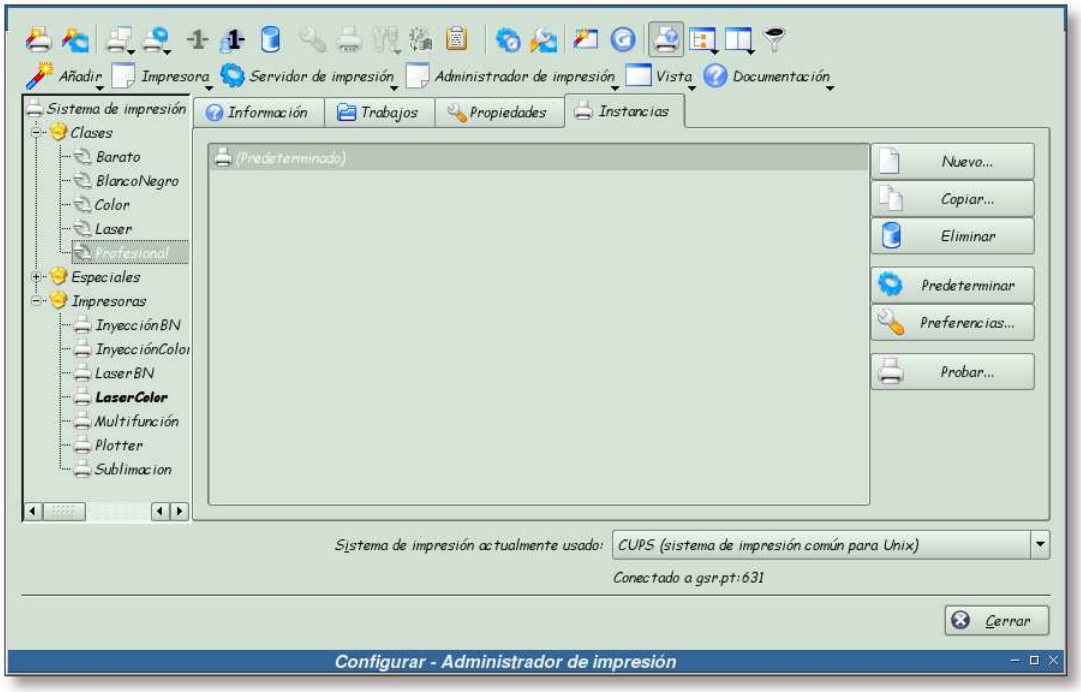


Clases que conforman la red organizacional del esquema mostrado en la la sección de nombre *Introducción.*

Probando la impresión en las clases

A continuación se realizará una prueba de impresión sobre una clase de impresoras, para comprobar que funciona. Para ello, ejecute el administrador de impresión de KDE y seleccione la clase sobre la cual quiera hacer la prueba.

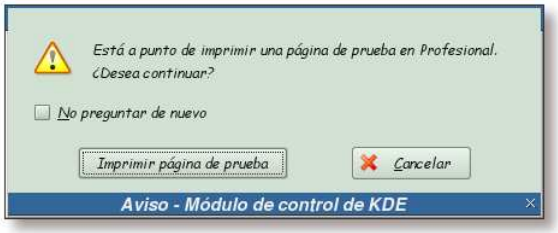
Figura 15-60. Realizando una prueba de impresión sobre una clase



Seleccione una clase sobre la cual realizar la prueba de impresión, y luego acceda a la pestaña *Instancias* y pulse sobre el botón “Probar...”

Esta acción enviará una prueba de impresión a la clase que haya seleccionado.

Figura 15-61. Confirmación del envío de la prueba de impresión



El sistema pide confirmación para realizar la prueba de impresión, pulse sobre “Imprimir página de prueba” para continuar.

Figura 15-62. Información de envío

El sistema informa de que la página de prueba ha sido enviada a la clase seleccionada.

Si ahora echa un vistazo a los logs de CUPS, más concretamente al archivo de log `/var/log/cups/page_log`, ha de ver una entrada similar a:

```
Sublimacion sergio 2 [10/Oct/2004:19:52:05 +0200] 1 1 - localhost
```

Finalmente, si mira en el directorio `cups-pdf` localizado en el HOME del usuario que ha realizado la prueba de impresión, tendrá que ver un archivo PDF denominado `Test_Page.pdf`, cuyo contenido será similar al mostrado en la imagen Prueba de impresión.

Instalación de los controladores de impresión para los equipos MS Windows

CUPS no da soporte, directamente, a los clientes MS Windows; para ello se ha de hacer uso de Samba. La forma de hacerlo, es compartiendo las impresoras gestionadas por CUPS en Samba, como ya se ha visto en los capítulos dedicados a Samba
(Parte II en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*).

En esta sección se verá la forma de exportar los controladores de impresión para los equipos MS Windows. Los controladores se almacenan en la instalación de CUPS, y se comparten, vía Samba, con los clientes MS Windows. Para realizar esta labor, se puede hacer uso de la herramienta **cupsaddsmb**.

cupsaddsmb transfiere los controladores de impresión al recurso Samba *[print$]*. Recuerde que los clientes esperan tener los controladores almacenados en este recurso, al que accederán en el momento de la instalación para bajarse los controladores de impresión.

cupsaddsmb facilita la compartición de cualquier (o todas) impresora CUPS instalada en el sistema. También puede utilizar los controladores PostScript de Adobe así como los controladores PostScript de CUPS para Windows NT/2000/XP.

Los controladores de impresión de CUPS se pueden obtener desde la sección *download* de la página de CUPS. El paquete de controladores se denomina *cups-samba-[version].tar.gz*.

Actualmente, CUPS provee controladores para los clientes Windows NT, 2000 y XP, pero no para los clientes Windows 95, 98 y ME. Estos últimos han de utilizar los drivers que provee Adobe.

Antes de poder exportar los controladores de impresión, estos se han de ubicar en el directorio `/usr/share/cups/drivers/`. Las siguientes secciones mostrarán como “instalar” los controladores PostScript de CUPS y Adobe en este directorio.

Instalación de los controladores PostScript de CUPS para Windows NT/2000/XP

Antes de proceder con la instalación, ha de bajarse los controladores de la página de CUPS[2].

Se supone que el paquete con los controladores se encuentra en el directorio `/tmp`, por lo que se procederá, en primer lugar, a su desempaquetado:

Ejemplo 15-5. Desempaquetado de los controladores PostScript de CUPS

```
$ /bin/tar xzvf /tmp/cups-samba-5.0rc3.tar.gz -C /tmp
cups-samba.install
cups-samba.license
cups-samba.readme
cups-samba.remove
cups-samba.ss
```

Como el proceso de instalación de los controladores PostScript de CUPS es muy sencillo, no se va a utilizar el script de instalación, `cups-samba.install`, que adjuntan.

El archivo `cups-samba.ss` no es más que un archivo *tar*[3], cuyo contenido son los controladores en cuestión. Por este motivo se desempaquetará en el directorio `/usr/share/cups/drivers/`, como se muestra en el siguiente ejemplo:

Ejemplo 15-6. Desempaquetado de los controladores PostScript de CUPS en el directorio `/usr/share/cups/drivers/`

```
# /bin/mkdir -v -m 755 /usr/share/cups/drivers/
/bin/mkdir: se ha creado el directorio ‘/usr/share/cups/drivers/’
# /bin/tar xvf /tmp/cups-samba.ss -C /
/usr/share/cups/drivers/cups5.hlp
/bin/tar: Removing leading ‘/’ from member names
/usr/share/cups/drivers/cupsdrv5.dll
/usr/share/cups/drivers/cupsui5.dll
```

A partir de este momento ya se encuentran disponibles los controladores PostScript de CUPS para Windows NT/2000/XP disponibles. Ahora sólo queda exportarlos en Samba, operación que se verá más adelante (la sección de nombre *Exportando los controladores con **cupsaddsmb***).

Instalación de los controladores PostScript de Adobe

Adobe proporciona controladores PostScript para los sistemas MS Windows 95/98/ME así como para MS Windows NT/2000/XP. Estos se pueden obtener de su página web, http://www.adobe.com/.

Los controladores PostScript de Adobe, actualmente, vienen en un archivo autoinstalable para los sistemas MS Windows, por lo que se tendrá que hacer uso de Wine para obtenerlos.

En primer lugar se ha de bajar el archivo que los contiene, que en este caso se denomina `winstspa.exe` (se corresponde con la versión española de estos controladores).

Ahora se ha de ejecutar el instalador, para ello se hace uso de wine, como se muestra en el siguiente ejemplo:

> **Nota:** Se supone que wine ya se encuentra instalado y correctamente configurado.

Ejemplo 15-7. Ejecución del instalador de controladores PostScript de Adobe con Wine (primera parte)

```
$ /usr/bin/wine winstspa.exe
```

Tras la ejecución de la orden del ejemplo anterior, comenzará el proceso de instalación de los controladores PostScript de Adobe en el sistema. Vea las siguientes capturas para más detalles:

Figura 15-63. Proceso de descompresión de los controladores y archivos de instalación

Justo después de ejecutar el instalador, se procede a la descompresión de los controladores PostScript y de los archivos necesarios para la instalación en los sistemas MS Windows.

Estos archivos son copiados al directorio `C:\Windows\Temp\`, que en el caso del sistema donde se ha ejecutado Wine, se encuentra bajo el directorio `$HOME/.wine/fake_windows/Windows/Temp`.

El proceso de instalación creará un directorio temporal, cuyo nombre será similar a `pft3405~tmp`. Este directorio se creará bajo el directorio `$HOME/.wine/fake_windows/Windows/Temp`, y es ahí de donde se obtendrán los controladores PostScript de Adobe.

Figura 15-64. Comienza el proceso de instalación

Tras descomprimir los archivos necesarios para la instalación, se ejecutará el instalador de los controladores PostScript de Adobe.

Figura 15-65. Pantalla de bienvenida del instalador

Una vez se ha llegado a la pantalla de bienvenida del instalador de los controladores PostScript de Adobe, se puede terminar la ejecución del programa.

> **Importante:** No cancele la instalación desde el programa de instalación de los controladores (ya que esto haría que se borrasen del sistema), simplemente finalice la ejecución de Wine, bien sea matando el proceso o pulsando la combinación de teclas **Ctrl**+**c**, siempre y cuando esté ejecutando Wine desde un terminal, por ejemplo.

Ejemplo 15-8. Ejecución del instalador de controladores PostScript de Adobe con Wine (segunda parte)

```
$ /usr/bin/wine winstspa.exe [Ctrl+c]
$ cd ~/.wine/fake_windows/Windows/Temp
$ /usr/bin/tree
.
|-- pftc3c~tmp
|   |-- DATA.TAG
|   |-- Leame.wri
|   |-- SETUP.INI
|   |-- Setup.exe
|   |-- Win2000 ❶
|   |   |-- DEFPRTR2.PPD
|   |   |-- PS5UI.DLL
|   |   |-- PSCRIPT.HLP
|   |   |-- PSCRIPT.NTF
```

```
|   |   |-- PSCRIPT5.DLL
|   |   `-- PSCRPTFE.NTF
|   |-- WinNT ❷
|   |   |-- ADOBEPSU.HLP
|   |   |-- AdobeJpn.ntf
|   |   |-- AdobeKor.ntf
|   |   |-- AdobePS5.dll
|   |   |-- AdobePS5.ntf
|   |   |-- AdobeZhS.ntf
|   |   |-- AdobeZhT.ntf
|   |   |-- DEFPRTR2.PPD
|   |   `-- adobepsu.dll
|   |-- WinXP ❸
|   |   |-- DEFPRTR2.PPD
|   |   |-- PS5UI.DLL
|   |   |-- PSCRIPT.HLP
|   |   |-- PSCRIPT.NTF
|   |   |-- PSCRIPT5.DLL
|   |   `-- PSCRPTFE.NTF
|   |-- Windows ❹
|   |   |-- ADOBEPS4.DRV
|   |   |-- ADOBEPS4.HLP
|   |   |-- DEFPRTR2.PPD
|   |   |-- ICONLIB.DLL
|   |   |-- PSMON.DLL
|   |   `-- adfonts.mfm
|   |-- _INST32I.EX_
|   |-- _ISDel.exe
|   |-- _Setup.dll
|   |-- _sys1.cab
|   |-- _sys1.hdr
|   |-- _user1.cab
|   |-- _user1.hdr
|   |-- data1.cab
|   |-- data1.hdr
|   |-- lang.dat
|   |-- layout.bin
|   |-- os.dat
|   |-- pftw1.pkg
|   |-- setup.bmp
|   |-- setup.ins
|   `-- setup.lid
`-- plfa2b.tmp

5 directories, 48 files
```

❶ Controladores PostScript de Adobe para MS Windows 2000.

❷ Controladores PostScript de Adobe para MS Windows NT.

❸ Controladores PostScript de Adobe para MS Windows XP.

❹ Controladores PostScript de Adobe para MS Windows 9x.

En el Ejemplo 15-8 se ha mostrado el listado de controladores PostScript que provee Adobe. Antes de copiarlos al directorio `/usr/share/cups/drivers` se van a renombrar, de forma que queden todos los archivos en mayúsculas. El proceso se muestra a continuación:

Ejemplo 15-9. Convirtiendo a mayúsculas los controladores PostScript de Adobe

En este ejemplo se hace uso del script presente en el Apéndice L. Se supone que el script está almacenado en el directorio `/usr/local/bin`.

```
$ cd ~/.wine/fake_windows/Windows/Temp/pftc3c~tmp
$ for x in "Win2000/* Windows/* WinNT/* WinXP/*";
> do
>    /bin/bash /usr/local/bin/uppercase $x;
> done
/usr/local/bin/uppercase: Win2000/DEFPRTR2.PPD not changed.
/usr/local/bin/uppercase: Win2000/PS5UI.DLL not changed.
/usr/local/bin/uppercase: Win2000/PSCRIPT5.DLL not changed.
/usr/local/bin/uppercase: Win2000/PSCRIPT.HLP not changed.
/usr/local/bin/uppercase: Win2000/PSCRIPT.NTF not changed.
/usr/local/bin/uppercase: Win2000/PSCRPTFE.NTF not changed.
/usr/local/bin/uppercase: Windows/adfonts.mfm -> Windows/ADFONTS.MFM
/usr/local/bin/uppercase: Windows/ADOBEPS4.DRV not changed.
/usr/local/bin/uppercase: Windows/ADOBEPS4.HLP not changed.
/usr/local/bin/uppercase: Windows/DEFPRTR2.PPD not changed.
/usr/local/bin/uppercase: Windows/ICONLIB.DLL not changed.
/usr/local/bin/uppercase: Windows/PSMON.DLL not changed.
/usr/local/bin/uppercase: WinNT/AdobeJpn.ntf -> WinNT/ADOBEJPN.NTF
/usr/local/bin/uppercase: WinNT/AdobeKor.ntf -> WinNT/ADOBEKOR.NTF
/usr/local/bin/uppercase: WinNT/AdobePS5.dll -> WinNT/ADOBEPS5.DLL
/usr/local/bin/uppercase: WinNT/AdobePS5.ntf -> WinNT/ADOBEPS5.NTF
/usr/local/bin/uppercase: WinNT/adobepsu.dll -> WinNT/ADOBEPSU.DLL
/usr/local/bin/uppercase: WinNT/ADOBEPSU.HLP not changed.
/usr/local/bin/uppercase: WinNT/AdobeZhS.ntf -> WinNT/ADOBEZHS.NTF
/usr/local/bin/uppercase: WinNT/AdobeZhT.ntf -> WinNT/ADOBEZHT.NTF
/usr/local/bin/uppercase: WinNT/DEFPRTR2.PPD not changed.
/usr/local/bin/uppercase: WinXP/DEFPRTR2.PPD not changed.
/usr/local/bin/uppercase: WinXP/PS5UI.DLL not changed.
/usr/local/bin/uppercase: WinXP/PSCRIPT5.DLL not changed.
/usr/local/bin/uppercase: WinXP/PSCRIPT.HLP not changed.
/usr/local/bin/uppercase: WinXP/PSCRIPT.NTF not changed.
/usr/local/bin/uppercase: WinXP/PSCRPTFE.NTF not changed.
```

Ahora sólo queda copiar los controladores necesarios al directorio `/usr/share/cups/drivers`. El siguiente ejemplo muestra como hacerlo:

Ejemplo 15-10. Copiando los controladores PostScript de Adobe a `/usr/share/cups/drivers`

Sustituya la variable *$HOME*, por el directorio home del usuario donde se encuentran los controladores PostScript de Adobe.

El contenido del script *mover-controladores* se encuentra en el Apéndice M.

```
# cd $HOME/.wine/fake_windows/Windows/Temp/pftc3c~tmp
```

```
# /bin/bash /usr/local/bin/mover-controladores
‘PATH/Windows/ADFONTS.MFM’ -> ‘/usr/share/cups/drivers/ADFONTS.MFM’
‘PATH/Windows/ADOBEPS4.DRV’ -> ‘/usr/share/cups/drivers/ADOBEPS4.DRV’
‘PATH/Windows/ADOBEPS4.HLP’ -> ‘/usr/share/cups/drivers/ADOBEPS4.HLP’
‘PATH/WinNT/DEFPRTR2.PPD’ -> ‘/usr/share/cups/drivers/DEFPRTR2.PPD’
‘PATH/WinXP/DEFPRTR2.PPD’ -> ‘/usr/share/cups/drivers/DEFPRTR2.PPD’
‘PATH/Win2000/DEFPRTR2.PPD’ -> ‘/usr/share/cups/drivers/DEFPRTR2.PPD’
‘PATH/Windows/DEFPRTR2.PPD’ -> ‘/usr/share/cups/drivers/DEFPRTR2.PPD’
‘PATH/Windows/ICONLIB.DLL’ -> ‘/usr/share/cups/drivers/ICONLIB.DLL’
‘PATH/Windows/PSMON.DLL’ -> ‘/usr/share/cups/drivers/PSMON.DLL’
‘PATH/WinNT/ADOBEPS5.DLL’ -> ‘/usr/share/cups/drivers/ADOBEPS5.DLL’
‘PATH/WinNT/ADOBEPSU.DLL’ -> ‘/usr/share/cups/drivers/ADOBEPSU.DLL’
‘PATH/WinNT/ADOBEPSU.HLP’ -> ‘/usr/share/cups/drivers/ADOBEPSU.HLP’
el modo de ‘/usr/share/cups/drivers/ADFONTS.MFM’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/ADOBEPS4.DRV’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/ADOBEPS4.HLP’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/ADOBEPS5.DLL’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/ADOBEPSU.DLL’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/ADOBEPSU.HLP’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/cups5.hlp’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/cupsdrv5.dll’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/cupsui5.dll’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/DEFPRTR2.PPD’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/ICONLIB.DLL’ cambia a 0644 (rw-r--r--)
el modo de ‘/usr/share/cups/drivers/PSMON.DLL’ cambia a 0644 (rw-r--r--)
```

Exportando los controladores con cupsaddsmb

Una vez copiados los controladores de impresión PostScript, tanto de Adobe como de CUPS al directorio `/usr/share/cups/drivers/`, se han de exportar en Samba; para ello se hará uso de la herramienta **cupsaddsmb**.

A parte de exportar los controladores de Adobe y CUPS, también se exportarán los controladores de las impresoras que se han añadido en la la sección de nombre *Creación de la estructura de impresión*.

> **Nota:** Actualmente en el directorio `/usr/share/cups/drivers/` se encuentran los controladores PostScript, para MS Windows NT/2000/XP, tanto de CUPS como de Adobe. Al exportar dichos controladores con la herramienta **cupsaddsmb**, esta priorizará la instalación de los controladores creados por el proyecto CUPS, sobre los creados por Adobe.
>
> Esto significa que exportará los controladores del proyecto CUPS para los sistemas operativos MS Windows NT/2000/XP, en lugar de los controladores que provee Adobe; y los controladores de Adobe para los sistemas operativos MS Windows 95/98/ME.

El siguiente ejemplo mostrará como realizar esta operación:

Ejemplo 15-11. Exportando los controladores de impresión con cupsaddsmb

La opción *-a* le dice a la orden **cupsaddsmb** que añada todas las impresoras presentes en el sistema.

```
$ /usr/bin/tree /var/lib/samba/printers

/var/lib/samba/printers
|-- W32X86
‘-- WIN40

2 directories, 0 files
$ /usr/sbin/cupsaddsmb -U root -a
Password for root required to access localhost via SAMBA: [Clave]
$ /usr/bin/tree /var/lib/samba/printers
/var/lib/samba/printers
|-- W32X86 ❶
|   ‘-- 2
|       |-- InyeccionBN.ppd
|       |-- InyeccionColor.ppd
|       |-- LaserBN.ppd
|       |-- LaserColor.ppd
|       |-- Multifuncion.ppd
|       |-- Plotter.ppd
|       |-- Sublimacion.ppd
|       |-- cups5.hlp
|       |-- cupsdrv5.dll
|       ‘-- cupsui5.dll
‘-- WIN40 ❷
    ‘-- 0
        |-- ADFONTS.MFM
        |-- ADOBEPS4.DRV
        |-- ADOBEPS4.HLP
        |-- DEFPRTR2.PPD
        |-- ICONLIB.DLL
        |-- InyeccionBN.PPD
        |-- InyeccionColor.PPD
        |-- LaserBN.PPD
        |-- LaserColor.PPD
        |-- Multifuncion.PPD
        |-- PSMON.DLL
        |-- Plotter.PPD
        ‘-- Sublimacion.PPD

4 directories, 23 files
```

❶ Controladores de impresión para MS Windows NT/2000/XP exportados mediante samba, gracias al recurso [print$]

❷ Controladores de impresión para MS Windows 95/98/ME exportados mediante samba, gracias al recurso [print$]

> **Nota:** En el Apéndice N se muestra la ejecución de la orden **cupsaddsmb** con la opción *-v* (modo *verbose*).

Una vez finalizada la exportación de los controladores de impresión, ya se tendría el sistema preparado para que los clientes MS Windows hagan uso de las impresoras administradas por CUPS.

Impresión desde Samba

> **Nota:** Como para la realización de esta documentación no se ha tenido acceso a un sistema MS Windows, no se ha podido comprobar el funcionamiento de la impresión desde dicho sistema operativo.

En esta sección se va a comprobar que las impresoras están realmente presentes en samba, para ello se va a añadir una impresora, compartida por Samba, al sistema. Pero antes de realizar esta operación, se verán los recursos compartidos por Samba, tras la incorporación de CUPS al sistema:

Ejemplo 15-12. Recursos compartidos por Samba, tras la instalación de CUPS

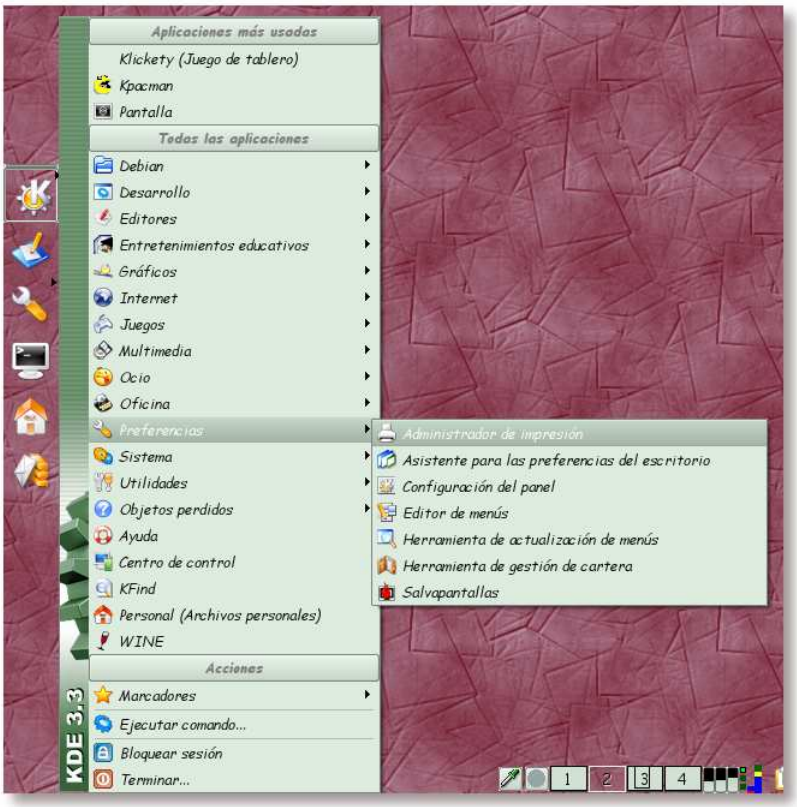
```
$ /usr/bin/smbclient -L TODOSCSI -U gsruser
Password: [Clave]
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk      Network Logon Service
        print$          Disk      Printer Drivers
        tmp             Disk      Temporal
        cdrom           Disk      Samba server's CD-ROM
        IPC$            IPC       IPC Service (SAMBA-LDAP PDC server)
        ADMIN$          IPC       IPC Service (SAMBA-LDAP PDC server)
        InyeccionBN     Printer   Impresora de inyeccion de tinta a Blanco y Negro
        LaserBN         Printer   Impresora Laser a Blanco y Negro
        LaserColor      Printer   Impresora Laser a Color
        Multifuncion    Printer   Impresora multifuncion
        Plotter         Printer   Plotter de impresion
        Barato          Printer   Impresoras para imprimir a bajo coste
        Sublimacion     Printer   Impresora de sublimacion
        BlancoNegro     Printer   Impresion a Blanco y Negro
        Color           Printer   Impresoras a color
        Laser           Printer   Impresion a Laser
        Profesional     Printer   Impresoras para trabajos de calidad
        gsruser         Disk      Home Directories
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]

        Server               Comment
        ---------            -------
```

```
TODOSCSI             SAMBA-LDAP PDC server

Workgroup            Master
---------            -------
GSRDOMAIN            TODOSCSI
```

Se puede comprobar en el ejemplo anterior, que ya se encuentran disponibles varias impresoras en Samba. A continuación se añadirá una impresora, compartida por Samba, al sistema. Para ello se hará uso del administrador de impresión de KDE.

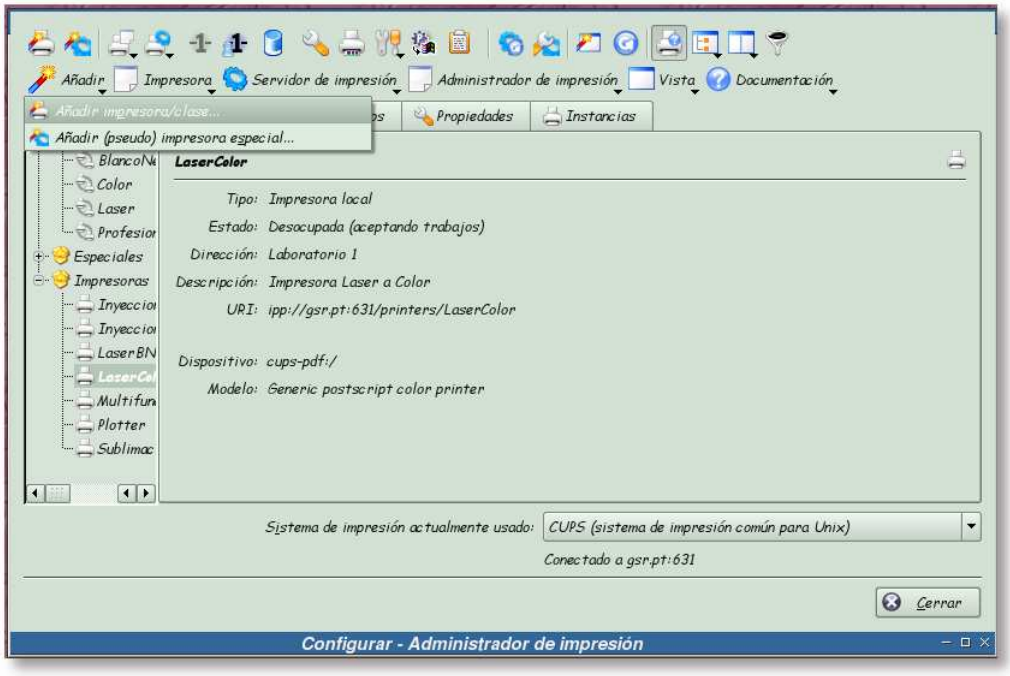
> **Nota:** Esta operación no tiene mucho sentido en un sistema GNU/Linux, pero sirva este ejemplo como muestra de las posibilidades que brinda el sistema.

Figura 15-66. Arrancando el administrador de impresión



Acceda al menú de KDE, y seleccione la herramienta *Administrador de impresión* desde el mismo; o bien teclee la orden **/usr/bin/kcmshell printers**.

Figura 15-67. Nueva impresora



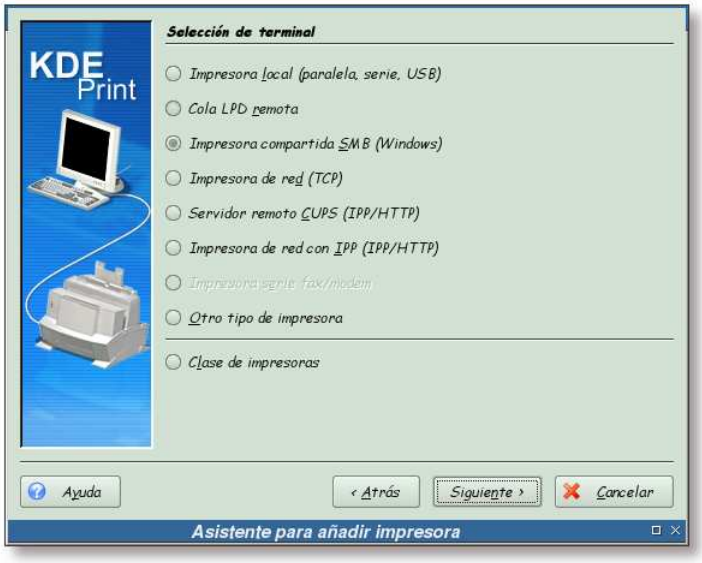
Para añadir una nueva impresora, pulse sobre el botón “Añadir” y seguidamente sobre la opción *Añadir impresora/clase...*

Figura 15-68. Bienvenida al asistente de impresión de KDE

Esta pantalla nos da la bienvenida al asistente que guiará el proceso de adición de una nueva impresora al

sistema. Pulse sobre el botón “Siguiente” para continuar.

Figura 15-69. Selección del tipo de impresora



En esta pantalla se selecciona el tipo de impresora que se va a añadir al sistema. En este caso, se va a añadir una impresora compartida por Samba, por lo que se selecciona la opción *Impresora compartida SMB (Windows)* y se pulsa sobre el botón “Siguiente”.

Figura 15-70. Usuario de acceso a la red Samba

Pulse sobre la opción “Cuenta de normal” y luego teclee un usuario y clave válidos para acceder al sistema Samba. Tenga en cuenta que este usuario ha de tener permisos de impresión (vea el Ejemplo 15-2 para más detalles).

Figura 15-71. Monitorizar la red

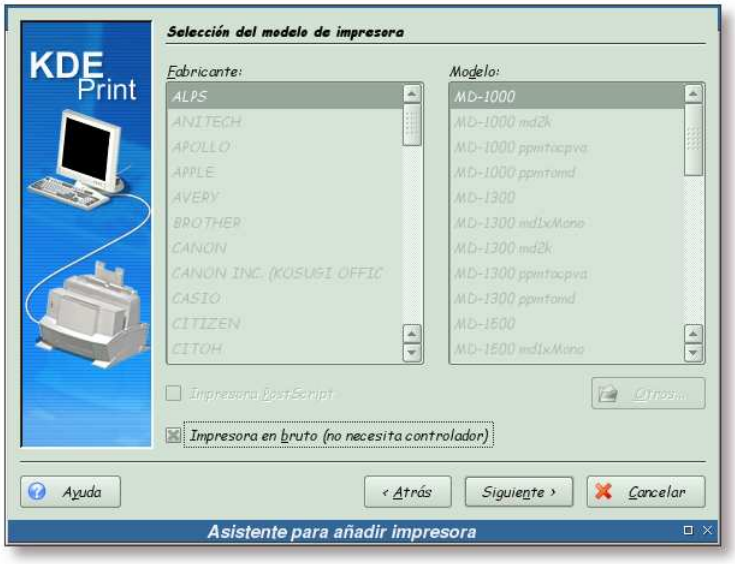
Pulse sobre el botón “Monitorizar”, para realizar una búsqueda de servidores Samba disponibles en la red.

Figura 15-72. Selección de la impresora

Una vez encontrado el servidor Samba, seleccione la impresora que quiera utilizar y pulse sobre el botón “Siguiente”.

Nota: Fíjese que en este caso se va a hacer uso de una clase de impresora.

Figura 15-73. Modelo de la impresora

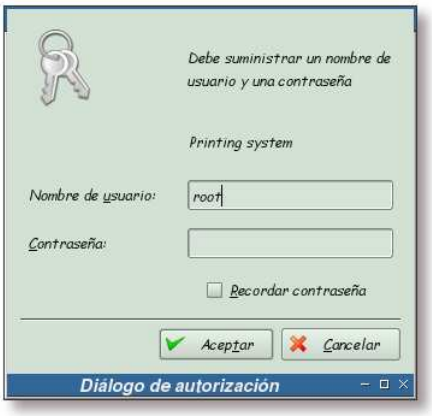


Para esta impresora no es necesario seleccionar un controlador, ya que es CUPS quien se encarga de procesar el trabajo, no Samba. Por este motivo, seleccione la opción “Impresora en bruto (no necesita controlador)” y pulse sobre el botón “Siguiente”.

Figura 15-74. Probando la impresora

Pulse sobre el botón “Probar” para enviar una prueba de impresión a la impresora que se está a punto de añadir.

Figura 15-75. Usuario con privilegios de administración de impresión



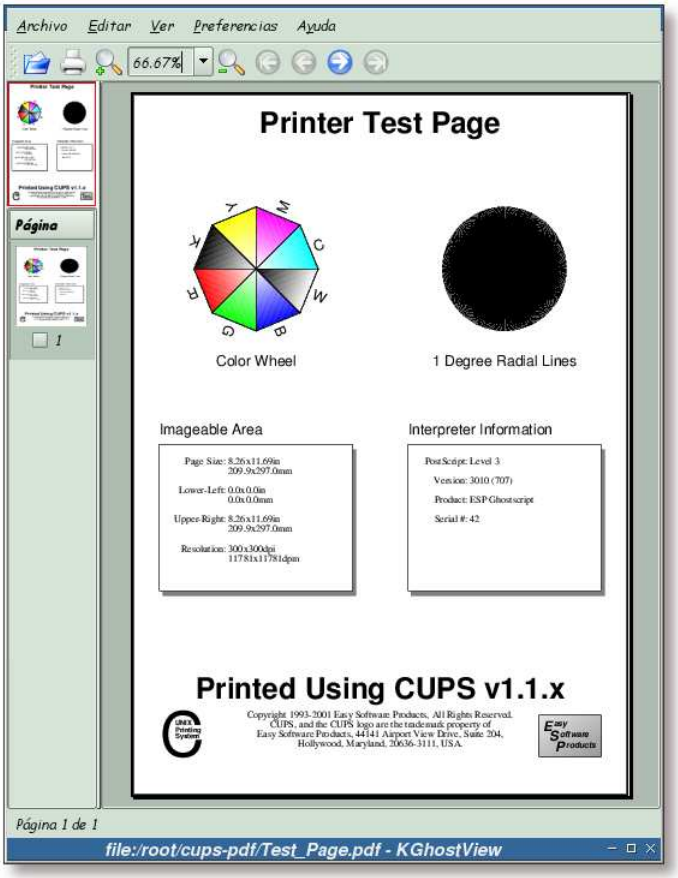
Teclee los datos de un usuario con privilegios de administración de impresión y pulse sobe el botón “Aceptar”.

Figura 15-76. Prueba enviada a la impresora

Esta pantalla nos informa de que se ha enviado la prueba de impresión a la impresora. Pulse sobre el botón “Aceptar” para continuar.

Si todo ha ido bien, en el home del usuario que se ha tecleado, aparecerá un nuevo directorio, `$HOME/cups-pdf` y dentro de este un archivo similar a `Test_Page.pdf`. Si se abre este archivo con un visualizador de archivos PDF, se podrá comprobar que es una prueba de impresión de CUPS.

Figura 15-77. Prueba de impresión



En esta pantalla se puede observar la prueba de impresión que se ha realizado en la imagen anterior.

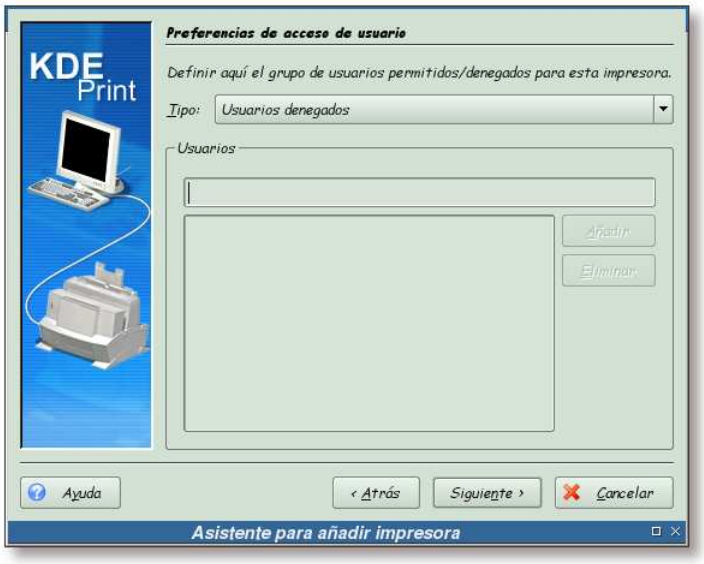
Figura 15-78. Selección de rótulos

CUPS permite imprimir páginas separadoras para los trabajos de impresión. Si desea hacer uso de esta característica, seleccione los rótulos que desee en esta pantalla, en caso contrario, pulse directamente sobre el botón “Siguiente”.

Figura 15-79. Cuotas de impresión

CUPS implemente un *rudimentario* sistema de cuotas de impresión. Como se va a hacer uso de PyKota para la administración de cuotas, esta opción no se utilizará. Pulse el botón “Siguiente” para continuar.

Figura 15-80. Permisos de acceso a la impresora

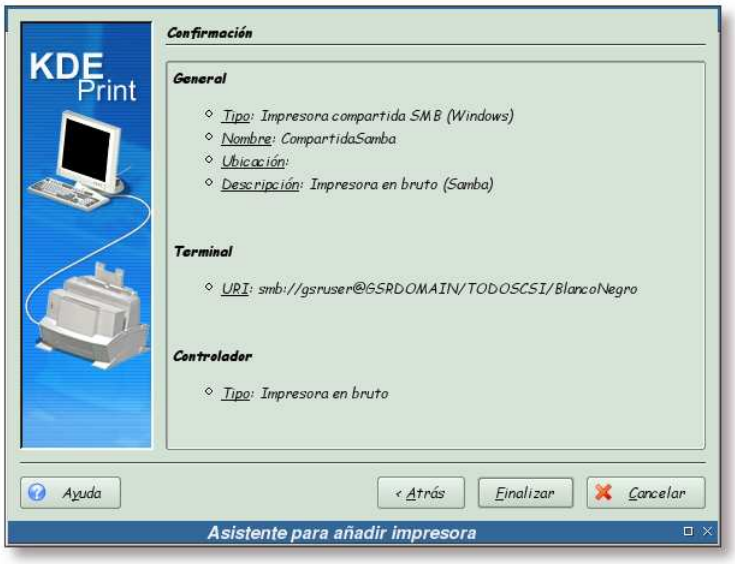


En esta pantalla se seleccionan los usuarios a los que se les permite, o no, imprimir. Como este control se realizará con la herramienta PyKota, pulse sobre el botón “Siguiente” directamente.

Figura 15-81. Información sobre la impresora

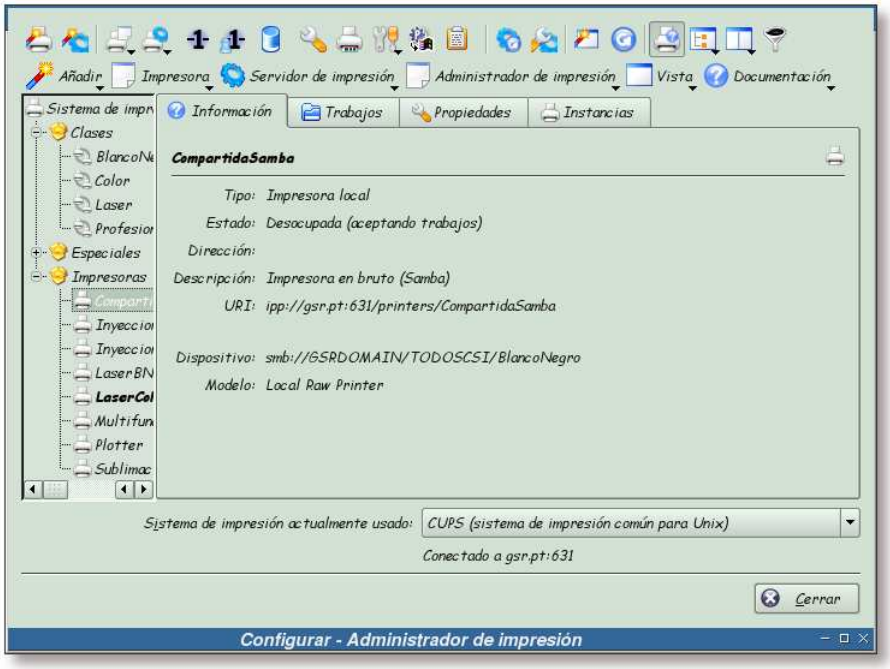
Complete los campos con el nombre, ubicación y descripción para la impresora que se está añadiendo. Pulse sobre el botón “Siguiente” para continuar.

Figura 15-82. Confirmación



Esta es la última pantalla antes de crear la nueva impresora. Revise la información sobre la misma, y si todo está correcto, pulse sobre el botón “Finalizar” para crear la impresora.

Figura 15-83. Nueva impresora *CompartidaSamba*



Se puede apreciar en el directorio de impresoras la aparición de una nueva entrada, en este caso la impresora *CompartidaSamba*.

Aquí finaliza la configuración de CUPS, el siguiente capítulo estará dedicado a la instalación y configuración de PyKota.

Notas

1. Recuérdese que las impresoras van a ser virtuales, gracias al paquete *cups-pdf*.
2. En el momento de generar esta documentación, la versión de estos controladores era la *5.0rc3*

```
$ /usr/bin/file /tmp/cups-samba.ss
cups-samba.ss: tar archive
```

IV. PyKota

Capítulo 16. Visión general

Introducción

PyKota es una aplicación GPL para dar soporte de cuotas de impresión a CUPS (*Common UNIX Printing System*) y LPRng (*LPR Next Generation*) en sistemas GNU/Linux y similares a Unix. Pykota ofrece una gran flexibilidad con respecto a los métodos empleados a la hora de contar las páginas. Por defecto, solicita directamente a la impresora el número de páginas que ha impreso, pero se puede utilizar el método para contar páginas que se desee.

Aplicaciones existentes

Las quotas de impresión son una característica muy útil para soluciones completas de impresión en red, desgraciadamente no existe mucho software de este tipo basadas en Software Libre bajo GNU/Linux.

Las siguientes aplicaciones cubren algunas de las necesidades de las cuotas de impresión:

- PrintBill (http://ieee.uow.edu.au/~daniel/software/printbill/) es una solución existente que hace un buen trabajo, pero todavía no soporta completamente CUPS, sólo LPRng.
- Printquota (http://printquota.sourceforge.net/) es otra solución existente, pero sólo trabaja con LPRng.
- CUPS, que es una aplicación de nueva generación para la impresión bajo sistemas Unix, posee cuotas de impresión, pero tiene una gran deficiencia en cuanto a características y no es extensible.

Comparativa de algunas soluciones existentes

La Tabla 16-1 muestra una comparativa entre PyKota, PrintBill, Printquota y PQuotas (http://pquota.free.fr/). Dicha tabla se ha obtenido de la página principal de PyKota y está elaborada por los autores de los sistemas de quota implicados (tabla original (www.librelogiciel.com/software/PyKota/pykota-vs-printbill-vs-printquota-vs-pquotas.html)).

Tabla 16-1. Comparativa entre 4 sistemas de quotas de impresión

Funcionalidad	PyKota	PrintBill	Printquota	PQuotas
Licencia	GNU GPL	GNU GPL, los módulos de Perl tiene doble licencia (Artística+GPL)	GNU GPL	La descarga y el uso es libre. No tiene licencia, sin embargo.
Soporte comercial	Sí	Sí	Sí	No
Paquetes propietarios	No	No	No	No
Madurez	Maduro	Maduro	Joven	Maduro

Funcionalidad	PyKota	PrintBill	Printquota	PQuotas
Lenguaje de programación	Python	Perl + C	C	Shell scripts + PHP
Uso de recursos computacionales	Ligero	Puede ser intenso si se hace uso de la cuenta de tinta	Ligero	Medio
Internacionalización	Sí: inglés, francés, español, portugués, brasileño, sueco, tailandés, alemán e italiano. Están planificadas más traducciones	Sí: inglés y francés. Están planificadas más traducciones	No	No, solamente francés
Interfaz web	Informe de quotas e historial únicamente, la interfaz web de administración está planificada	Sí, incluyendo informes gráficos	Todavía no. Una interfaz CGI está en preparación	Sí. Interfaz de administración completa en PHP
Almacenamiento central	Sí	Centralizado en la máquina donde se ejecuta PrintBill, pero no se puede disponer fácilmente de los datos desde fuera de PrintBill	Sí	Sí

Funcionalidad	PyKota	PrintBill	Printquota	PQuotas
Dependencias	• Python (requerido) • Módulo mxDateTime de Python (requerido) • PostgreSQL u OpenLDAP (requerido) • Módulo PyGreSQL o python-ldap de Python (requerido) • CUPS o LPRng (requerido) • Ghostscript (recomendado) • Net-SNMP (recomendado) • netatalk (recomendado) • Apache (recomendado)	• Perl (requerido) • Módulo File::Temp de Perl • Ghostscript (requerido) • LPRng (requerido) • Apache (recomendado) • Magicfilter (recomendado) • Samba (recomendado) • Libpng (requerido) • Ghostscript fonts (requerido) • GnuPlot (recomendado)	• LPRng (requerido) • libpopt (requerido) • Ghostscript (requerido) • PostgreSQL o MySQL (recomendado)	• LPRng o LPD (requerido) • Ghostscript (requerido) • enscript (requerido) • psselect (requerido) • pdf2ps (recomendado) • MySQL (requerido) • Apache (recomendado) • PHP (recomendado)
Sistemas de impresión soportados	CUPS y LPRng	LPRng y CUPS	LPRng	LPRng y LPD
¿Trabaja con clientes Windows?	Sí. Bien sea directamente a través de IPP o a través de Samba. Puede enviar mensajes Winpopup también.	Sí. Puede enviar mensajes Winpopup también.	Sí. Probado con Windows + Samba y directamente a través del sistema de impresión TCP de Windows	Sí

Funcionalidad	PyKota	PrintBill	Printquota	PQuotas
Documentación	Sí, todavía en desarrollo (formato en DocBook)	Sí, FAQ, Howto (en formato de texto)	Sí, instrucciones de instalación y post-instalación (en formato de texto)	Sí, sólo en francés (en formato HTML)
Métodos de contabilidad soportados	• Petición al contador interno de la impresora (contabilidad por hardware) • Delegación del control de copias a cualquier orden externa a su elección • Escaneo de trabajos de impresión muy poco confiable	• Computación de los niveles de tinta • Escaneo rápido de los trabajos de impresión	• Obtención del número de hojas de un trabajo de impresión a partir de Ghostscript	• Obtención del número de hojas de un trabajo de impresión a partir de Ghostscript
Modo de sólo contabilidad (no se aplican las quotas)	Sí	Sí	No	Sí
Cuotas de usuario por impresora	Sí	Sí	Sí	Sí
Cuotas de grupos de usuarios por impresora	Sí	No (en la lista de trabajos por hacer)	No	No
Cuotas para grupos de impresoras	Sí	No	No	No
Políticas de impresión con usuarios desconocidos	Completamente configurable	No	No	No
Cuotas de impresión	Sí	Sí	No	No
Gasto en dinero	Sí	Sí	Sí	No
Contador de páginas	Sí	Sí	Sí	Sí
Contador de tinta	Sí	Sí, por color	No	No

Funcionalidad	PyKota	PrintBill	Printquota	PQuotas
Cambio de configuración inmediata	Sí	No, se ha de reiniciar el demonio	Sí	Sí
Trabaja con impresoras en red	Sí	Sí	Sí	Sí
Trabaja con impresoras locales	Sí	Sí	Sí	Sí
Trabaja con impresoras tontas (*dumb*)	Depende del método contador y del sistema de impresión	Sí	Sí	Sí
Tipo de base de datos	PostgreSQL y OpenLDAP	Archivos planos (en la lista de tareas pendientes SQL y LDAP)	PostgreSQL, MySQL y archivos planos	MySQL (+NIS) (LDAP está planificado para el 2004)
Fácilmente extensible	Más que fácil. Se pueden añadir instrucciones externas simplemente en cualquier punto estratégico	Puede adaptarse a otros sistemas de impresión fácilmente	No	No
Paquetes para Debian	No, planificado. Algunos scripts permiten una integración fácil en un sistema Debian	Sí	No, planificado	No
Paquetes RPM	Sí, con recargo monetario	No, sin embargo se incluye un archivo .spec	No	No
Paquetes tar	Sí, con recargo monetario	Sí	Sí	Sí
Acceso CVS	Sí	No	Sí	Sí

Funcionalidad	PyKota	PrintBill	Printquota	PQuotas
Precisión	Con el método de contabilidad por defecto, PyKota mantiene el número de páginas impresas solicitando dicha información a la impresora, por lo tanto la precisión es justamente el número de hojas consumidas. Con LPRng, PyKota siempre lleva un trabajo de impresión de retraso, sin embargo, en caso de atasco de papel o problemas similares, los usuario son debidamente cobrados. Como algunas impresoras no poseen un contador de páginas almacenado en la NVRAM, o no actualizan dicho contador en tiempo real (Hewlett-Packard), este contador es incorrecto en algunas ocasiones cuando se enciende una impresora, PyKota intenta solucionar lo mejor posible esta limitación de las impresoras. Con métodos contadores externos, la precisión la marcan estos métodos, ya que se especifica directamente la orden a utilizar para computar el tamaño del trabajo. Sin embargo, se puede sufrir los mismos problemas	Printbill mantiene los consumos de papel y tinta preguntando a Ghostscript y/o calculando los niveles de tinta, lo que puede consumir muchos recursos. De todas formas, es exacto y justo en sus cálculos, al menos en teoría. En caso de atascos de papel o problemas similares, los usuarios no son justamente cobrados. Printbill puede escanear rápidamente los trabajos de impresión para contar únicamente el número de páginas, lo que no conlleva un consumo intensivo de recursos, sin embargo el contador de páginas puede ser explotado por usuarios con los conocimientos necesarios	Printquota está diseñado para contar páginas. Si el contador de páginas y si el usuario posee la cuota suficiente (de páginas) permite imprimir. Printquota es injusto con aquellas personas que hacen poco uso de la tinta.	Tan justo como lo pueda ser Ghostscript. PQuotas borra automáticamente todos los trabajos que no están en el formato permitido (text/ps/pdf), para evitar la mayoría de las impresiones no deseadas. Los usuarios pueden ver su historial de impresiones, lo que evita muchas reclamaciones

Funcionalidad	PyKota	PrintBill	Printquota	PQuotas

Características y funcionalidades de PyKota

Sistemas operativos

- Cualquier sistema operativo similar a Unix que actúe como un servidor de impresión
- Cualquier sistema operativo que actúe como cliente

Sistemas de impresión

- Soporta tanto el sistema de impresión CUPS como LPRng

Bases de datos

- Soporta PostgreSQL como backend de almacenamiento de quotas. Se incluye un script completo para la creación de la base de datos en SQL
- Soporta OpenLDAP como backend de almacenamiento de quotas. Se incluyen un esquema y un ejemplo de árbol para LDAP. Añadir PyKota a su infraestructura LDAP existente es realmente fácil gracias a la gran configurabilidad de PyKota

Impresoras

- Los métodos de contabilidad por hardware o por software son completamente configurables
- Soporta cualquier impresora que pueda devolver su contador interno de páginas. Puede preguntar a las impresoras por su contador interno de páginas vía SNMP, Netatalk, PJL, PS o cualquier otra forma. Esto es completamente configurable
- Soporta DSC y PostScript binarios, PDF, PCL5, PCLXL (o PCL6) e impresoras ESC/P2 nativamente por métodos de contabilidad software. Se están preparando más formatos

Sistemas de cuotas

- Soporta cuotas por impresora y por grupos de impresoras

- Soporta cuotas por usuario y por grupos de usuarios
- Soporta cuotas de papel. Se pueden establecer de forma diferente las cuotas de papel para una impresora o para los usuarios/grupos
- Soporta cuotas sobre el balance de consumo en cualquier moneda. Se pueden asignar cuotas sobre el balance de consumo a cada usuario. Los balances de las cuentas se comparten entre todas las impresoras
- Las cuotas de papel y de balance de consumo se pueden establecer/restablecer independientemente
- Se puede asignar un factor limitante, quota de papel o balance de consumo, a cada usuario o grupo de usuarios
- Los precios por página o por trabajo se pueden establecer independientemente en cualquier impresora
- Se puede establecer la cuota mínima de consumo de papel o balance de consumo
- Tanto los límites por software como por hardware así como el intervalo de *gracia* se pueden establecer para una cuota de papel
- Posibilidad de deshabilitar las quotas a cualquier usuario o grupo de usuarios, mientras que se sigue manteniendo el contador de páginas

Administración

- Se pueden utilizar potentes herramientas de administración para automatizar el establecimiento o restablecimiento de las cuotas o los balances de consumo en intervalos específicos
- Las herramientas de configuración pueden modificar varios usuarios, grupos o impresoras a la vez
- Los balances de consumo se pueden establecer, incrementar y decrementar
- Tanto las impresoras como los usuarios se pueden añadir automáticamente con la primera impresión, de una manera completamente configurable
- Existe un generador de informes sobre cuotas disponible tanto desde la consola como desde cualquier navegador web. El generador de informes basado en web puede protegerse con clave.
- El generador de informes sobre las cuotas, puede adelantar la información sobre el coste de un trabajo de impresión
- Se puede configurar una política de actuación para los usuarios no registrados para cada impresora, tanto para denegar la impresión, permitirla o delegar la decisión a una herramienta externa
- Los mensajes de aviso y de error se pueden enviar automáticamente a través de correo electrónico al administrador, al usuario, a ambos o a ninguno
- El contenido de los mensajes de error y aviso es completamente configurable
- La configuración se puede cambiar sin necesidad de reiniciar el sistema de impresión
- Se mantiene un historial de impresión completo. Se puede deshabilitar se es preciso
- Se pueden ajustar automáticamente las cuotas mínimas o el balance de saldo de forma regular o lanzarlo manualmente

- Herramienta de exportación de datos muy potente, que permite llevar los datos de PyKota a otro software

Interfaz de usuario

- Todas las órdenes de consola aceptan el parámetro -h | --help, que mostrará todas las opciones disponibles y ejemplos de uso
- Completamente internacionalizada. Actualmente soporta los idiomas: inglés, francés, español, portugués, brasileño, sueco, tailandés, alemán e italiano. Más en camino

Información adicional sobre el proyecto

Página principal

Pykota dispone de una página principal, www.librelogiciel.com/software/PyKota/Presentation/action_Presentation (http://www.librelogiciel.com/software/PyKota/Presentation/action_Presentation), desde donde puede obtener mucha información. De hecho, para elaborar esta sección ha utilizado la información allí disponible.

Cómo obtener PyKota

El código fuente de Pykota se distribuye bajo los términos de la licencia GPL (vea los GNU General Public License y Apéndice AW para más información) y su código fuente está disponible desde distintas fuentes, como se verá a continuación.

Hay dos formas de conseguir PyKota, de forma gratuita y de pago. A continuación se verá en que consisten:

- **Obtención gratuita del código:** La única forma de conseguir Pykota de forma gratuita es bajando el código fuente desde su CVS, para más información visite: http://savannah.nongnu.org/cvs/?group=pykota.

  Si obtiene el código fuente de esta forma, estará obteniendo una copia “no oficial” de PyKota, lo que implicará ver la palabra “unofficial” cuando se muestre la información sobre la versión del programa desde la línea de comandos con el parámetro *--version*.
- **Obtención del código pagando:** De esta forma podrá obtener el código fuente empaquetado con *tar*. El autor de este programa ha optado por una forma de distribución retributiva de su software, lo que es perfectamente legal y no atenta en ningún momento con la licencia que está utilizando. Si se emplea esta forma de obtención del código, se estará ayudando al autor a continuar con el desarrollo del

programa, por lo que se le anima a comprar su versión oficial de PyKota (la cual trae muchas ventajas, como soporte durante un año).

Para más detalles sobre las formas de obtener PyKota, visite el siguiente enlace: www.librelogiciel.com/software/PyKota/Download/action_Download (http://www.librelogiciel.com/software/PyKota/Download/action_Download).

Documentación

El código fuente de PyKota viene con un directorio destinado a la documentación, `doc/`. Bajo el mismo está la documentación "oficial" del programa así como un documento escrito en OpenOffice.org (http://www.openoffice.org/) por Dennis Romero L., con la salvedad de que está en español.

Información de soporte

Actualmente hay tres vías principales para obtener ayuda sobre Pykota:

IRC: Puede acceder al canal de #pykota alojado en el servidor irc.freenode.net. Más información en: www.librelogiciel.com/software/PyKota/IRC/action_IRC (http://www.librelogiciel.com/software/PyKota/IRC/action_IRC).

Lista de correo: PyKota pone a su disposición una lista de correo desde donde se podrán formular preguntas relativas a PyKota, más información en: http://cgi.librelogiciel.com/mailman/listinfo/pykota.

Soporte derivado de la obtención de una copia oficial de PyKota: Al comprar una versión oficial de PyKota, está también adquiriendo un año de soporte técnico privilegiado sobre el programa.

Reporte de bugs

La página principal de PyKota pone a su disposición un formulario desde el cual se podrán enviar sugerencias, retroalimentación y posibles errores encontrados en el programa al autor del mismo. Más detalles en: www.librelogiciel.com/software/PyKota/Features/Feedback (http://www.librelogiciel.com/software/PyKota/Features/Feedback).

Aunque si lo desea, puede hacer uso de la dirección de correo electrónico del autor para tal fin: Jerome Alet, <`alet@librelogiciel.com`>.

Cómo contactar

Para obtener más información sobre PyKota, Jerome Alet (autor del programa) pone a su disposición su cuenta de correo: <`alet@librelogiciel.com`>.

Capítulo 17. Obtención del código fuente y generación de un paquete *deb*

Introducción

El objetivo final de este capítulo es obtener un paquete deb de PyKota, con el cual poder instalar dicho software en el sistema. Se ha decidido generar un paquete deb para mantener el sistema lo más *limpio y ordenado* posible.

Los pasos para lograr esto serán, en primer lugar obtener el código fuente de PyKota, hacer las modificaciones oportunas para generar el paquete deb y finalmente generar dicho paquete.

En las siguientes secciones se mostrará el proceso seguido para cumplir con este primer objetivo.

Generación de un paquete *deb* para PyKota

Descarga del código fuente de PyKota

Para obtener el código fuente de pykota, refiérase a la
la sección de nombre *Cómo obtener PyKota* en Capítulo 16.

Para la realización de esta documentación se ha elegido descargar el código fuente directamente del CVS. La versión que se ha empleado es la 1.20alpha25.

Modificaciones para generar el paquete *deb*

Lo único que se modificará en el código fuente de PyKota será la versión del paquete que se genere. Para ello, aplique el siguiente parche a la versión 1.20alpha25 de pykota (en el Ejemplo 17-1 se muestra como hacerlo):

```
diff -urN pykota/debian/changelog pykota-1.20alpha25/debian/changelog
--- pykota/debian/changelog     2004-10-13 18:35:03.000000000 +0200
+++ pykota-1.20alpha25/debian/changelog 2004-10-13 18:45:06.000000000 +0200
@@ -1,3 +1,9 @@
+pykota (1.20alpha25) unstable; urgency=low
+
+  * Update from CVS.
+
+ -- Sergio González González <sergio.gonzalez@hispalinux.es>  Wed, 13 Oct 2004 18:44:34
+
 pykota (1.20alpha24) unstable; urgency=low

   * Update from CVS.
```

Ejemplo 17-1. Aplicación del parche de modificaciones al código de PyKota

Sitúese en el directorio que contenga el código fuente de PyKota y teclee la siguiente orden, suponiendo que el parche se encuentra en el directorio padre, se llama `patch-pykota` y está en texto plano:

```
$ /bin/cat ../patch-pykota | /usr/bin/patch -p1
patching file debian/changelog
```

Generación del paquete deb

Ejemplo 17-2. Generando el paquete *deb* de PyKota

Sitúese en el directorio que contenga el código fuente de PyKota, edite el archivo `setup.py` y cambie el valor de la variable *DEBIAN_BUILD_PACKAGE* a "1".

Asegúrese de que el archivo `debian/rules` tiene permisos de ejecución y teclee:

```
$ /usr/bin/dpkg-buildpackage -rfakeroot -us -uc -b
dpkg-buildpackage: source package is pykota
dpkg-buildpackage: source version is 1.20alpha25
dpkg-buildpackage: source maintainer is Sergio González González <sergio.gonzalez@hispalinux.es>
dpkg-buildpackage: host architecture is i386
 fakeroot debian/rules clean
dh_testdir
dh_testroot
rm -f build-stamp
/usr/bin/python setup.py clean --all
running clean

...

dpkg-deb: construyendo el paquete 'pykota' en '../pykota_1.20alpha25_all.deb'.
 dpkg-genchanges -b
dpkg-genchanges: binary-only upload - not including any source code
dpkg-buildpackage: binary only upload (no source included)
```

La acción anterior debería haber generado un archivo *deb* en el directorio padre del actual. El archivo en cuestión debería denominarse `pykota_1.20alpha25_all.deb`.

A partir de este momento, ya se está en disposición de instalar PyKota, el siguiente capítulo mostrará la forma de hacerlo.

Capítulo 18. Instalación

Introducción

Este capítulo va a describir el proceso de instalación de PyKota, que tras la generación del paquete *deb* en el capítulo anterior, Capítulo 17, se simplificará mucho.

Instalación del paquete

El proceso de instalación de PyKota se reduce a la instalación del paquete generado en la la sección de nombre *Generación del paquete deb* en Capítulo 17. Para ello sitúese en el directorio donde se encuentre dicho paquete y siga los pasos del siguiente ejemplo:

Ejemplo 18-1. Instalación del paquete *pykota*

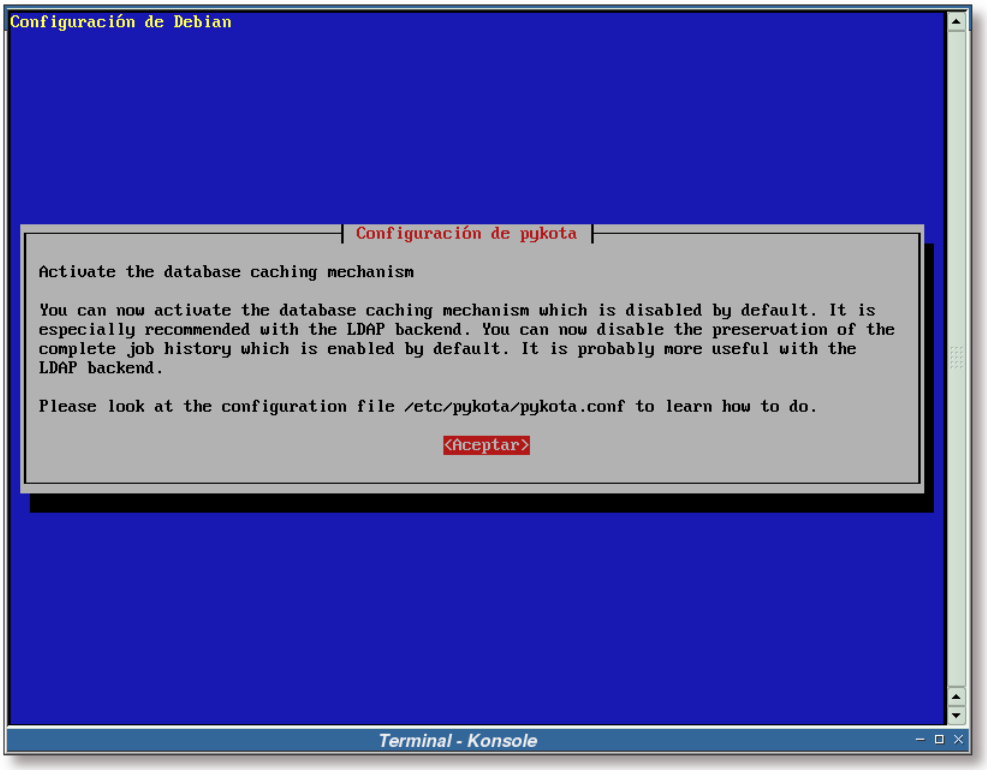
```
# /usr/bin/dpkg -i pykota_1.20alpha25_all.deb
Seleccionando el paquete pykota previamente no seleccionado.
(Leyendo la base de datos ...
141967 ficheros y directorios instalados actualmente.)
Preparando para reemplazar pykota 1.20alpha25 (usando pykota_1.20alpha25_all.deb) ...
Desempaquetando el reemplazo de pykota ...
Configurando pykota (1.20alpha25) ...
```

Nota: Si quiere ver información relativa a PyKota, tal vez tenga que teclear la siguiente orden:

```
# /usr/sbin/dpkg-reconfigure --priority=low pykota
```

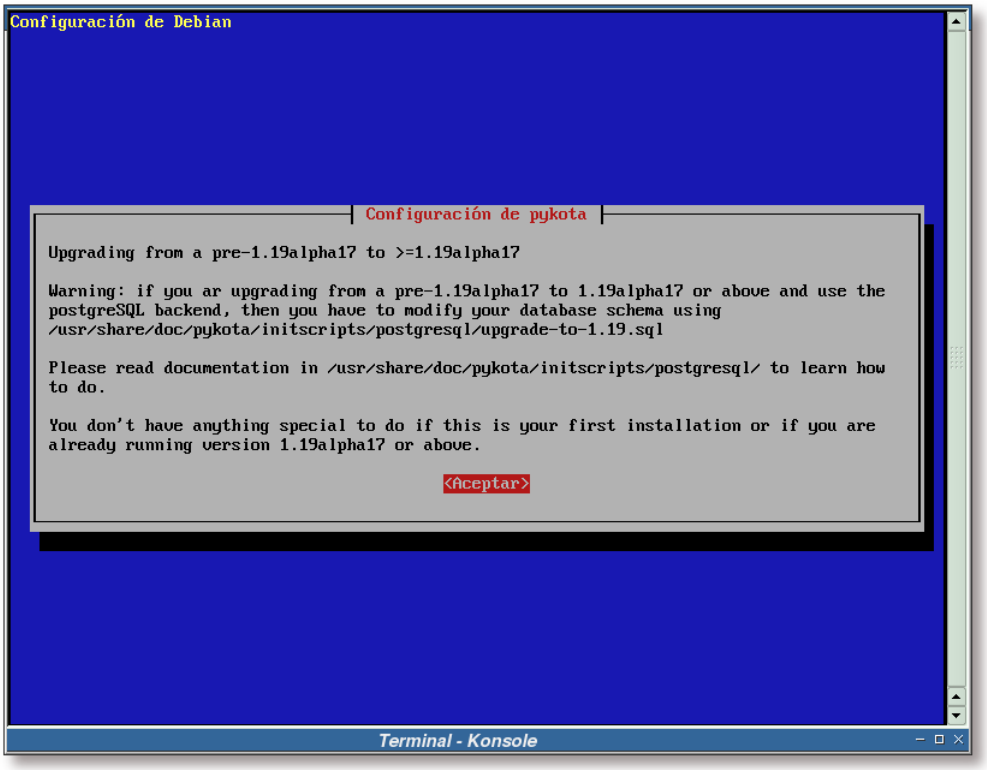
El resultado de esta orden se muestra en las siguientes capturas de pantalla:

Figura 18-1. Información de PyKota a través de debconf I



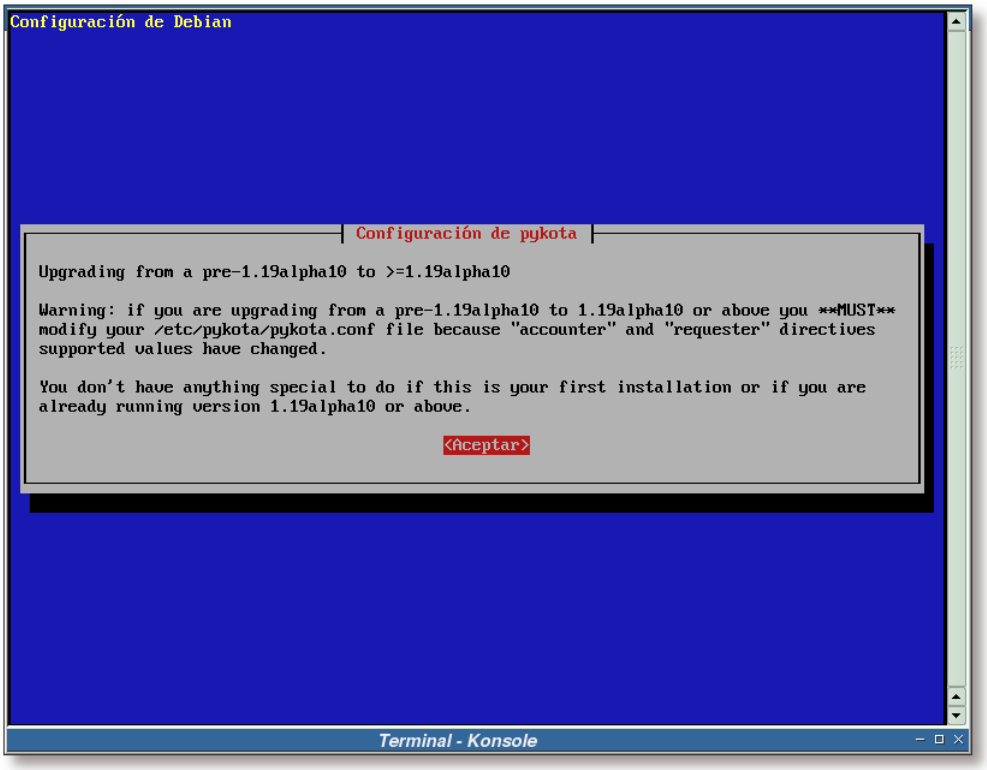
Información sobre el mecanismo de caché existente para la base de datos que utiliza PyKota.

Figura 18-2. Información de PyKota a través de debconf II



Información de actualización de versiones pre-1.19alpha17 a versiones iguales o superiores a 1.19alpha17.

Figura 18-3. Información de PyKota a través de debconf III



Información de actualización de versiones pre-1.19alpha10 a versiones iguales o superiores a 1.19alpha10.

Con esto concluiría el proceso de instalación, ahora sólo queda configurar PyKota, tema que se abordará en el Capítulo 20.

Capítulo 19. Retoques iniciales en el sistema

Introducción

Antes de proceder con la configuración de PyKota, es necesario realizar una serie de ajustes en el sistema. En primer lugar hay que elegir la base de datos sobre la cual se almacenarán los datos de las cuotas. PyKota da la posibilidad de almacenar estos datos sobre Postgresql o sobre un directorio LDAP.

La elección ha sido LDAP, por lo que habrá que modificar el servidor slapd para que soporte los datos de PyKota y, finalmente, crear la estructura necesaria en el directorio LDAP para PyKota.

Este capítulo mostrará como realizar estas modificaciones en el sistema.

Modificaciones en la configuración de slapd

En primer lugar se ha añadir una línea similar a la siguiente en el archivo de configuración de slapd (`/etc/ldap/slapd.conf`), en la sección de definiciones de esquemas y objectClass (añádala al final de la lista de esquemas, para evitar problemas):

```
include         /etc/ldap/schema/pykota.schema
```

Y, finalmente, puede añadir una serie de índices que acelerarán un poco las búsquedas sobre los atributos de PyKota. Para ello añada las siguientes entradas en la sección de índices del archivo de configuración de slapd:

```
# PyKota
index pykotaUserName          pres,eq,sub
index pykotaGroupName         pres,eq,sub
index pykotaPrinterName       pres,eq,sub
index pykotaLastJobIdent      eq
```

En este momento sólo queda regenerar los índices de slapd y reiniciar el demonio:

Ejemplo 19-1. Regenerando los índices de LDAP y reiniciando el demonio slapd

```
# /usr/sbin/slapindex -v
indexing id=00000001
indexing id=00000002
indexing id=00000016
indexing id=00000017
indexing id=00000018
indexing id=00000019
indexing id=0000001b
indexing id=0000001c
indexing id=0000001d
indexing id=0000001e
indexing id=00000020
indexing id=00000021
```

```
indexing id=00000022
indexing id=00000023
indexing id=00000024
indexing id=00000025
indexing id=00000027
indexing id=00000028
indexing id=0000002a
indexing id=0000002b
# /etc/init.d/slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: slapd.
```

Con esto finalizarían las modificaciones en el servidor slapd.

Creación de la estructura para PyKota en LDAP

En esta sección se creará la estructura para PyKota en el directorio LDAP. Las siguientes líneas muestran, en formato LDIF, las entradas que se han de incorporar al directorio LDAP:

> **Nota:** Esta estructura se ha basado en el archivo `/usr/share/doc/pykota/initscripts/ldap/pykota-sample.ldif` que se distribuye con PyKota.

```
# Entry 1: ou=pykota,dc=gsr,dc=pt
dn:ou=pykota,dc=gsr,dc=pt
ou: pykota
objectClass: top
objectClass: organizationalUnit

# Entry 2: ou=printers,ou=pykota,dc=gsr,dc=pt
dn:ou=printers,ou=pykota,dc=gsr,dc=pt
ou: printers
objectClass: top
objectClass: organizationalUnit

# Entry 3: ou=jobs,ou=pykota,dc=gsr,dc=pt
dn:ou=jobs,ou=pykota,dc=gsr,dc=pt
ou: jobs
objectClass: top
objectClass: organizationalUnit

# Entry 4: ou=uquotas,ou=pykota,dc=gsr,dc=pt
dn:ou=uquotas,ou=pykota,dc=gsr,dc=pt
ou: uquotas
objectClass: top
objectClass: organizationalUnit

# Entry 5: ou=gquotas,ou=pykota,dc=gsr,dc=pt
dn:ou=gquotas,ou=pykota,dc=gsr,dc=pt
ou: gquotas
```

```
objectClass: top
objectClass: organizationalUnit

# Entry 6: ou=lastjobs,ou=pykota,dc=gsr,dc=pt
dn:ou=lastjobs,ou=pykota,dc=gsr,dc=pt
ou: lastjobs
objectClass: top
objectClass: organizationalUnit
```

Suponiendo que la estructura anterior se encuentra almacenada en el archivo `pykota.ldif`, ejecute la siguiente orden para incorporarla a su directorio LDAP:

Ejemplo 19-2. Creando la estructura para PyKota en LDAP

```
$ /usr/bin/ldapadd -x -D "cn=admin,dc=gsr,dc=pt" -W -h gsr.pt -f pykota.ldif
Enter LDAP Password: [clave]
adding new entry "ou=pykota,dc=gsr,dc=pt"

adding new entry "ou=printers,ou=pykota,dc=gsr,dc=pt"

adding new entry "ou=jobs,ou=pykota,dc=gsr,dc=pt"

adding new entry "ou=uquotas,ou=pykota,dc=gsr,dc=pt"

adding new entry "ou=gquotas,ou=pykota,dc=gsr,dc=pt"

adding new entry "ou=lastjobs,ou=pykota,dc=gsr,dc=pt"
```

Esto completaría las modificaciones iniciales a realizar en el sistema, ahora se puede proceder a la configuración de PyKota, para ello vea el Capítulo 20

Capítulo 20. Configuración

Introducción

La configuración de PyKota se realiza en dos archivos: `/etc/pykota/pykota.conf` y `/etc/pykota/pykotadmin.conf`. Como dichos archivos son suficientemente explicativos, sólo se van a realizar una serie de apuntes sobre los mismos. Refiérase a los apéndices: Apéndice AG y Apéndice AH para ver un ejemplo de configuración de PyKota.

Usuarios de pykota

PyKota hace uso de dos usuarios para el acceso al directorio LDAP: uno destinado a la lectura de la base de datos de cuotas de impresión y otro destinado a la administración de esta base de datos. El primer usuario sólo ha de tener permisos de lectura y el segundo de lectura/escritura en la base de datos.

Los usuarios utilizados en esta documentación son:

- *pykotauser:* usuario de sólo lectura.
- *pykotaadmin:* administrador de PyKota.

Puede hacer uso del siguiente LDIF para generar dichos usuarios en su sistema:

```
# Entry: cn=pykotauser,dc=gsr,dc=pt
dn:cn=pykotauser,dc=gsr,dc=pt
cn: pykotauser
objectClass: simpleSecurityObject
objectClass: organizationalRole
userPassword: {crypt}y1pYJeZPC49BY
description: Usuario de acceso como sólo lectura para PyKota

# Entry: cn=pykotaadmin,dc=gsr,dc=pt
dn:cn=pykotaadmin,dc=gsr,dc=pt
cn: pykotaadmin
objectClass: simpleSecurityObject
objectClass: organizationalRole
userPassword: {crypt}y1pYJeZPC49BY
description: Usuario de acceso como sólo lectura para PyKota
```

En el siguiente ejemplo se muestra como añadirlos al directorio LDAP. Se supone que el archivo `usuarios-pykota.ldif` contiene los datos LDIF anteriores:

Ejemplo 20-1. Añadiendo los usuarios relativos a PyKota en el directorio LDAP

```
$ /usr/bin/ldapadd -x -D "cn=admin,dc=gsr,dc=pt" -W  -f usuarios-pykota.ldif
Enter LDAP Password: [Clave]
adding new entry "cn=pykotauser,dc=gsr,dc=pt"
```

```
adding new entry "cn=pykotaadmin,dc=gsr,dc=pt"
```

El siguiente paso consiste en dar los permisos adecuados a los usuarios en el directorio LDAP. Para ello edite el archivo de configuración de OpenLDAP, `/etc/ldap/slapd.conf`, y añada las siguientes líneas en los atributos *userPassword, sambaLMPassword,sambaNTPassword y* * de las listas de control de acceso:

```
by dn="cn=pykotaadmin,dc=gsr,dc=pt" write
by dn="cn=pykotauser,dc=gsr,dc=pt" read
```

Por último, para asegurarse de que los usuarios con los que se autentificará PyKota en el servidor OpenLDAP no tienen límites de peticiones de búsquedas, añada las siguientes líneas:

```
# User Limits
limits dn="cn=pykotauser,dc=gsr,dc=pt" size.soft=-1 size.hard=soft
limits dn="cn=pykotaadmin,dc=gsr,dc=pt" size.soft=-1 size.hard=soft
```

Nota: En el Apéndice Q tiene un archivo de configuración completo.

Repaso sobre las principales opciones de configuración

En esta sección se realizará un breve repaso sobre las opciones más importantes de configuración de PyKota.

Opciones del archivo `/etc/pykota/pykota.conf`

Este es el archivo de configuración principal de PyKota. Posee una sección *[global]*, donde se configuran las opciones por defecto para todas las impresoras administradas por PyKota. Opcionalmente, pueden existir otras secciones (*[nombreimpresora]*), destinadas a personalizar la configuración de una impresora en concreto.

Aquí sólo se tratará la sección global, por ser las demás secciones similares a esta y dependientes del sistema donde se instale PyKota.

Datos de LDAP

Las siguientes opciones le indican a PyKota el *backend* que ha de utilizar y los datos relativos al mismo:

```
storagebackend: ldapstorage
storageserver: ldap://gsr.pt:389
storagename: dc=gsr,dc=pt
storageuser: cn=pykotauser,dc=gsr,dc=pt
storageuserpw: ********
```

La base a partir de la cual se almacenarán los usuarios de PyKota en el directorio LDAP:

```
userbase: ou=people,dc=gsr,dc=pt
```

```
userrdn: uid
```

La base a partir de la cual se almacenará el crédito que poseen los usuarios de PyKota:

```
balancebase: ou=people,dc=gsr,dc=pt
balancerdn: uid
```

La base a partir de la cual se almacenarán los grupos de PyKota en el directorio LDAP:

```
groupbase: ou=groups,dc=gsr,dc=pt
grouprdn:  cn
```

La base a partir de la cual se almacenarán los datos de las impresoras de PyKota en el directorio LDAP:

```
printerbase: ou=printers,ou=pykota,dc=gsr,dc=pt
printerrdn: cn
```

La base a partir de la cual se almacenarán los trabajos de impresión, cuotas de usuario, cuotas de grupo y el último trabajo realizado, respectivamente:

```
jobbase: ou=jobs,ou=pykota,dc=gsr,dc=pt
userquotabase: ou=uquotas,ou=pykota,dc=gsr,dc=pt
groupquotabase: ou=gquotas,ou=pykota,dc=gsr,dc=pt
lastjobbase: ou=lastjobs,ou=pykota,dc=gsr,dc=pt
```

Creación de usuarios/grupos

Estas dos opciones informan a PyKota como se han de añadir los datos de los usuarios y grupos en el sistema. Se ha seleccionado la opción de añadir la información sobre la cuota de impresión a los usuarios/grupos ya existentes:

```
newuser : attach(posixAccount, warn)
newgroup : attach(posixGroup, warn)
```

Correo electrónico de los usuarios

Esta opción indica cual es el atributo, dentro del directorio LDAP, que ha de buscar PyKota para obtener el correo electrónico de los usuarios:

```
usermail : mail
```

Atributo que contiene la lista de miembros de un grupo

Indique en esta variable el atributo que contiene la lista de miembros de un grupo determinado:

```
groupmembers: memberUid
```

Servidor SMTP

Servidor de correo utilizado para enviar correos:

> **Sugerencia:** Si desea integrar su servidor de correo con el sistema que se está configurando en esta documentación, le aconsejo que lea el documento http://guepardo.dyndns.org:8080/sergio-gonzalez/doc/08-postfix-ldap/html/

```
smtpserver: localhost
```

Dominio para los correos electrónicos

Esta variable establece el dominio al cual se enviarán los correos electrónicos de los usuarios del sistema. Es decir, será el valor que se ponga detrás de la @ como se muestra a continuación: *usuario@gsr.pt*.

```
maildomain: gsr.pt
```

Contado de páginas

Pykota permite realizar el contado de las páginas que se han impreso de dos maneras: mediante hardware (dejándole el trabajo de contado a la impresora) o mediante software (haciendo uso de un contador de páginas propio).

En esta documentación, por el tipo de impresoras utilizadas (impresoras virtuales), se ha elegido el contado de páginas mediante software:

```
accounter: software(/usr/bin/pkpgcounter)
```

Qué hacer ante un error del subsistema de contado de páginas

Existen dos posibles comportamientos ante un error en la contabilidad de las páginas: *continuar* con la cola de trabajos pendientes, como si nada hubiese ocurrido o *detener* la cola de trabajos pendientes.

La opción elegida es la segunda, se detendrá el sistema de impresión ante un fallo en la contabilidad de las páginas.

```
onaccountererror: stop
```

Información sobre el administrador de PyKota

Información sobre quien es y cual es la dirección de correo electrónico del administrador de PyKota:

```
admin: Sergio González González
adminmail: root@localhost
```

Envío de notificaciones

Se le indica a PyKota que envíe, tanto al usuario como al administrador, notificaciones sobre el estado de la cuota de un usuario determinado:

```
mailto: both
```

Texto de las notificaciones

Por defecto, PyKota provee una serie de mensajes de ejemplo que se emplearán para el envío de correos electrónicos cuando las cuotas de los usuarios se hayan sobrepasado o hayan alcanzado un cierto límite.

Puede personalizar estos mensajes, las siguientes líneas le muestran un ejemplo:

```
# Poor man’s warning message
# The warning message that is sent if the "poorman" value is reached
# Again this must appear in the global section
poorwarn: Su saldo en la cuota de impresión es bajo.
 Dentro de poco no podrá volver a imprimir.

# Soft limit reached warning message
# The warning message that is sent if the soft quota limit is reached
# May appear either globally or on a per-printer basis
softwarn: Ha alcanzado su límite blando en la cuota de impresión.
 Esto significa que podrá seguir imprimiendo algún tiempo,
 pero debería contactar con su administrador para comprar
 más cuota de impresión.

# Hard limit reached error message
# The error message that is sent if the hard quota limit is reached
# May appear either globally or on a per-printer basis
hardwarn: Ha alcanzado su límite duro en la cuota de impresión.
 Esto significa que no podrá volver a imprimir.
 Contacte con su administrador en <root@gsr.pt> tan
 pronto como le sea posible para solucionar el
 problema.
```

¿Se permite a los usuarios sobrepasar la cuota de impresión?

Esta variable controla si se permite o no a un usuario completar un trabajo, si durante la impresión del mismo, se termina su cuota de impresión.

La opción *strict* no permite esta situación, por lo que alertará al usuario y no permitirá la impresión. Esta es la opción elegida.

La opción *laxist* permite finalizar el trabajo de impresión, si durante el trascurso del mismo, se termina la cuota de impresión del usuario.

```
enforcement: strict
```

Opciones del archivo `/etc/pykota/pykotadmin.conf`

En este archivo se configura el usuario que tendrá acceso de escritura en la base de datos de PyKota. En este caso se utilizará el usuario *pykotaadmin*, por lo que se configurará de la siguiente forma:

```
# Quota Storage administrator's name and password
storageadmin: cn=pykotaadmin,dc=gsr,dc=pt
storageadminpw: **********
```

> **Importante:** Asegúrese de que el archivo `/etc/pykota/pykotadmin.conf` sólo puede ser leído por el usuario *root* y por el usuario con el que se ejecuta el sistema de impresión.

Capítulo 21. Modificaciones en las impresoras de CUPS

Introducción

En el apartado dedicado a CUPS
(Parte III en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*) se añadieron una serie de impresoras al sistema y se comentó que la cuota de impresión se iba a administrar con PyKota.

Este capítulo trata de mostrar las modificaciones que se han de realizar en las impresoras presentes en el sistema para que PyKota controle las cuotas de impresión de las mismas.

Modificación del archivo `/etc/cups/printers.conf`

En el archivo `/etc/cups/printers.conf` se encuentra disponible la configuración para cada una de las impresoras presentes en el sistema, y administradas por CUPS.

Para conseguir que PyKota administre las cuotas de impresión para todas, o algunas de las impresoras allí presentes (usted elige qué impresoras estarán o no administradas por PyKota), sólo tendrá que modificar el parámetro *DeviceURI*, anteponiéndole el valor “cupspykota:” a la dirección de la impresora.

De esta forma, suponga que tiene la siguiente definición en dicho archivo:

```
</Printer>
<Printer InyeccionBN>
Info Impresora de inyección de tinta en Blanco y Negro
Location Laboratorio 2
DeviceURI cups-pdf:/
State Idle
Accepting Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
</Printer>
```

Para que la impresora *InyeccionBN* pasase a estar administrada por PyKota, habría que anteponer al valor del parámetro *DeviceURI* la cadena “cupspykota:”, como se muestra a continuación:

```
</Printer>
<Printer InyeccionBN>
Info Impresora de inyección de tinta en Blanco y Negro
Location Laboratorio 2
DeviceURI cupspykota:cups-pdf:/
State Idle
Accepting Yes
JobSheets none none
QuotaPeriod 0
```

```
PageLimit 0
KLimit 0
</Printer>
```

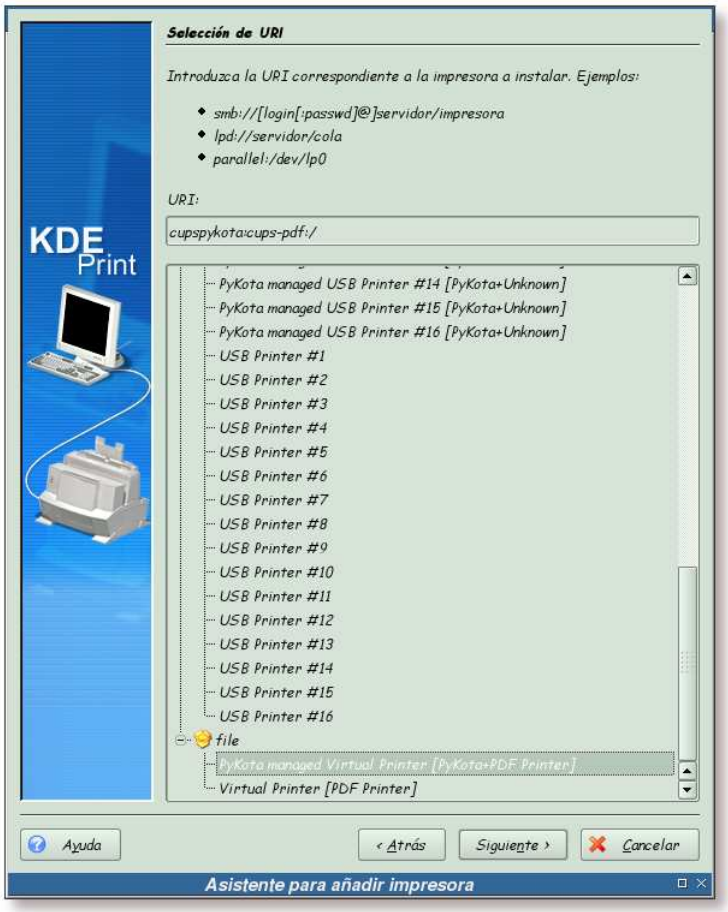
Ha de realizar esta operación con todas las impresoras, cuya cuota de impresión, quiera que se administre con PyKota

Una vez haya realizado las modificaciones oportunas, sólo queda reiniciar el demonio **cupsd** (vea el Ejemplo 15-4). A partir de ese momento, la impresión en las impresoras modificadas pasará a estar controlada por PyKota.

Añadiendo una impresora bajo el control de PyKota

Una vez se ha instalado PyKota en el sistema, a la hora de añadir una nueva impresora, se presentará la opción de instalar la nueva impresora bajo el control de PyKota. En la siguiente imagen se muestra esta nueva posibilidad:

Figura 21-1. Añadiendo una impresora con soporte para PyKota



Tras la instalación de PyKota, en el cuadro de selección del URI de una impresora, aparecerá la posibilidad de instalar la impresora con y sin soporte de PyKota.

Capítulo 22. Estableciendo las cuotas de impresión

Introducción

Ahora que el sistema de impresión ya está configurado para hacer uso de PyKota en el control de la cuotas de impresión, falta por establecer dichas cuotas.

Este capítulo le va a guiar en el proceso de establecimiento de las cuotas de impresión para las impresoras presentes en el sistema. También le mostrará como realizar la gestión de los usuarios y grupos del sistema para que interoperen con el sistema de impresión.

Estableciendo los precios en las impresoras

En la siguiente tabla se muestran los precios que se establecerán en las impresoras creadas en la parte dedicada a CUPS (Parte III en *Integración de redes con OpenLDAP, Samba, CUPS y PyKota*). Hay dos tipos de precios: por página (obligatorio) y por trabajo (opcional):

Tabla 22-1. Cuotas que se establecerán en las impresoras

Impresora	Precio por página	Precio por trabajo
LaserColor	0.09	0
LaserBN	0,03	0
Plotter	0.5	1
Sublimacion	0.65	0.75
Multifuncion	0.025	0
InyeccionColor	0.07	0
InyeccionBN	0.025	0

La orden que se va a utilizar para el establecimiento de los precios de la tabla anterior en las impresoras es: **pkprinters**. El siguiente ejemplo le mostrará como hacerlo:

> **Nota:** Si ejecuta la orden **pkprinters --help**, obtendrá un listado con las opciones que acepta **pkprinters** así como una serie de ejemplos de uso.

Ejemplo 22-1. Estableciendo los precios en las impresoras con pkprinters

```
$ /usr/bin/pkprinters --add --charge 0.09 LaserColor
$ /usr/bin/pkprinters --add --charge 0.03 LaserBN
$ /usr/bin/pkprinters --add --charge 0.5,1 Plotter
$ /usr/bin/pkprinters --add --charge 0.65,0.75 Sublimacion
```

```
$ /usr/bin/pkprinters --add --charge 0.025 Multifuncion InyeccionBN
$ /usr/bin/pkprinters --add --charge 0.07 InyeccionColor
$ /usr/bin/pkprinters --list
LaserColor [] (0.0 + #*0.09)
LaserBN [] (0.0 + #*0.03)
Plotter [] (1.0 + #*0.5)
Sublimacion [] (0.75 + #*0.65)
Multifuncion [] (0.0 + #*0.025)
InyeccionBN [] (0.0 + #*0.025)
InyeccionColor [] (0.0 + #*0.07)
$ /usr/bin/repykota
Informe para la cuota user en la impresora LaserColor ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.090
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
                                                Real : Desconocido

Informe para la cuota user en la impresora LaserBN ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.030
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
                                                Real : Desconocido

Informe para la cuota user en la impresora Plotter ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 1.000
Precio por página: 0.500
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
                                                Real : Desconocido

Informe para la cuota user en la impresora Sublimacion ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.750
Precio por página: 0.650
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
                                                Real : Desconocido

Informe para la cuota user en la impresora Multifuncion ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.025
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
                                                Real : Desconocido

Informe para la cuota user en la impresora InyeccionBN ()
Tiempo de gracia para páginas: 7 día(s)
```

```
Precio por trabajo: 0.000
Precio por página: 0.025
Usuario         usado   blando  duro    saldo gracia          total     pagado
------------------------------------------------------------------------------
                                                  Real : Desconocido

Informe para la cuota user en la impresora InyeccionColor ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.070
Usuario         usado   blando  duro    saldo gracia          total     pagado
------------------------------------------------------------------------------
                                                  Real : Desconocido
```

Con esto se completaría el establecimiento de los precios por impresora; en la siguiente sección se verá como permitir a los usuarios hacer uso del sistema de impresión.

Gestionando los usuarios

Los usuarios pueden tener dos tipos de cuota de impresión: por páginas impresas o por precio. De esta forma se puede establecer un límite de páginas impresas para un período de tiempo concreto, pasado el cual, se resetea dicho valor a cero.

La otra forma de gestión de las cuotas, es estableciendo un saldo por usuario, que tras agotarse, no se podrá volver a imprimir hasta que no se recargue.

En los siguientes ejemplos se verá la forma de establecer ambas cuotas de impresión, para ello se hará uso de la orden **edpykota**:

> **Nota:** Si ejecuta la orden **edpykota --help**, obtendrá un listado con las opciones que acepta **edpykota** así como una serie de ejemplos de uso.

Ejemplo 22-2. Estableciendo una cuota de impresión a un usuario

En este ejemplo se le asignará un límite de 10 páginas impresas para el usuario *printquota*.

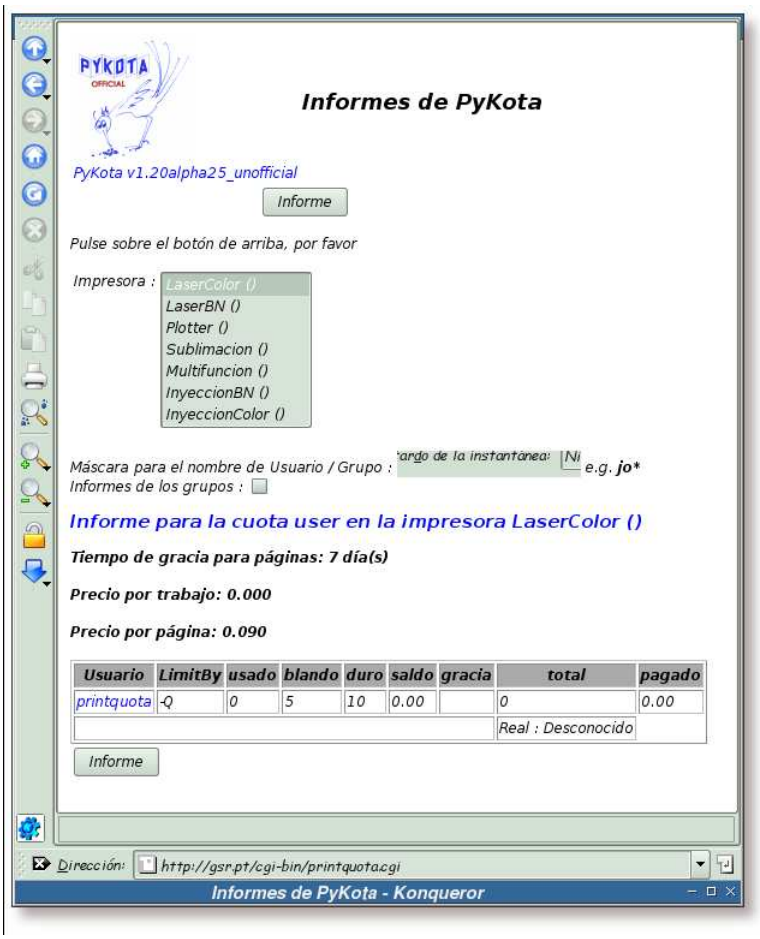
Como el usuario *printquota* no existe en el sistema, el comando **edpykota** lo añadirá automáticamente.

```
# /usr/bin/edpykota --add -P LaserColor -S 5 -H 10 printquota
WARN: No se ha podido encontrar una entrada objectClass posixAccount existente con \
uid=printquota para anexionar el objectClass pykotaAccount. A new entry will be created instead.
# /usr/bin/repykota --printer LaserColor
Informe para la cuota user en la impresora LaserColor ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.090
Usuario         usado   blando  duro    saldo gracia          total     pagado
------------------------------------------------------------------------------
printquot -Q       0       5      10       0.00                  0       0.00
```

```
                                                    Real : Desconocido
```

Pykota provee un CGI que muestra gráficamente el estado de las cuotas. Para acceder a este programa, teclee la URL del servidor web donde ha instalado PyKota seguido de la ubicación del citado CGI. En el sistema que se ha empleado para realizar esta documentación, el CGI se encuentra en la siguiente URL: http://gsr.pt/cgi-bin/printquota.cgi

Figura 22-1. Informe de la impresora *LaserColor*



Información sobre la impresora *LaserColor* generado por el CGI que provee PyKota.

Ejemplo 22-3. Asignando un saldo de impresión a un usuario

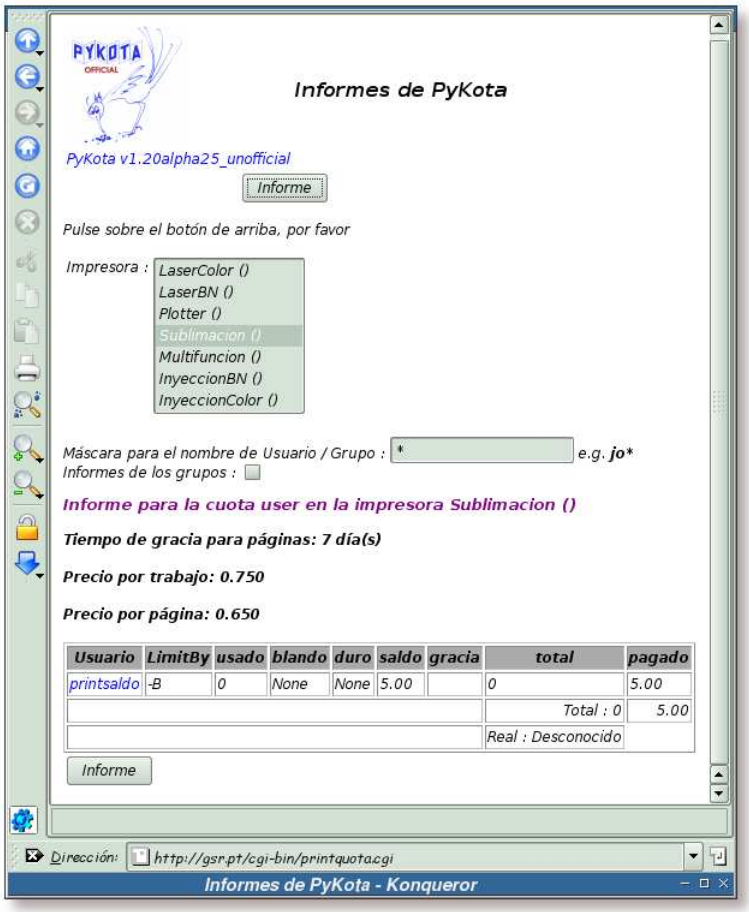
En este ejemplo se le asignará un saldo de 5 euros al usuario *printsaldo*.

Como el usuario *printsaldo* no existe en el sistema, el comando **edpykota** lo añadirá automáticamente.

```
# /usr/bin/edpykota --add -P Sublimacion --limitby balance --balance 5 printsaldo
WARN: No se ha podido encontrar una entrada objectClass posixAccount existente con uid=printsaldo p
anexionar el objectClass pykotaAccount. A new entry will be created instead.
```

```
# /usr/bin/repykota --printer Sublimacion
Informe para la cuota user en la impresora Sublimacion ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.750
Precio por página: 0.650
Usuario         usado   blando  duro    saldo gracia          total     pagado
------------------------------------------------------------------------------
printsald -B       0    None    None       5.00                   0       5.00
                                                    Total :       0       5.00
                                                     Real : Desconocido
```

Figura 22-2. Informe de la impresora *Sublimacion*



Información sobre la impresora *Sublimacion* generado por el CGI que provee PyKota.

Con esto finalizaría la asignación de cuotas de impresión a los usuarios. En la siguiente sección se verá el funcionamiento de dichas cuotas.

Capítulo 23. Probando el sistema de cuotas

Introducción

Este capítulo pondrá a prueba el sistema de cuotas de impresión, para ver si funciona como debe. Se realizarán pruebas sobre los dos tipos de cuotas empleados.

Usuario *printquota*

En las siguientes secciones se van a mostrar tres ejemplos a la hora de imprimir un determinado documento:

- Se alcanza el límite blando de la cuota de impresión, la sección de nombre *Alcanzando el límite blando.*
- Se intenta imprimir un documento mayor que la cuota disponible, la sección de nombre *Impresión de un documento mayor a la cuota disponible.*
- Se alcanza el límite duro de la cuota de impresión, la sección de nombre *Alcanzando el límite duro.*

Alcanzando el límite blando

Recuerde que este usuario tiene un límite de impresión de 10 páginas (vea el Ejemplo 22-2 para más detalles). Se va a imprimir un documento de 5 páginas y se va a comprobar que ocurre en el sistema de cuotas:

Figura 23-1. Impresión de un documento de 5 páginas I

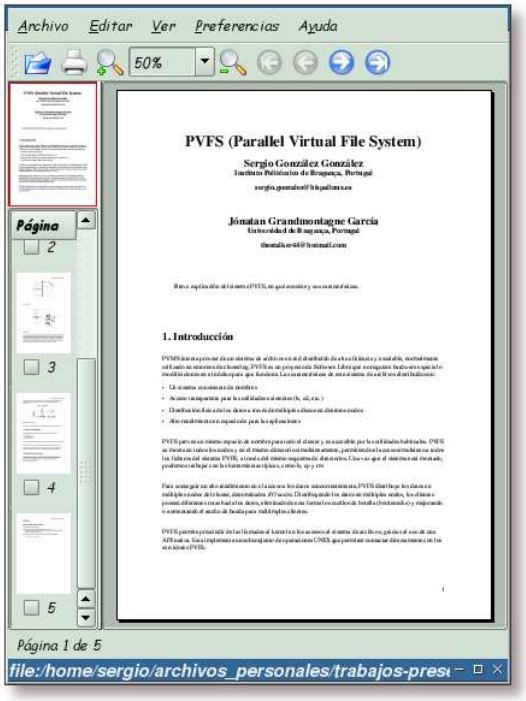


Figura 23-2. Impresión de un documento de 5 páginas II

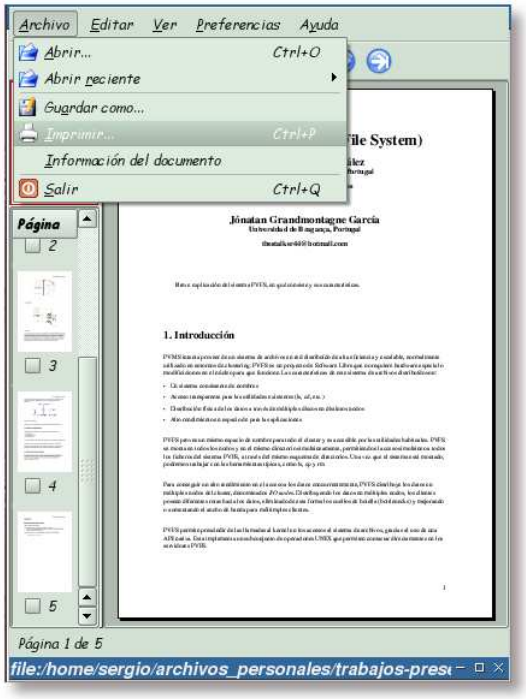


Figura 23-3. Impresión de un documento de 5 páginas III

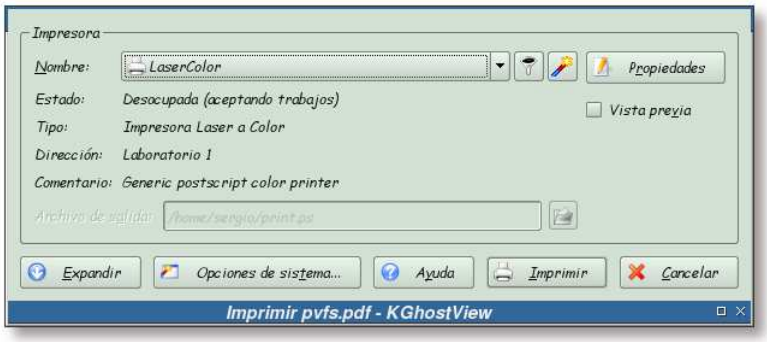


Figura 23-4. Impresión de un documento de 5 páginas IV

Tras la impresión de este documento, aparece un nuevo archivo PDF bajo el directorio `cups-pdf` del home del usuario *printquota* con un nombre similar a: `job_2-untitled_document.pdf`.

Si ahora se revisa el estado de la cuota de este usuario, se obtendrá algo similar a:

Ejemplo 23-1. Revisando la cuota de impresión del usuario *printquota* I

```
# /usr/bin/repykota --printer LaserColor
Informe para la cuota user en la impresora LaserColor ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.090
Usuario         usado   blando  duro    saldo gracia          total     pagado
------------------------------------------------------------------------------
printquot +Q       5       5      10      -0.45 2004-10-21        5       0.00
                                                  Total :       5       0.00
                                                   Real :       0
```

Se puede observar que ha consumido 5 páginas de su cuota de impresión. PyKota también informa del coste de la impresión (-0.45), el valor negativo indica que el usuario no ha pagado por esta impresión. A continuación se va a imprimir una página más, para rebasar el límite suave de la cuota, y ver qué ocurre.

Tras realizar esta primera impresión, el usuario *printquota* recibirá un correo electrónico, informándole de que ha alcanzado su límite blando de impresión. Así mismo, el administrador del sistema de impresión, recibirá otro correo, informándole de que el usuario *printquota* tiene su cuota de impresión baja (recuerde que este comportamiento se ha definido en la la sección de nombre *Envío de notificaciones* en Capítulo 20). A continuación puede ver los correos enviados:

Ejemplo 23-2. Correo de aviso enviado al usuario *printquota* - límite suave sobrepasado -

```
From: root@localhost
Subject: Cuota de Impresión Baja
To: printquota@gsr.pt

Ha alcanzado su límite blando en la cuota de impresión.
Esto significa que podrá seguir imprimiendo algún tiempo,
pero debería contactar con su administrador para comprar
más cuota de impresión.

Entre en contacto con su administrador de sistema, por favor :
```

```
        Sergio González González - <root@localhost>
```

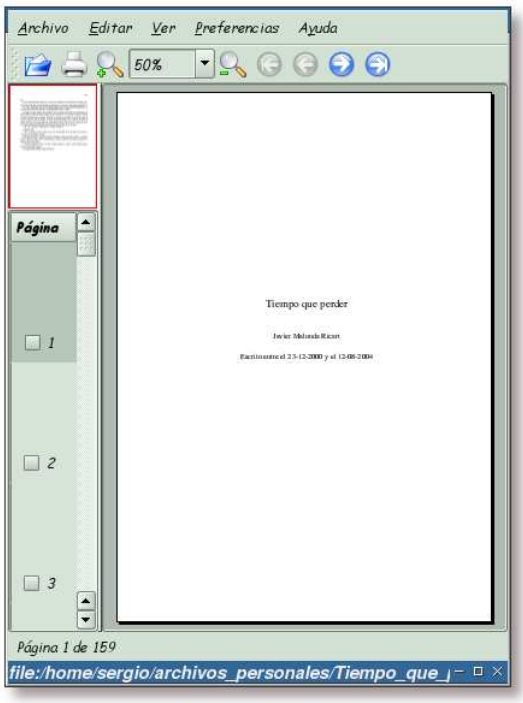
Ejemplo 23-3. Correo de aviso enviado al administrador - cuota de impresión baja -

```
From: root@localhost
Subject: Cuota de impresión
To: root@localhost

Cuota de impresión baja para el usuario printquota en la impresora LaserColor
```

Impresión de un documento mayor a la cuota disponible

En esta sección se ha intentado imprimir un documento de dimensiones superiores a la cuota del usuario *printquota*:

Figura 23-5. Impresión de un documento que supera la cuota disponible



Intento de impresión de un documento que superaría la cuota de impresión del usuario.

Debido a que se ha configurado PyKota en modo *strict* (vea la
la sección de nombre *¿Se permite a los usuarios sobrepasar la cuota de impresión?* en Capítulo 20), el

documento que se ha tratado de imprimir, no se imprimirá. Como resultado a esta acción, el usuario *printquota* y el administrador del sistema de impresión recibirán los siguientes correos:

Ejemplo 23-4. Correo de aviso enviado al usuario *printquota* - límite duro sobrepasado -

```
From: root@localhost
Subject: Cuota de Impresión Excedida
To: printquota@gsr.pt

Ha alcanzado su límite duro en la cuota de impresión.
Esto significa que no podrá volver a imprimir.
Contacte con su administrador en <root@gsr.pt> tan
pronto como le sea posible para solucionar el
problema.

Entre en contacto con su administrador de sistema, por favor :

        Sergio González González - <root@localhost>
```

Ejemplo 23-5. Correo de aviso enviado al administrador - cuota de impresión excedida -

```
From: root@localhost
Subject: Cuota de impresión
To: root@localhost

Cuota de impresión excedida para el usuario printquota en la impresora LaserColor
```

> **Importante:** Si se hubiese utilizado el modo *laxist*, el documento se habría impreso en su totalidad, obteniéndose como resultado una cuota negativa para el usuario en cuestión.

El aviso recibido, tanto por el usuario *printquota* como por el administrador del sistema de impresión, no es del todo cierto. Es cierto que se ha alcanzado el límite duro de la cuota de impresión con el trabajo enviado a la cola de impresión, pero debido a que este sobrepasaba el límite de la cuota de impresión, el trabajo no se ha impreso. Como resultado, la cuota del usuario *printquota* permanece igual que antes de haber enviado el trabajo a la cola de impresión:

Ejemplo 23-6. Revisando la cuota de impresión del usuario *printquota*

```
# /usr/bin/repykota --printer LaserColor
Informe para la cuota user en la impresora LaserColor ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.090
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
printquot +Q       5       5      10      -0.45 2004-10-21        5       0.00
                                                  Total :         5       0.00
                                                   Real :         0
```

Alcanzando el límite duro

Ahora se van a imprimir 4 páginas más, acabando de esta forma la cuota de impresión.

> **Nota:** Si se intentan imprimir 5 páginas, alcanzando de esta forma el límite duro, ocurrirá lo mismo que el ejemplo mostrado en la
> la sección de nombre *Impresión de un documento mayor a la cuota disponible*.

Ejemplo 23-7. Revisando la cuota de impresión del usuario *printquota*

```
# /usr/bin/repykota --printer LaserColor
Informe para la cuota user en la impresora LaserColor ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.090
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
printquot +Q       9       5      10      -0.81 2004-10-21        9       0.00
                                                  Total :       9       0.00
                                                   Real :       5
```

Los correos de notificación que se han recibido en esta ocasión son los siguientes:

Ejemplo 23-8. Correo de aviso enviado al usuario *printquota* - límite blando sobrepasado -

```
From: root@localhost
Subject: Cuota de Impresión Baja
To: printquota@gsr.pt

Ha alcanzado su límite blando en la cuota de impresión.
Esto significa que podrá seguir imprimiendo algún tiempo,
pero debería contactar con su administrador para comprar
más cuota de impresión.

Entre en contacto con su administrador de sistema, por favor :

        Sergio González González - <root@localhost>
```

Ejemplo 23-9. Correo de aviso enviado al administrador - cuota excedida -

```
From: root@localhost
Subject: Cuota de impresión
To: root@localhost

Cuota de impresión excedida para el usuario sergio en la impresora LaserColor
```

A partir de este momento, el usuario *printquota* no podrá volver a imprimir, hasta que no obtenga más cuota de impresión.

Nota: El comportamiento del sistema de impresión con la opción *laxist* hubiese sido ligeramente diferente. Por lo tanto, la elección de uno u otro comportamiento ha de elegirse en función de sus preferencias.

Reinicio de la cuota de impresión

Supongamos ahora que el sistema reinicia las cuotas de los usuarios cada cierto período de tiempo:

Ejemplo 23-10. Reinicio de la cuota de impresión para el usuario *printquota*

```
# /usr/bin/edpykota --reset printquota
```

A partir de ese momento, el usuario *printquote* dispone de nuevo de una cuota de impresión de 10 páginas:

Ejemplo 23-11. Información sobre la cuota del usuario *printquota*, tras su reinicio I

```
# /usr/bin/repykota --printer LaserColor
Informe para la cuota user en la impresora LaserColor ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.090
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
printquot -Q       0       5      10      -0.81 2004-10-21        9       0.00
                                                  Total :       9       0.00
                                                   Real :       9
```

Si se realiza en este momento una nueva impresión, el informe para el usuario *printquota* sería:

Ejemplo 23-12. Información sobre la cuota del usuario *printquota*, tras su reinicio II

```
# /usr/bin/repykota --printer LaserColor
Informe para la cuota user en la impresora LaserColor ()
Tiempo de gracia para páginas: 7 día(s)
Precio por trabajo: 0.000
Precio por página: 0.090
Usuario         usado   blando  duro    saldo gracia          total     pagado
--------------------------------------------------------------------------------
printquot +Q       5       5      10      -1.26 2004-10-21       14       0.00
                                                  Total :       14       0.00
                                                   Real :        9
```

Como se ha podido comprobar, el sistema de cuotas funciona de la manera esperada. Con esto concluirían las pruebas sobre el sistema de cuotas de impresión.

usuario *printsaldo*

El usuario *printsaldo* posee una cuota de impresión basada en saldo; su comportamiento es similar al mostrado en la la sección de nombre *Usuario printquota,* por lo que se deja como trabajo para el lector las pruebas con este tipo de cuotas.

Sugerencia: Imagínese que el usuario *printsaldo* desea imprimir el documento que está leyendo, pero no tiene ni idea de lo que puede costar su impresión. Por este motivo, ha decidido consultar, antes de imprimir, el precio de impresión en cada una de las impresoras disponibles en el sistema. El resultado ha sido el siguiente:

Ejemplo 23-13. Coste de impresión de un documento

```
$ /usr/bin/pykotme ldap+samba+cups+pykota.ps
Tamaño del trabajo : 759 página(s)
Coste en la impresora LaserColor : 68.31
Coste en la impresora LaserBN : 22.77
Coste en la impresora Plotter : 380.50
Coste en la impresora Sublimacion : 494.10
Coste en la impresora Multifuncion : 18.98
Coste en la impresora InyeccionBN : 18.98
Coste en la impresora InyeccionColor : 53.13
```

V. Misceláneo

Apéndice A. Creación y configuración de un usuario de sólo lectura para el directorio LDAP

Introducción

Este apéndice tiene por objetivo la creación y configuración de un usuario que tenga permisos de lectura en todo el directorio LDAP, pero no de escritura.

El usuario que se cree, no podrá acceder a las claves de otros usuarios, únicamente a la suya

Este usuario se hace necesario cuando el acceso al directorio LDAP se limita a usuarios autentificados (como es el caso de esta documentación).

Creación

Se supone que se posee un archivo denominado `readadmin.ldif`, con el siguiente contenido:

```
# Entry: cn=readadmin,dc=gsr,dc=pt
dn:cn=readadmin,dc=gsr,dc=pt
cn: readadmin
objectClass: simpleSecurityObject
objectClass: organizationalRole
userPassword: {crypt}y1pYJeZPC49BY
description: LDAP administrator (read only admin)
```

El ejemplo siguiente muestra como añadir el usuario *readadmin* al directorio LDAP:

Ejemplo A-1. Creación del usuario *readadmin*

```
$ /usr/bin/ldapadd -x -ZZ -D "cn=admin,dc=gsr,dc=pt" -W -f readadmin.ldif
Enter LDAP Password: [Clave]
adding new entry "cn=readadmin,dc=gsr,dc=pt"
```

Configuración

Una vez creado el usuario *readadmin*, se han de configurar los permisos que tendrá dentro del directorio LDAP. Esta operación se realiza en el archivo `/etc/ldap/slapd.conf`.

Debido a que el proceso de configuración de OpenLDAP se extiende por toda la documentación, en este apéndice se indicará únicamente la línea que se añadirá a las distintas ACLs a lo largo de la documentación:

```
by dn="cn=readadmin,dc=gsr,dc=pt" read
```

Nota: En el Apéndice Q tiene un archivo completo de configuración de OpenLDAP.

Apéndice B. Demonio de caché para el servicio de nombres: nscd

Introducción

Este demonio evita, en los equipos donde se encuentra instalado, que las órdenes del tipo **/bin/ls -l /home** constantemente consulten al servidor LDAP con cada ejecución. nscd mantiene una caché con información sobre los datos de los usuarios, que refresca cada cierto tiempo, de forma que las estaciones de trabajo la utilizarán en lugar de consultar al servidor LDAP.

Las siguientes secciones comprenderán el proceso de instalación y configuración de este demonio.

Instalación

La instalación es muy sencilla, como se verá a continuación:

Ejemplo B-1. Instalación de nscd

```
# /usr/bin/apt-get install nscd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  nscd
0 actualizados, 1 se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 0B/90,4kB de archivos.
Se utilizarán 217kB de espacio de disco adicional después de desempaquetar.
(Leyendo la base de datos ...
273953 ficheros y directorios instalados actualmente.)
Desempaquetando nscd (de .../nscd_2.3.2.ds1-16_i386.deb) ...
Configurando nscd (2.3.2.ds1-16) ...
Starting Name Service Cache Daemon: nscd.
```

Para ver la información acerca del paquete, teclee:

Ejemplo B-2. Instalación de nscd

```
$ /usr/bin/apt-cache show nscd
Package: nscd
Priority: optional
Section: admin
Installed-Size: 212
Maintainer: GNU Libc Maintainers <debian-glibc@lists.debian.org>
Architecture: i386
Source: glibc
Version: 2.3.2.ds1-16
```

```
Replaces: libc6 (<< 2.1-4)
Depends: libc6 (>= 2.3.2.ds1-16)
Filename: pool/main/g/glibc/nscd_2.3.2.ds1-16_i386.deb
Size: 90436
MD5sum: 4830a171d3ef40bef18315bcfb47be3a
Description: GNU C Library: Name Service Cache Daemon
 A daemon which handles passwd, group and host lookups
 for running programs and caches the results for the next
 query. You should install this package only if you use
 slow Services like LDAP, NIS or NIS+
```

Configuración

nscd se configura a través del archivo `/etc/nscd.conf` (puede encontrar un ejemplo del mismo en el Apéndice AA). Los únicos parámetros que se tocarán de ese archivo de configuración son los siguientes:

```
logfile                 /var/log/nscd.log
server-user             nscd
```

El primer parámetro especifica el archivo de log que va a emplear el demonio nscd y el segundo el usuario con el que se ejecutará en el sistema. Como el usuario *nscd* no existe en la máquina, se crea:

Ejemplo B-3. Creación del usuario *nscd*

```
# /usr/sbin/addgroup --system nscd

Añadiendo el grupo nscd (135)...
Hecho.
# /usr/sbin/adduser --system --no-create-home --shell /bin/false \
--ingroup nscd --disabled-password --disabled-login nscd

Añadiendo usuario del sistema nscd...
No se crea el directorio home.
```

Antes de arrancar el demonio nscd, se modifican el propietario y grupo del archivo de log y, si es necesario, el del archivo `/var/run/nscd.pid`.

Ejemplo B-4. Cambio del propietario y grupo de algunos archivos relativos a *nscd*

```
# /bin/chown nscd\:nscd /var/log/nscd.log /var/run/nscd.pid
```

Ahora ya se puede arrancar el demonio:

Ejemplo B-5. Arranque del demonio *nscd*

```
# /etc/init.d/nscd start
Starting Name Service Cache Daemon: nscd.
```

Apéndice C. Ejecución de Samba desde (x)inetd

Introducción

Para poder ejecutar Samba desde el superservidor (x)inetd, hay que indicarlo en el archivo `/etc/defaul/samba` (en el Apéndice AB tiene un ejemplo de este archivo de configuración). La forma de hacerlo sería asignando el valor "inetd" a la variable *RUN_MODE* (esta variable acepta los valores "daemons" e "inetd").

Una vez hecho esto, sólo quedaría configurar el superservidor para que gestione las conexiones de Samba. En las siguientes secciones se verá como hacerlo para los superservidores inetd y xinetd.

Superservidor inetd

En el Ejemplo 7-4 se puede ver como en la instalación de Samba se añade la siguiente línea al archivo de configuración del superservidor inetd:

```
#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/smbd
```

Como se puede ver al comienzo de la línea, esta se encuentra desactivada (#<off># ...) por defecto; si se quieren gestionar las conexiones de Samba desde inetd, se ha de activar. En el Ejemplo C-1 se ve como hacerlo:

Ejemplo C-1. Habilitando el servicio "netbios-ssn" en el superservidor inetd

```
# /usr/sbin/update-inetd --verbose --enable netbios-ssn
Processing /etc/inetd.conf
Processing service 'netbios-ssn' ... enabled
```

Ahora sólo queda hacer que el superservidor inetd lea de nuevo su configuración, para ello se ha de teclear (suponiendo que el superservidor ya se esté ejecutando):

Ejemplo C-2. Haciendo que el superservidor inetd relea su configuración

```
# /usr/bin/killall --verbose -HUP inetd
Killed inetd(3005) with signal 1
```

Si todo ha ido bien, en este punto el superservidor inetd gestionaría las conexiones de Samba.

Superservidor xinetd

Para ejecutar Samba desde el superservidor xinetd se ha de crear la configuración para este servicio en dicho superservidor. Esto se realiza creando un nuevo archivo denominado `samba` bajo el directorio `/etc/xinetd.d`, cuyo contenido sea:

Ejemplo C-3. Contenido del archivo `/etc/xinetd.d/samba`

```
service netbios-ssn
{
        disable         = no ❶
        socket_type     = stream
        protocol        = tcp
        wait            = no
        user            = root
        server          = /usr/sbin/smbd
}
```

❶ Variable que controla si el servicio está o no activo. Si su valor es igual a “yes”, el servicio estará deshabilitado, si es “no”, estará habilitado.

Ahora haga que el superservidor xinetd relea su configuración de la siguiente manera:

Ejemplo C-4. Releyendo la configuración de xinetd

```
# /etc/init.d/xinetd reload
Reloading internet superserver configuration: xinetd.
```

Una vez ejecutada la orden del Ejemplo C-4, el superservidor xinetd pasaría a gestionar las conexiones a Samba.

Apéndice D. Opciones del kernel Linux para Samba

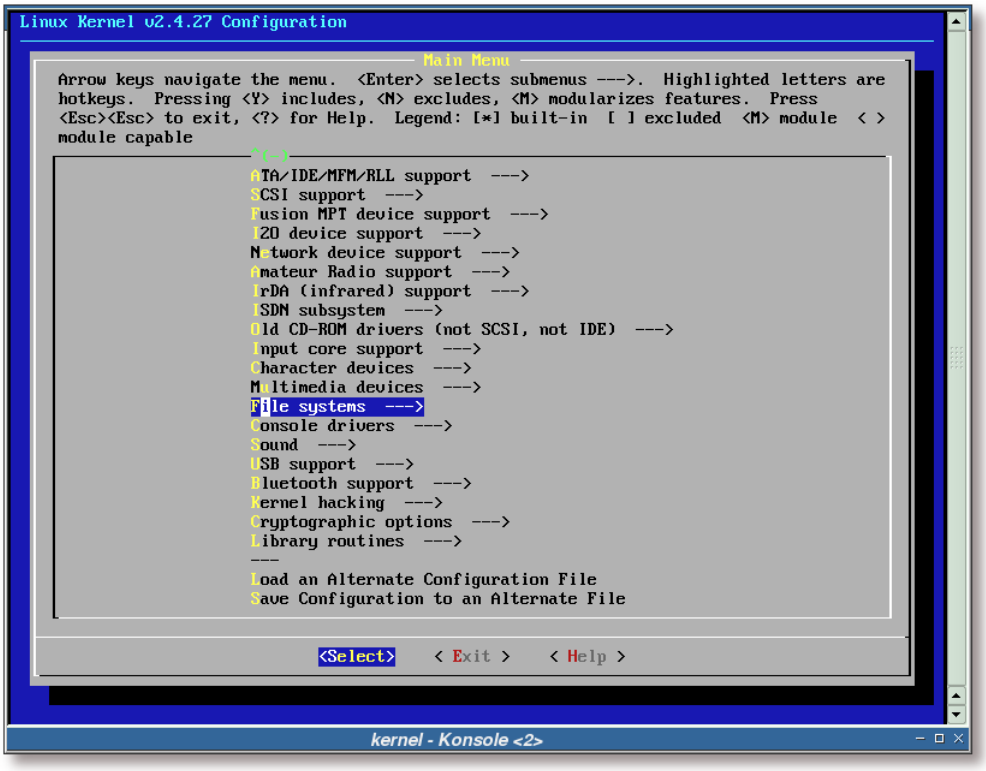
Para poder montar los sistemas de archivos que sirve Samba, es necesario que el núcleo Linux del ordenador donde se pretenden montar, tenga soporte para dicho sistema de archivos. Las opciones necesarias para conseguir este soporte en el núcleo Linux se verán a continuación (tanto para la versión 2.4.27 como para la 2.6.8.1, que son la versiones con las que se ha trabajado para realizar este documento):

Kernel 2.4.*

Tecleando **make menuconfig** en el directorio raíz de las fuentes del núcleo, veamos como llegar a las opciones necesarias:

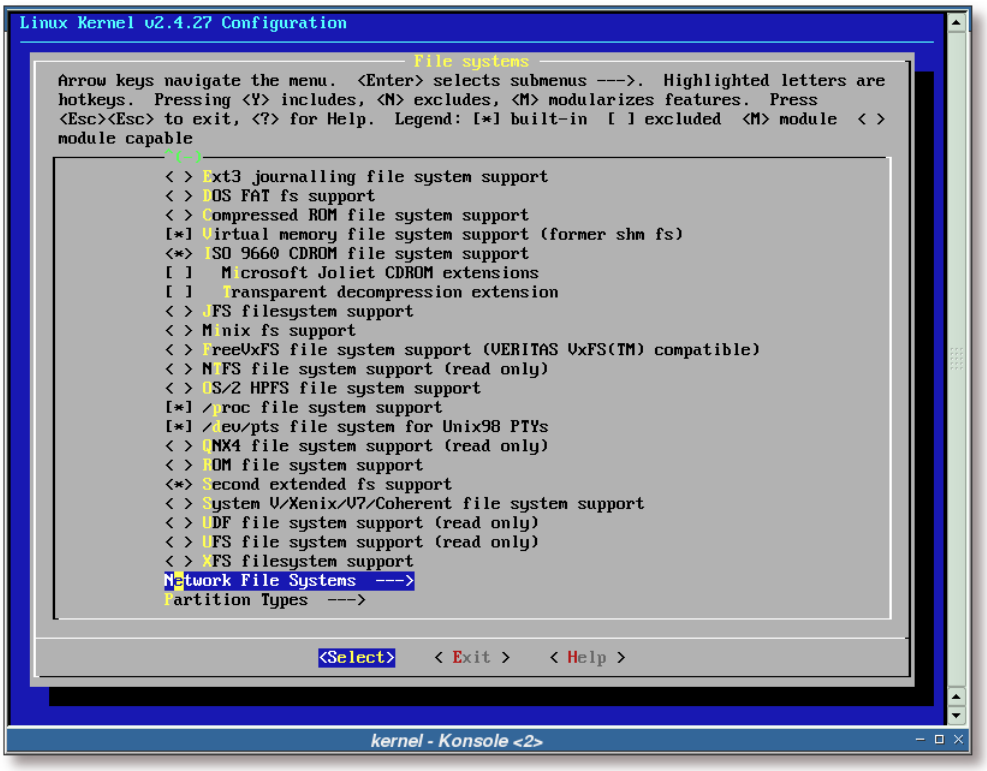
Nota: En esta documentación se ha empleado la versión 2.4.27 del núcleo Linux.

Figura D-1. Sistema de archivos



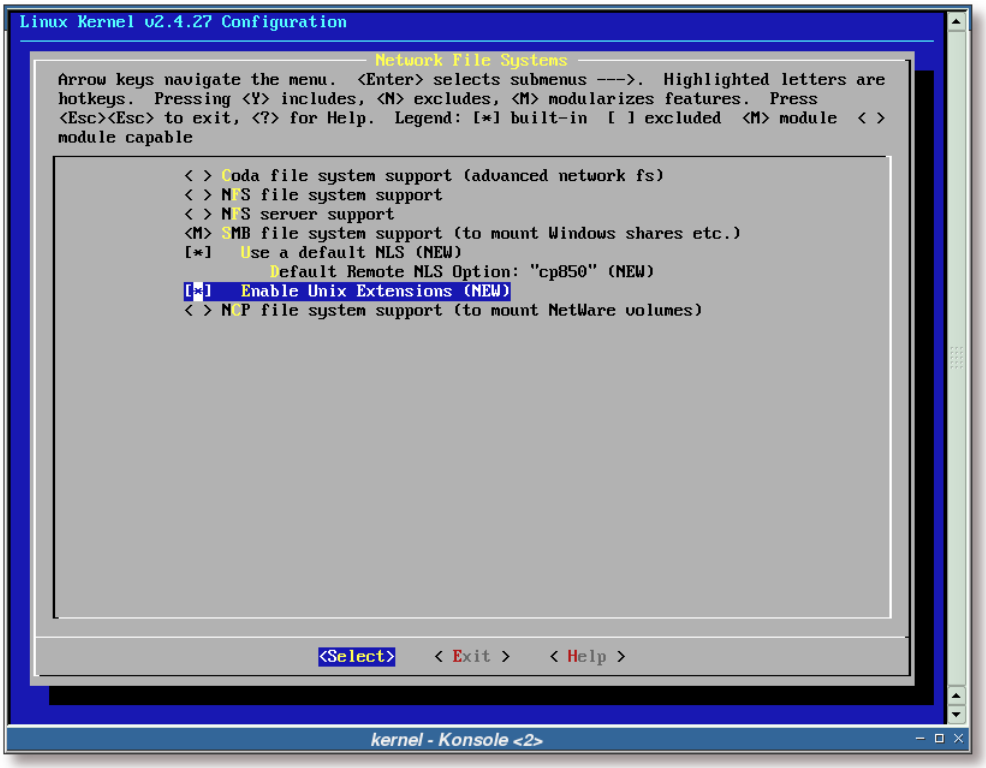
Entramos en la selección de los distintos sistemas de archivos soportados por el núcleo.

Figura D-2. Sistema de archivos en red



Seleccionamos la opción sistema de archivos en red.

Figura D-3. Opciones relativas Samba



Soporte para el protocolo SMB y CIFS.

Las opciones seleccionadas en la Figura D-3 se pueden resumir en:

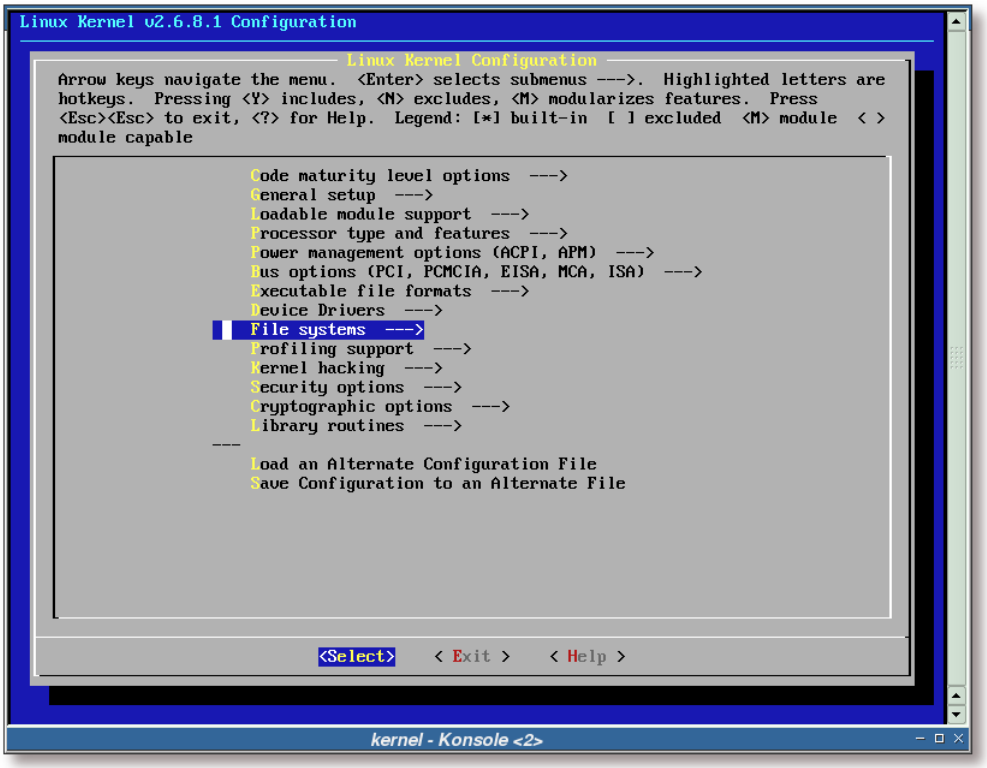
```
CONFIG_SMB_FS=m
CONFIG_SMB_NLS_DEFAULT=y
CONFIG_SMB_NLS_REMOTE="cp850"
CONFIG_SMB_UNIX=y
```

Kernel 2.6.*

Tecleando **make menuconfig** en el directorio raíz de las fuentes del núcleo, veamos como llegar a las opciones necesarias:

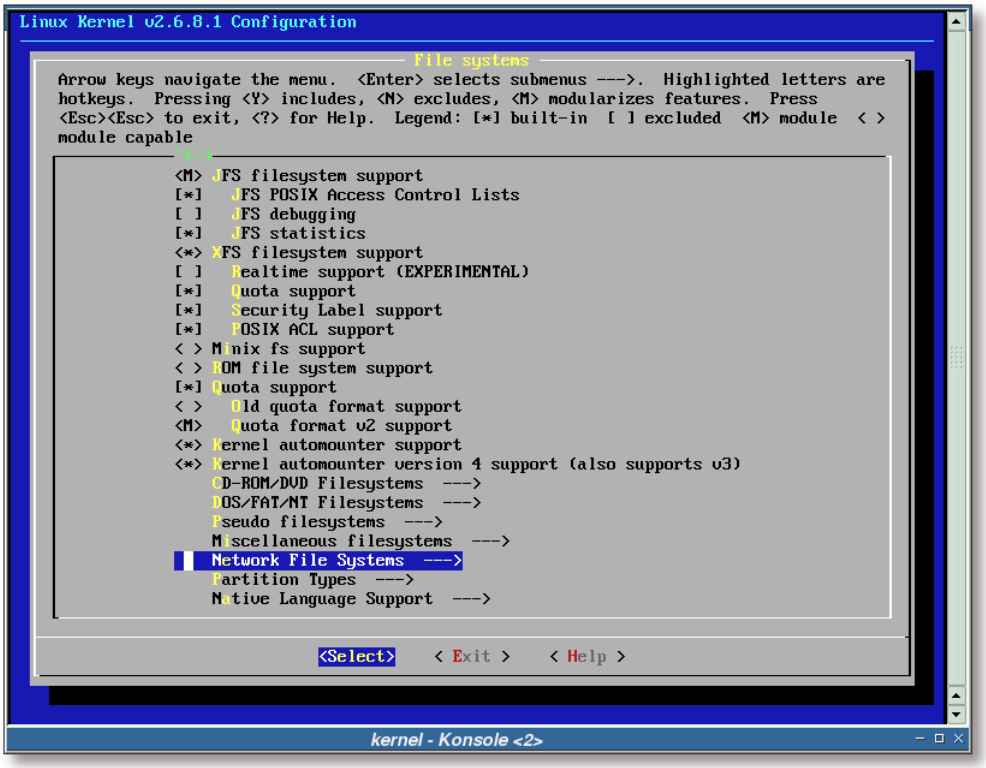
> **Nota:** En esta documentación se ha empleado la versión 2.6.8.1 del núcleo Linux.

Figura D-4. Sistema de archivos



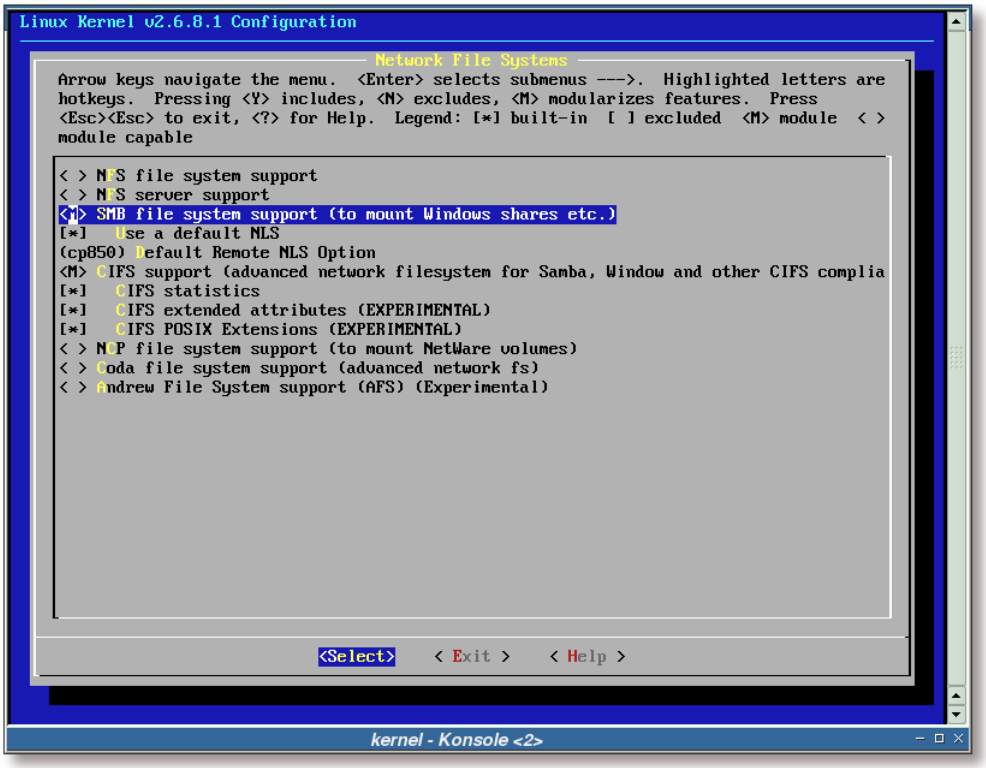
Entramos en la selección de los distintos sistemas de archivos soportados por el núcleo.

Figura D-5. Sistema de archivos en red



Seleccionamos la opción sistema de archivos en red.

Figura D-6. Opciones relativas Samba



Soporte para el protocolo SMB y CIFS.

Las opciones seleccionadas en la Figura D-6 se pueden resumir en:

```
CONFIG_SMB_FS=m
CONFIG_SMB_NLS_DEFAULT=y
CONFIG_SMB_NLS_REMOTE="cp850"
CONFIG_CIFS=m
CONFIG_CIFS_STATS=y
CONFIG_CIFS_XATTR=y
CONFIG_CIFS_POSIX=y
```

Apéndice E. Instalación y configuración de SWAT

Introducción

SWAT es una herramienta de configuración de Samba vía web. En las siguientes secciones se verán los pasos para ponerla en funcionamiento.

Instalación de SWAT

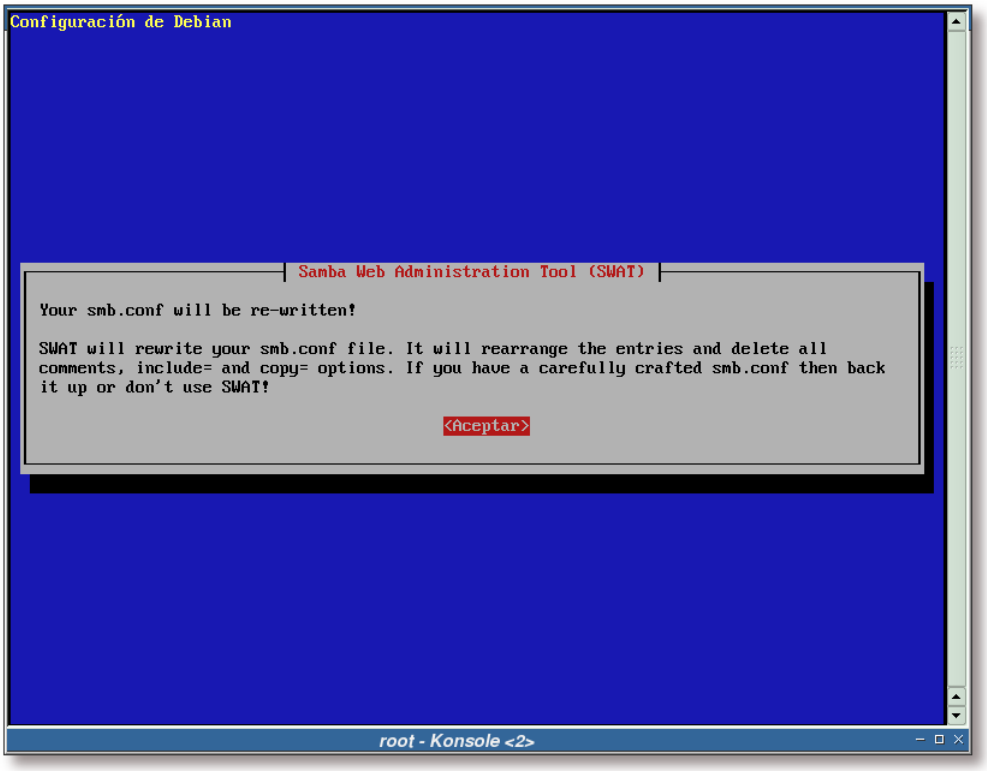
En el siguiente ejemplo se muestra la información relativa al paquete swat y la forma de instalarlo:

Ejemplo E-1. Instalación de SWAT (primera parte)

```
$ /usr/bin/apt-cache show swat
Package: swat
Priority: optional
Section: net
Installed-Size: 8968
Maintainer: Eloy A. Paris <peloy@debian.org>
Architecture: i386
Source: samba
Version: 3.0.7-1
Depends: debconf, samba (= 3.0.7-1), libc6 (>= 2.3.2.ds1-4),
libcomerr2 (>= 1.33-3), libcupsys2-gnutls10 (>= 1.1.20final-1),
libkrb53 (>= 1.3.2), libldap2 (>= 2.1.17-1), libpam0g (>= 0.76),
libpopt0 (>= 1.7)
Recommends: samba-doc
Filename: pool/main/s/samba/swat_3.0.7-1_i386.deb
Size: 3964890
MD5sum: d84a020935c85831d8d81321b7391ed4
Description: Samba Web Administration Tool
 The Samba software suite is a collection of programs that
 implements the SMB protocol for unix systems, allowing you to serve
 files and printers to Windows, NT, OS/2 and DOS clients. This protocol
 is sometimes also referred to as the LanManager or NetBIOS protocol.
 .
 This package contains the components of the Samba suite that are needed
 for Web administration of the Samba server.
 .
 Note: if you want to use the on-line documentation that is accesible
 through the Swat front-end you must install the samba-doc package.
Task: file-server, print-server


#/usr/bin/apt-get install swat
```

```
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  swat
0 actualizados, 1 se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 0B/3965kB de archivos.
Se utilizarán 9183kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...
```

Figura E-1. Aviso de sobreescritura del archivo `/etc/samba/smb.conf`



El programa SWAT sobreescribe el archivo de configuración de Samba, eliminado los comentarios, entre otras cosas. Esta pantalla avisa de este hecho, y recomienda no utilizar SWAT en aquellos casos en los que se tenga muy personalizado el archivo de configuración de Samba.

Ejemplo E-2. Instalación de SWAT (segunda parte)

```
Seleccionando el paquete swat previamente no seleccionado.
(Leyendo la base de datos ...
133905 ficheros y directorios instalados actualmente.)
Desempaquetando swat (de .../archives/swat_3.0.7-1_i386.deb) ...
Configurando swat (3.0.7-1) ...
--------- IMPORTANT INFORMATION FOR XINETD USERS ----------
```

```
The following line will be added to your /etc/inetd.conf file:

#<off># swat\t\tstream\ttcp\tnowait.400\troot\t/usr/sbin/tcpd\t/usr/sbin/swat

If you are indeed using xinetd, you will have to convert the
above into /etc/xinetd.conf format, and add it manually. See
/usr/share/doc/xinetd/README.Debian for more information.
------------------------------------------------------------


localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

Gestión de SWAT desde un superservidor (x)inetd

A continuación se verá la forma de configurar SWAT para que sea gestionado desde los superservidores inetd y xinetd:

Gestión de SWAT desde inetd

Tras la instalación de SWAT, se ha de activar en el archivo de configuración de inetd:

Ejemplo E-3. Activación de SWAT en inetd

```
# /usr/sbin/update-inetd --verbose --enable swat
Processing /etc/inetd.conf
Processing service ‘swat’ ... enabled
```

Ahora se hace que el superservidor inetd relea su configuración, quedando el servicio SWAT disponible en el sistema:

Ejemplo E-4. Haciendo que el superservidor inetd relea su configuración

```
# /usr/bin/killall --verbose -HUP inetd
Killed inetd(3005) with signal 1
```

Como se puede ver en el Ejemplo E-5, SWAT está a la espera de peticiones:

Ejemplo E-5. Mostrando las conexiones de SWAT

```
# /bin/netstat -puta | /bin/grep swat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:swat                  *:*                     LISTEN     1265/inetd
```

Gestión de SWAT desde xinetd

Para ejecutar SWAT desde el superservidor xinetd se ha de crear la configuración para este servicio en dicho superservidor. Esto se realiza creando un nuevo archivo denominado `swat` bajo el directorio `/etc/xinetd.d`, cuyo contenido sea:

Ejemplo E-6. Contenido del archivo `/etc/xinetd.d/swat`

```
service swat
{
        disable         = no ❶
        socket_type     = stream
        protocol        = tcp
        wait            = no
        user            = root
        server          = /usr/sbin/swat
#       server_args     = -a ❷
}
```

❶ Variable que controla si el servicio está o no activo. Si su valor es igual a “yes”, el servicio estará deshabilitado, si es “no”, estará habilitado.

❷ Esta línea, en caso de estar descomentada, está destinada al paso de parámetros para el servidor swat. La opción “-a” deshabilitaría la autentificación, permitiendo a cualquier persona modificar la configuración de Samba. ¡Tenga cuidado con su uso!

Ahora haga que el superservidor xinetd relea su configuración de la siguiente manera:

Ejemplo E-7. Releyendo la configuración de xinetd

```
# /etc/init.d/xinetd reload
Reloading internet superserver configuration: xinetd.
```

Una vez ejecutada la orden del Ejemplo E-7, el superservidor xinetd pasaría a gestionar las conexiones a Samba:

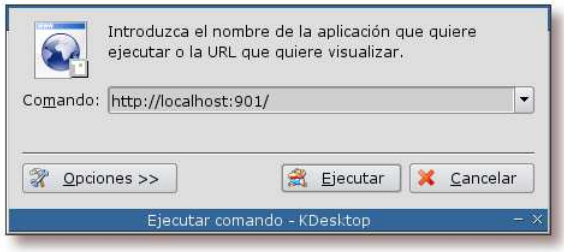
Ejemplo E-8. Mostrando las conexiones de SWAT

```
# /bin/netstat -puta | /bin/grep swat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:swat                  *:*                     LISTEN      4687/xinetd
```

Accediendo a SWAT

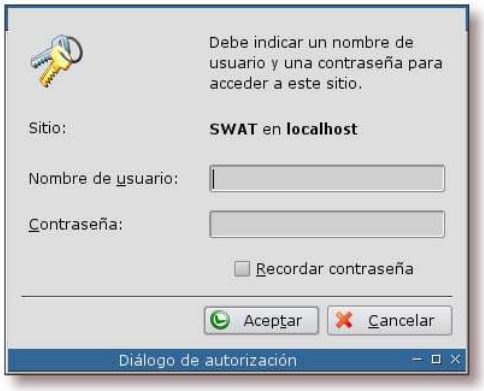
Para ejecutar SWAT, teclee en su navegador favorito la siguiente dirección: http://localhost:901/ y verá algo similar a:

Figura E-2. Acceso a SWAT



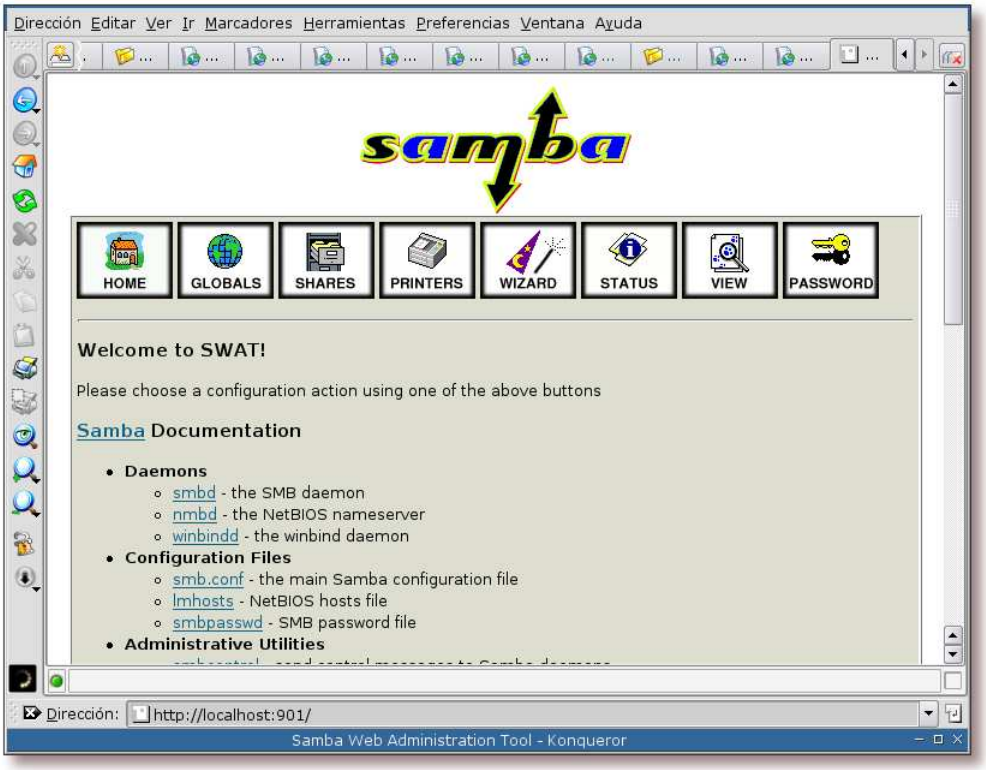
Ventana de ejecución de KDE, aparece tecleando: **Alt**+**F2**.

Figura E-3. Autentificación



Si no se ha utilizado el parámetro “-a” en el arranque de SWAT, será necesario autentificarse antes de poder entrar en la herramienta.

Figura E-4. Pantalla principal de SWAT



Pantalla principal de SWAT, desde aquí se puede acceder a todas las partes de la configuración de Samba.

Apéndice F. Instalación y configuración de *LAM* (LDAP Account Manager)

Instalación

LAM es un *frontend* web para la administración de usuarios para cuentas unix y Samba dentro de un directorio LDAP. Su descripción es la siguiente:

Ejemplo F-1. Descripción de LAM

```
$ /usr/bin/apt-cache show ldap-account-manager
Package: ldap-account-manager
Priority: extra
Section: web
Installed-Size: 2208
Maintainer: Roland Gruber <post@rolandgruber.de>
Architecture: all
Version: 0.4.6-2
Depends: php4 | php4-cgi | libapache2-mod-php4, php4-ldap,
apache | apache-ssl | httpd, perl, wwwconfig-common, debconf
Recommends: php4-mhash
Suggests: ldap-server, sudo, php4-mcrypt
Conflicts: php4-apc
Filename: pool/main/l/ldap-account-manager/ldap-account-manager_0.4.6-2_all.deb
Size: 406002
MD5sum: 03bb45d124c8783415631f884c97692e
Description: Webfrontend for managing Unix and Samba accounts in a LDAP directory
 LDAP Account Manager (LAM) runs on an existing webserver. LAM
 supports LDAP connections via SSL and TLS. It uses the
 Samba 2.x or Samba 3 schema and manages user, group and host
 accounts. You can use templates for account creation and use
 multiple configuration profiles. Account information can be
 exported as PDF file. There is also a script
 included which manages quota and homedirectories, you have to
 setup sudo if you want to use it. LAM is translated to
 English, French, German, Hungarian and Japanese.
 .
 Homepage: http://lam.sourceforge.net/
```

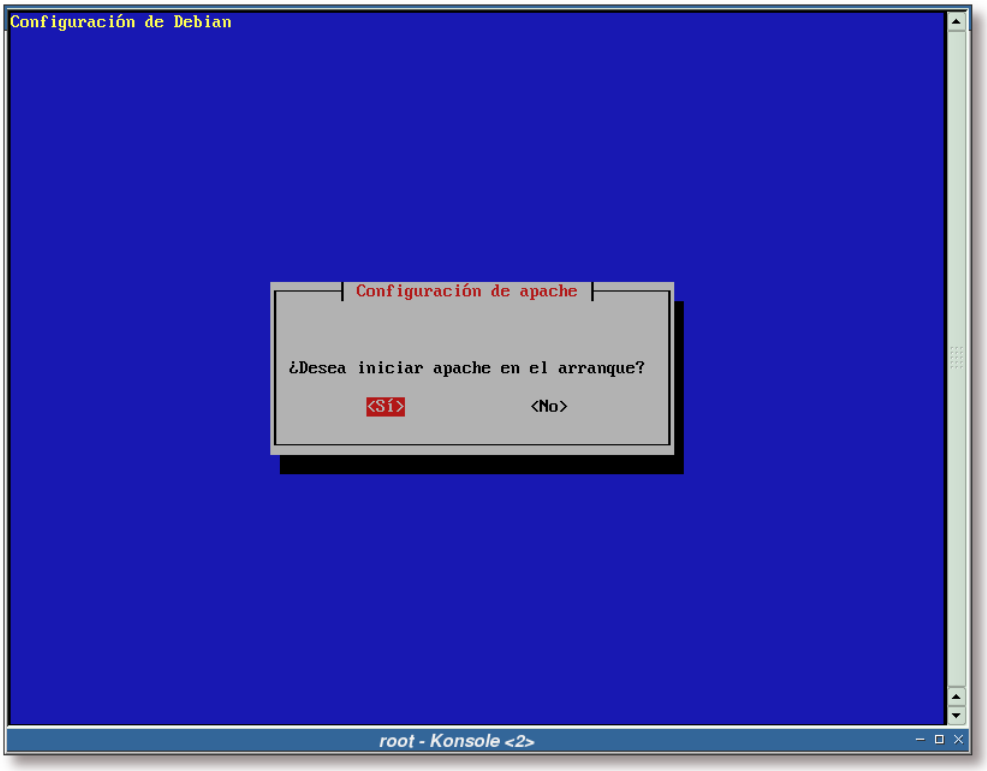
La manera de instalar este software se muestra a continuación:

Ejemplo F-2. Instalación de LAM (primera parte)

```
# /usr/bin/apt-get install ldap-account-manager
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
```

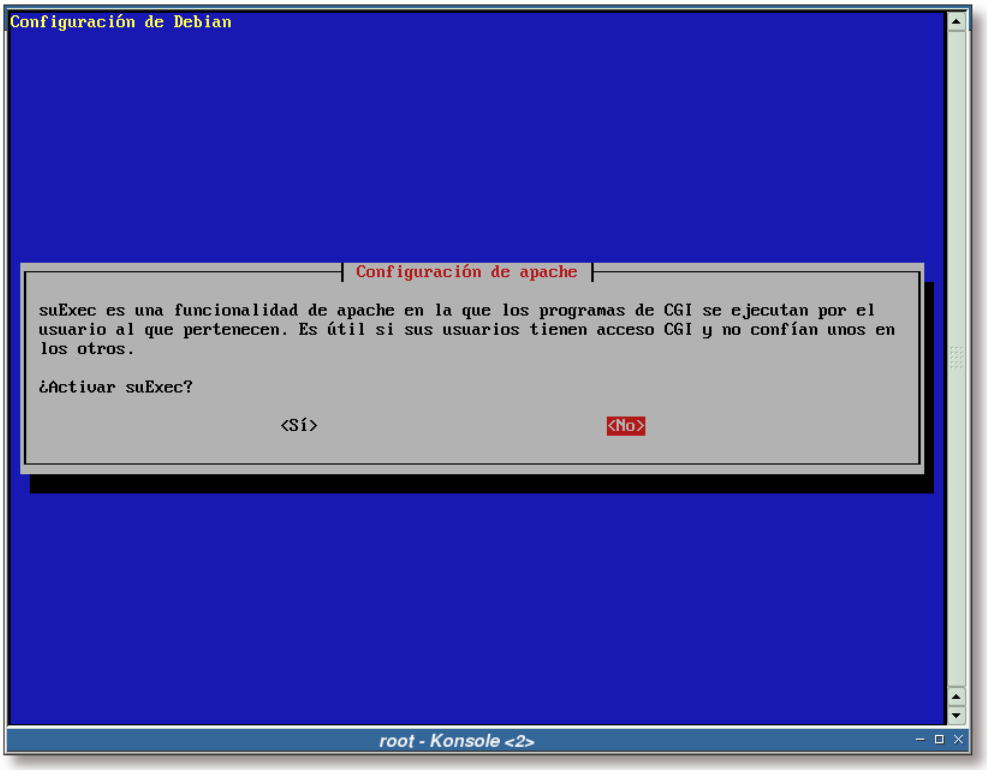
```
  apache apache-common apache-utils libapache-mod-php4 libapache-mod-ssl libmm13 php4
  php4-common php4-ldap wwwconfig-common
Paquetes sugeridos:
  apache-doc apache-ssl apache-perl sudo php4-mcrypt php4-pear libapache-mod-ssl-doc
  mysql-client postgresql-client
Paquetes recomendados
  php4-mhash
Se instalarán los siguientes paquetes NUEVOS:
  apache apache-common apache-utils ldap-account-manager libapache-mod-php4 libapache-mod-ssl
  libmm13 php4 php4-common php4-ldap wwwconfig-common
0 actualizados, 11 se instalarán, 0 para eliminar y 2 no actualizados.
Se necesita descargar 0B/3958kB de archivos.
Se utilizarán 11,3MB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n]
Preconfiguring packages ...
```

Figura F-1. ¿Arrancar Apache en el arranque?



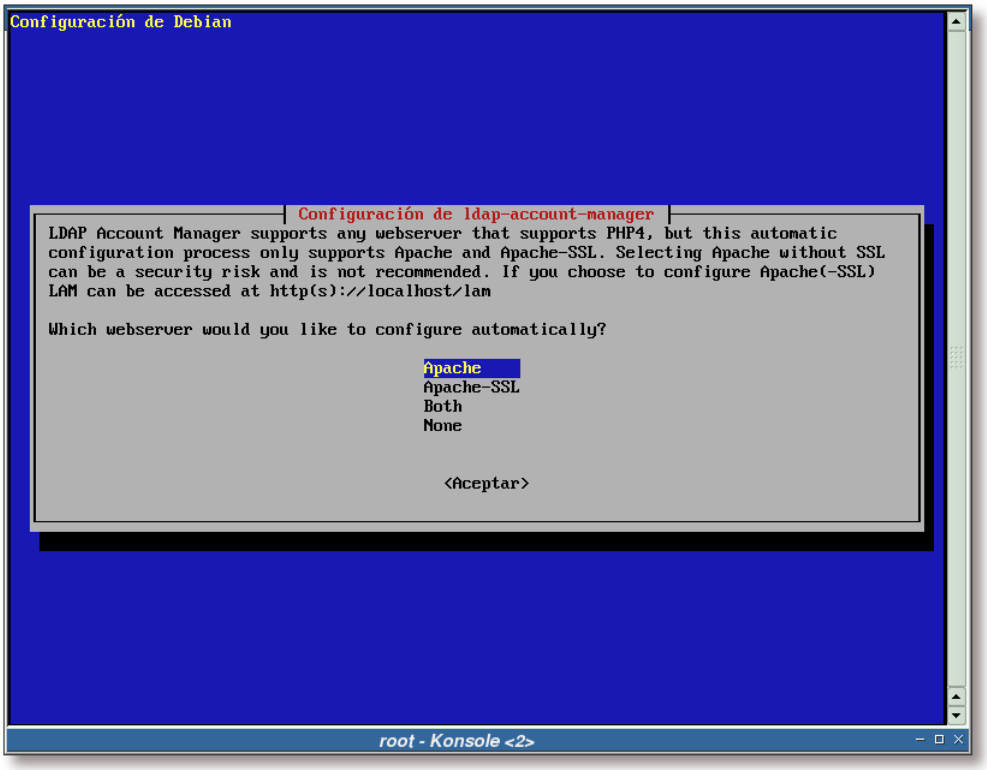
Adapte la respuesta a esta pregunta a sus necesidades, en este caso se ha decidido arrancar Apache en el arranque.

Figura F-2. ¿Activar suExec?



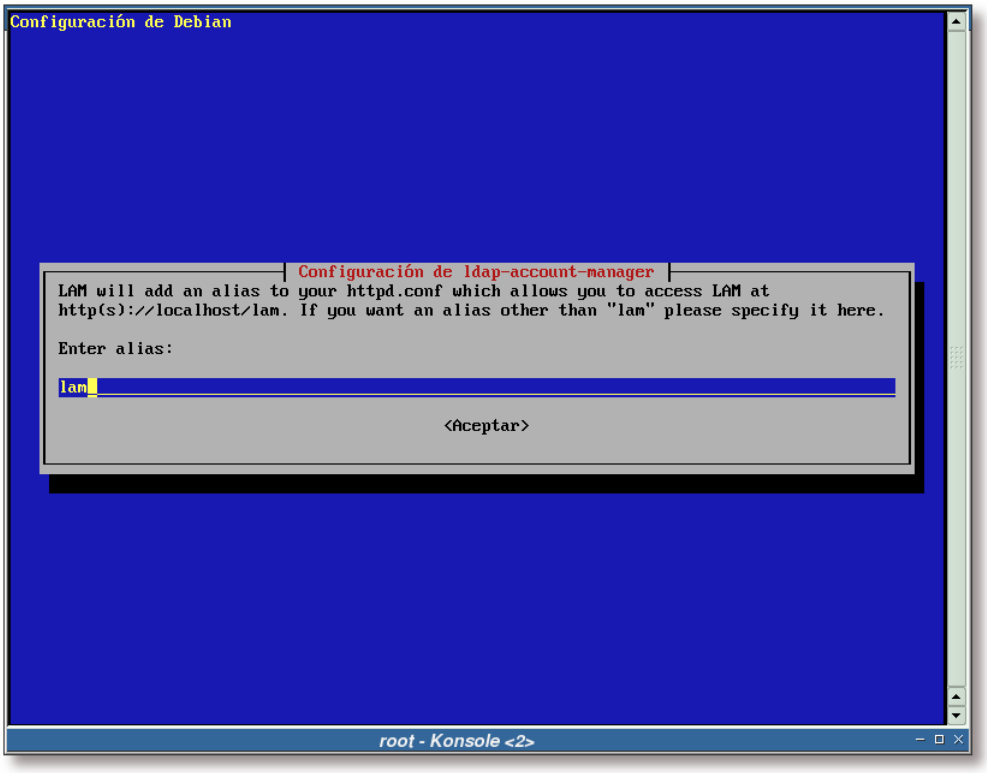
La respuesta a esta pregunta es negativa, de momento no se va a necesitar esta funcionalidad, por lo que así se evita tener un archivo *setuid* más en el sistema.

Figura F-3. ¿Para qué servidor(es) web se ha de configurar LAM?



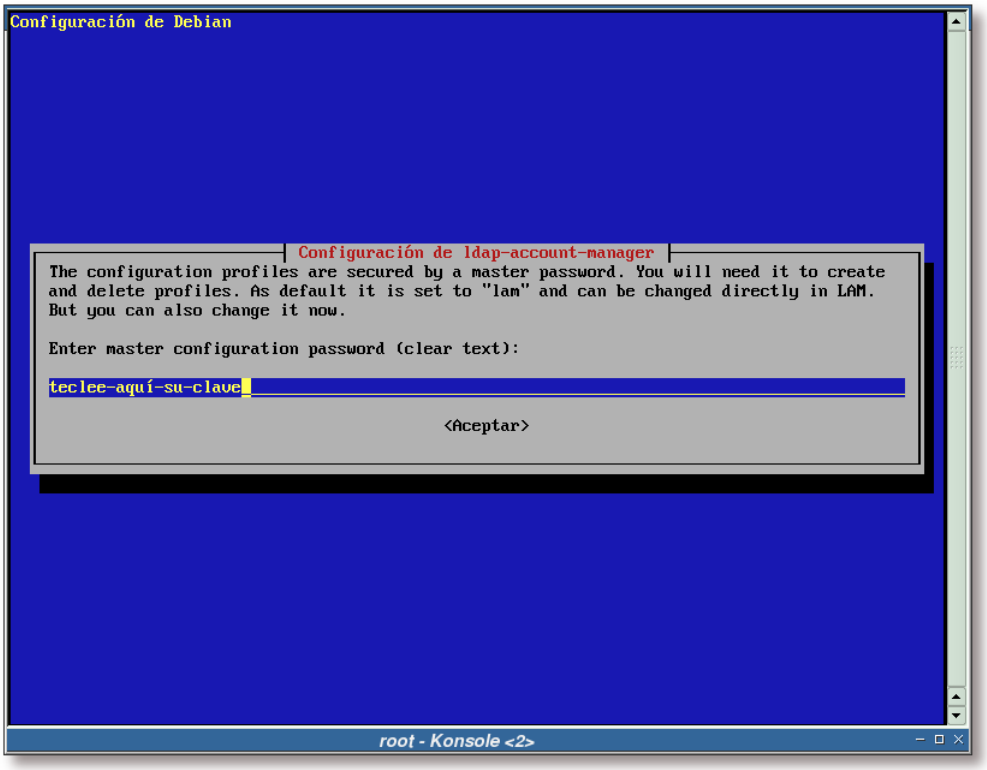
En esta documentación sólo se ha instalado el servidor web Apache, por lo que se elige esta opción. La funcionalidad SSL en Apache se provee mediante el módulo *mod_ssl* (paquete *libapache-mod-ssl*).

Figura F-4. Alias para el acceso a LAM desde el servidor web



Teclee en esta pantalla el alias con el que quiera acceder a la aplicación LAM desde su servidor web. En este caso se ha seleccionado el alias *lam*, por lo que para acceder a la herramienta, se hará a través de: *http://gsr.pt/lam/*.

Figura F-5. Clave para el administrador de los perfiles dentro de LAM



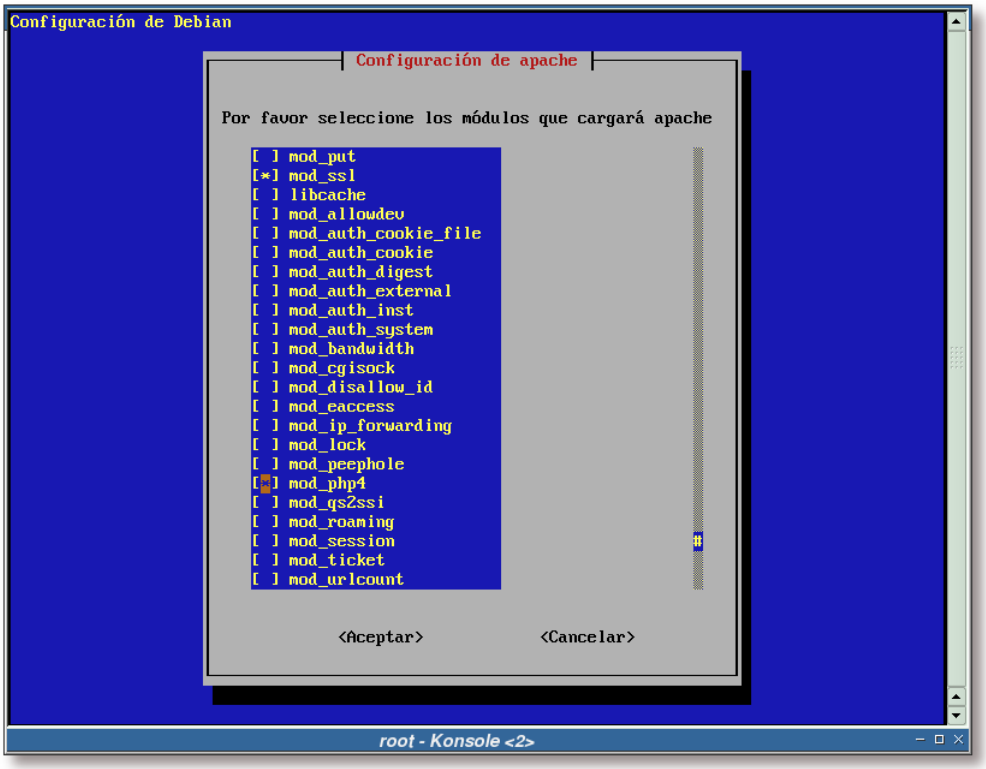
Teclee la clave, en texto plano, que desee para el administrador de perfiles de la herramienta LAM.

Ejemplo F-3. Instalación de LAM (segunda parte)

```
Seleccionando el paquete apache-utils previamente no seleccionado.
(Leyendo la base de datos ...
134049 ficheros y directorios instalados actualmente.)
Desempaquetando apache-utils (de .../apache-utils_1.3.31-6_i386.deb) ...
Seleccionando el paquete apache-common previamente no seleccionado.
Desempaquetando apache-common (de .../apache-common_1.3.31-6_i386.deb) ...
Seleccionando el paquete apache previamente no seleccionado.
Desempaquetando apache (de .../apache_1.3.31-6_i386.deb) ...
Seleccionando el paquete libmm13 previamente no seleccionado.
Desempaquetando libmm13 (de .../libmm13_1.3.0-3_i386.deb) ...
Seleccionando el paquete libapache-mod-ssl previamente no seleccionado.
Desempaquetando libapache-mod-ssl (de .../libapache-mod-ssl_2.8.19-1_i386.deb) ...
Seleccionando el paquete php4-common previamente no seleccionado.
Desempaquetando php4-common (de .../php4-common_4%3a4.3.8-12_i386.deb) ...
Seleccionando el paquete libapache-mod-php4 previamente no seleccionado.
Desempaquetando libapache-mod-php4 (de .../libapache-mod-php4_4%3a4.3.8-12_i386.deb) ...
Seleccionando el paquete php4 previamente no seleccionado.
Desempaquetando php4 (de .../php4_4%3a4.3.8-12_all.deb) ...
```

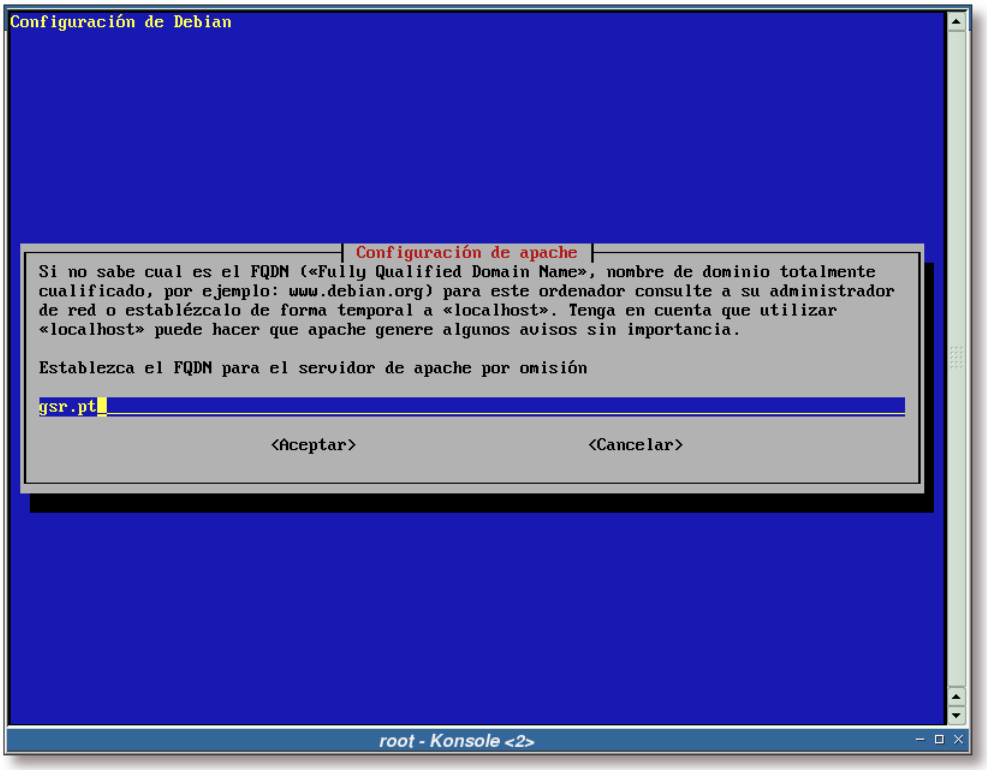
```
Seleccionando el paquete php4-ldap previamente no seleccionado.
Desempaquetando php4-ldap (de .../php4-ldap_4%3a4.3.8-12_i386.deb) ...
Seleccionando el paquete wwwconfig-common previamente no seleccionado.
Desempaquetando wwwconfig-common (de .../wwwconfig-common_0.0.40_all.deb) ...
Seleccionando el paquete ldap-account-manager previamente no seleccionado.
Desempaquetando ldap-account-manager (de .../ldap-account-manager_0.4.6-2_all.deb) ...
Configurando apache-utils (1.3.31-6) ...
Configurando apache-common (1.3.31-6) ...

Configurando apache (1.3.31-6) ...
```

Figura F-6. Módulos que cargará Apache



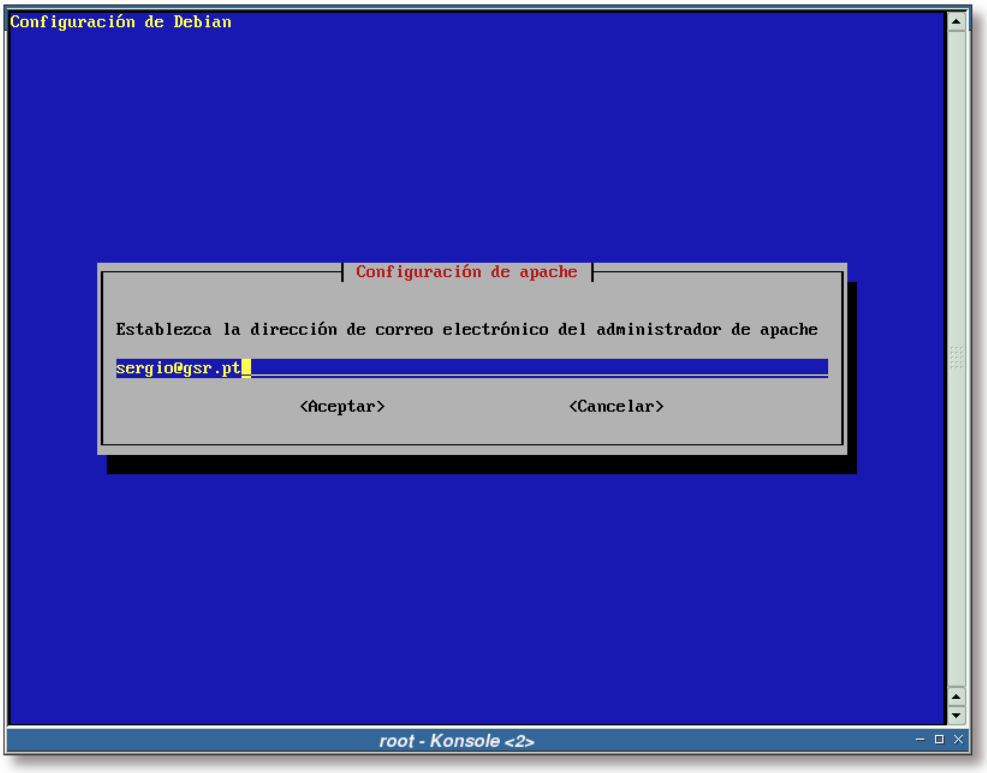
Asegúrese de que están marcados los módulos *mod_ssl* y *mod_php4*. El primero será necesario para activar el soporte SSL en Apache y el segundo para activar el soporte PHP4.

Figura F-7. Nombre del dominio que servirá Apache por defecto



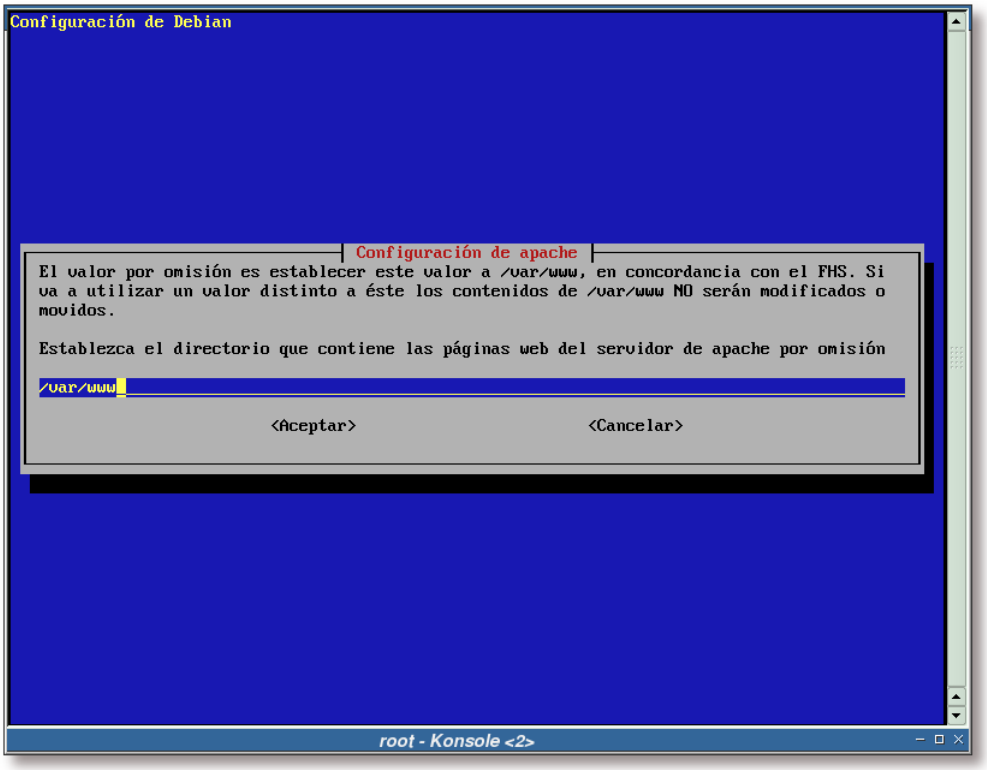
Teclee en esta pantalla el FQDN de su servidor web.

Figura F-8. Dirección de correo electrónico del administrador de Apache



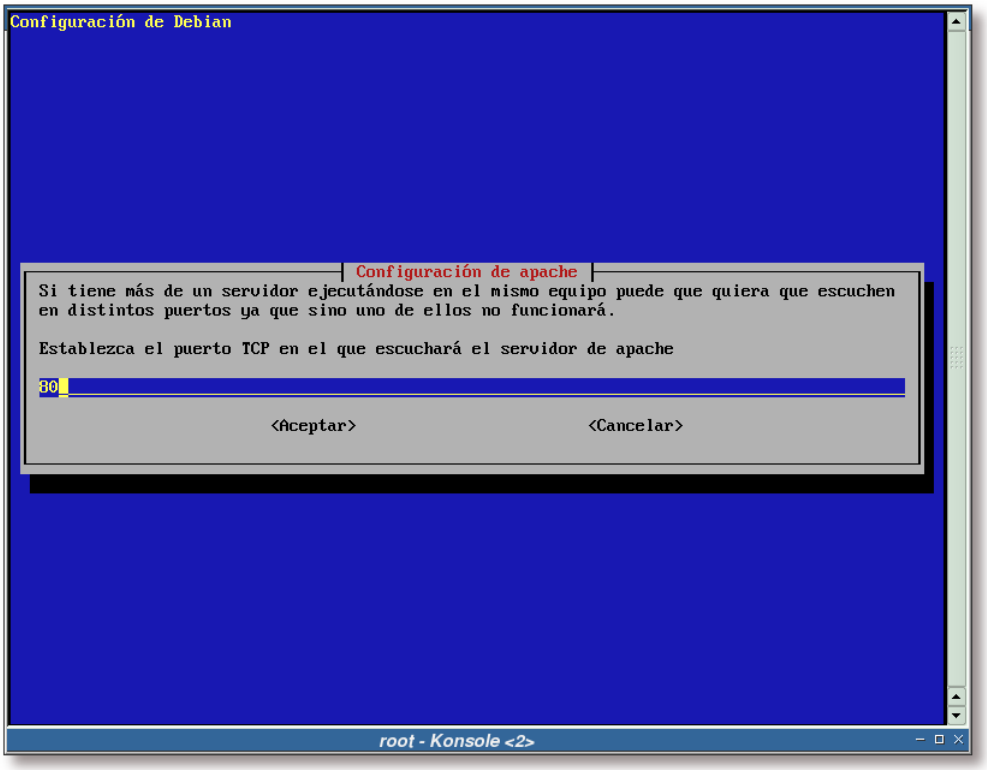
Complete el campo de la captura con la dirección del administrador encargado del servidor Apache.

Figura F-9. Directorio raíz de Apache por defecto



Sería recomendable dejar la sugerencia que se muestra en esta pantalla como directorio raíz de su servidor web.

Figura F-10. Puerto de escucha de Apache



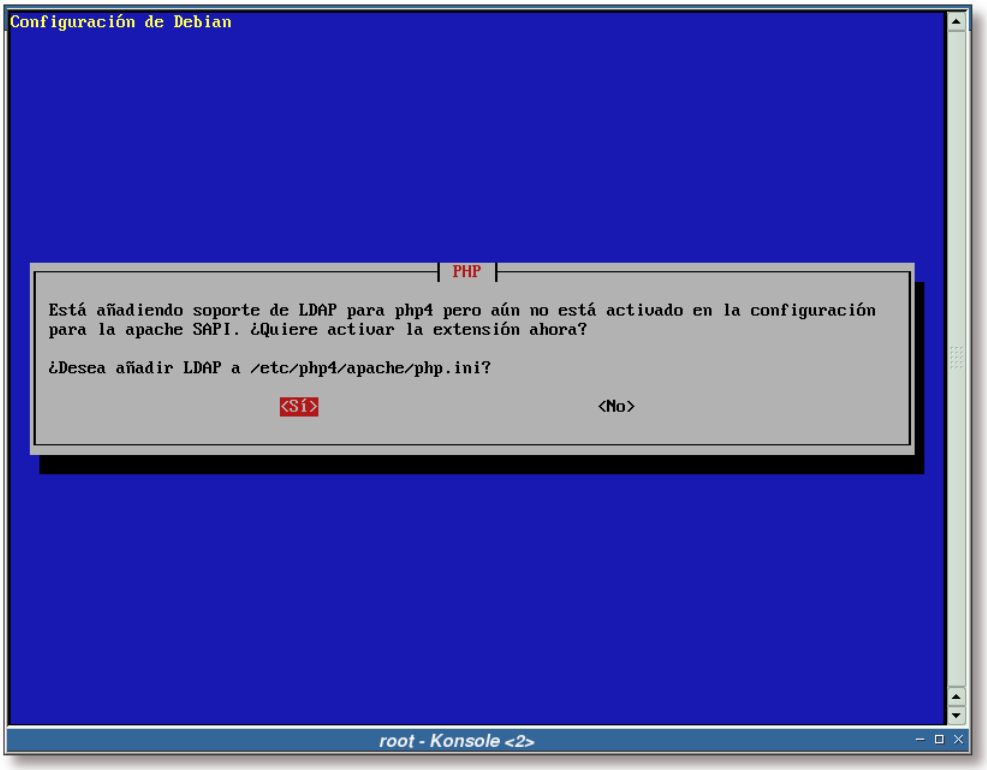
Establezca el puerto donde ha de escuchar Apache.

Ejemplo F-4. Instalación de LAM (tercera parte)

```
Creating config file /etc/apache/httpd.conf with new version

Creating config file /etc/apache/srm.conf with new version

Creating config file /etc/apache/access.conf with new version

Creating config file /etc/apache/modules.conf with new version
Starting web server: apache.

Configurando libmm13 (1.3.0-3) ...

Configurando libapache-mod-ssl (2.8.19-1) ...
./snakeoil-ca-rsa.crt ... e52d41d0.0
./ca-bundle.crt ... Skipped
./snakeoil-dsa.crt ... 5d8360e1.0
./snakeoil-rsa.crt ... 82ab5372.0
./snakeoil-ca-dsa.crt ... 0cf14d7d.0
```

```
Configurando php4-common (4.3.8-12) ...
Configurando libapache-mod-php4 (4.3.8-12) ...

Configurando php4 (4.3.8-12) ...

Configurando php4-ldap (4.3.8-12) ...
```

Figura F-11. Activar la extensión LDAP en PHP4



Seleccione *Sí* si desea activar la extensión LDAP en PHP4, sería recomendable, para que LAM funcionase.

Ejemplo F-5. Instalación de LAM (cuarta parte)

```
Configurando wwwconfig-common (0.0.40) ...
Configurando ldap-account-manager (0.4.6-2) ...

localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

Nota: Si no ve alguna de las pantallas de configuración que aquí se muestran, tal vez sea necesario forzar la configuración de algunos paquetes a “bajo nivel”. Para ello puede teclear:

```
# /usr/sbin/dpkg-reconfigure ldap-account-manager
```

O

```
# /usr/sbin/dpkg-reconfigure apache
```

O

```
# /usr/sbin/dpkg-reconfigure php4-ldap
```

Configuración

Configuración relativa a Apache

Nota: Si desea ver como se configura Apache para el soporte SSL, vea el Apéndice I.

Antes de proceder a la configuración de la herramienta, se va a obligar al servidor web Apache a servir las páginas relacionadas con LAM en modo SSL. Para ello, edite el archivo `/etc/ldap-account-manager/apache.conf` y añada las siguientes líneas al final del archivo:

```
# redirect to https when available (thanks omen@descolada.dartmouth.edu)
<IfModule mod_rewrite.c>
    <IfModule mod_ssl.c>
        <Location /lam>
            RewriteEngine on
            RewriteCond %{HTTPS} !=on
            RewriteRule . https://%{HTTP_HOST}%{REQUEST_URI}  [L]
        </Location>
    </IfModule>
</IfModule>
```

El siguiente paso será hacer que el servidor Apache relea su configuración:

Ejemplo F-6. Releyendo la configuración de Apache

```
# /etc/init.d/apache reload
Reloading apache configuration.
```

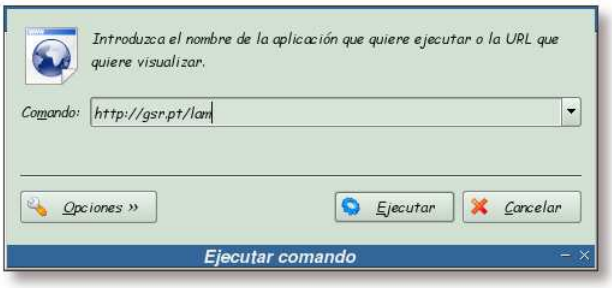
Configuración desde la interfaz web

Ahora que ya está instalado LAM en el sistema, el siguiente paso será acceder a la interfaz LAM con un navegador web. Para ello se ha de teclear la siguiente URL en su navegador favorito: *http://gsr.pt/lam* (suponiendo que "gsr.pt" sea su dominio).

En las siguientes capturas se mostrará el proceso de configuración de LAM desde la interfaz web. Durante el proceso se creará un nuevo perfil.

Importante: No utilice caracteres especiales al reyenar los campos, pues LAM no los reconoce.

Figura F-12. URL donde está instalado LAM



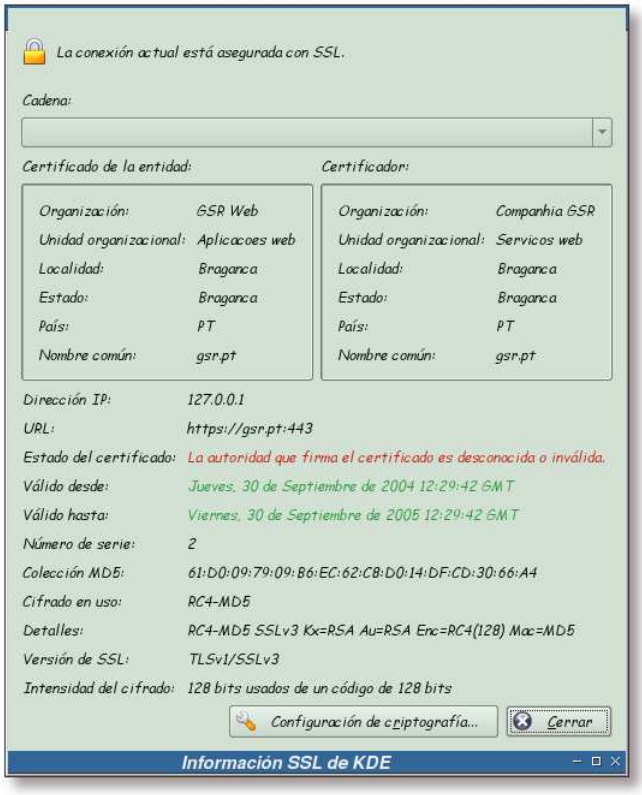
Si se encuentra en un entorno de escritorio con KDE, teclee **Alt**+**F2** e introduzca la dirección donde se encuentre instalado LAM.

Figura F-13. Aviso acerca del certificado del servidor web I

Si ha configurado correctamente el servidor web, a la hora de acceder a la aplicación LAM por el protocolo *http*, Apache le tendría que redireccionar a la misma dirección, pero bajo el protocolo *https*.

Esto es lo que ha ocurrido en esta pantalla, Apache ha redirigido la petición realizada (http://gsr.pt/lam/) hacia el protocolo *https*. Por este motivo, y debido a que la entidad certificadora que se ha creado es desconocida, sale este aviso. Pulse sobre el botón *Detalles* para obtener más información.

Figura F-14. Información SSL



En esta pantalla se muestra la información del certificado y la entidad certificadora que ha creado dicho certificado. Si se fija, aquí aparecerán los datos tecleados en el Apéndice I. Pulse sobre el botón *Cerrar* para continuar.

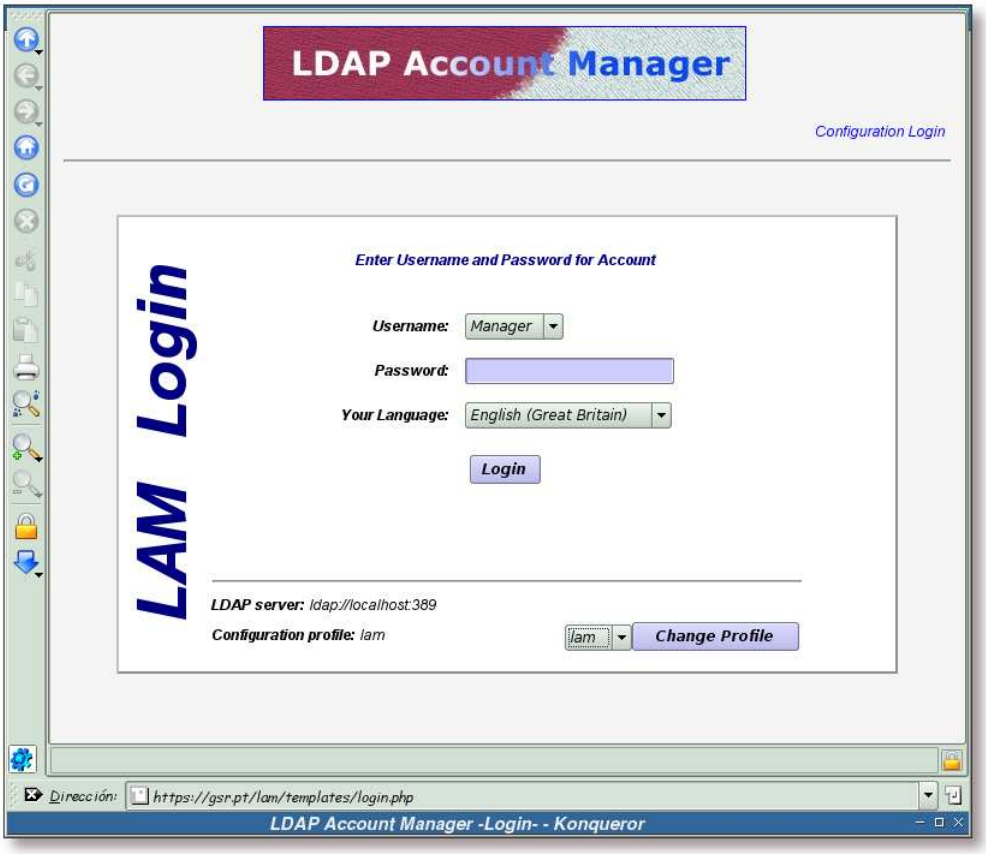
Figura F-15. Aviso acerca del certificado del servidor web II

Pulse ahora sobre el botón *Continuar* para seguir con la carga de la página.

Figura F-16. Período de aceptación del certificado

Seleccione la opción deseada y pulse sobre ella.

Figura F-17. Pantalla de ingreso

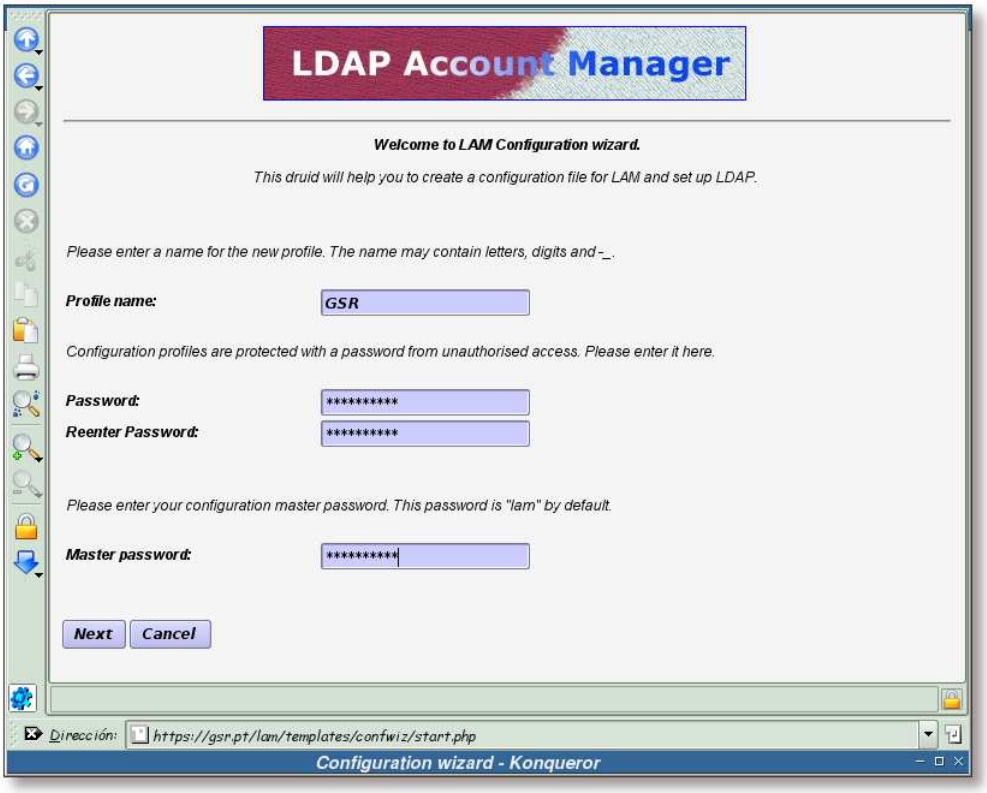


Pantalla principal de LAM antes del ingreso. Como es la primera vez que se accede, se creará un nuevo perfil adaptado a las necesidades del sistema. Para ello pulse sobre *Configuration Login*.

Figura F-18. Pantalla de configuración

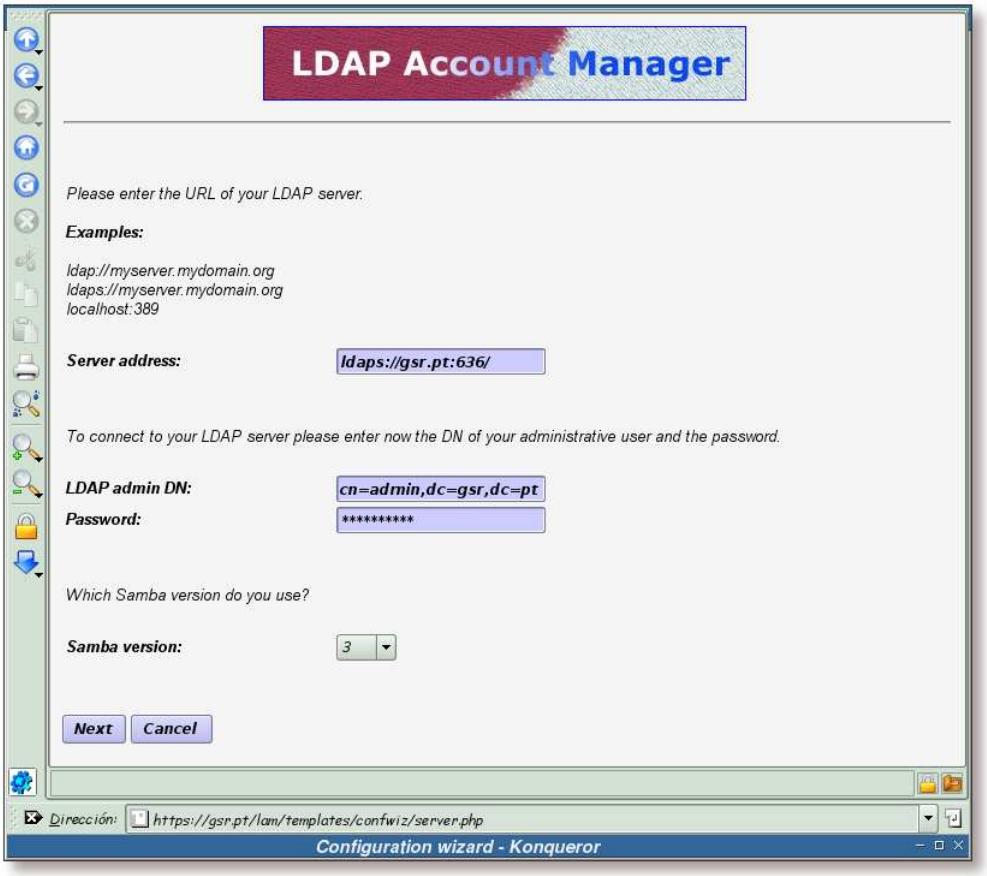
Esta imagen presenta la pantalla de configuración de LAM, aquí seleccione el enlace: *Configuration wizard*.

Figura F-19. Asistente de configuración, datos del perfil



A partir de esta pantalla, se irán completando las distintas opciones que presente el asistente de configuración de LAM. Aquí se pide el nombre para el nuevo perfil (*Profile name*), la clave para acceder al nuevo perfil creado (*Password*) y la clave principal (*Master password*) de LAM, recuerde que esta clave se estableció en el proceso de instalación (Figura F-5).

Figura F-20. Asistente de configuración, datos del servidor LDAP y Samba



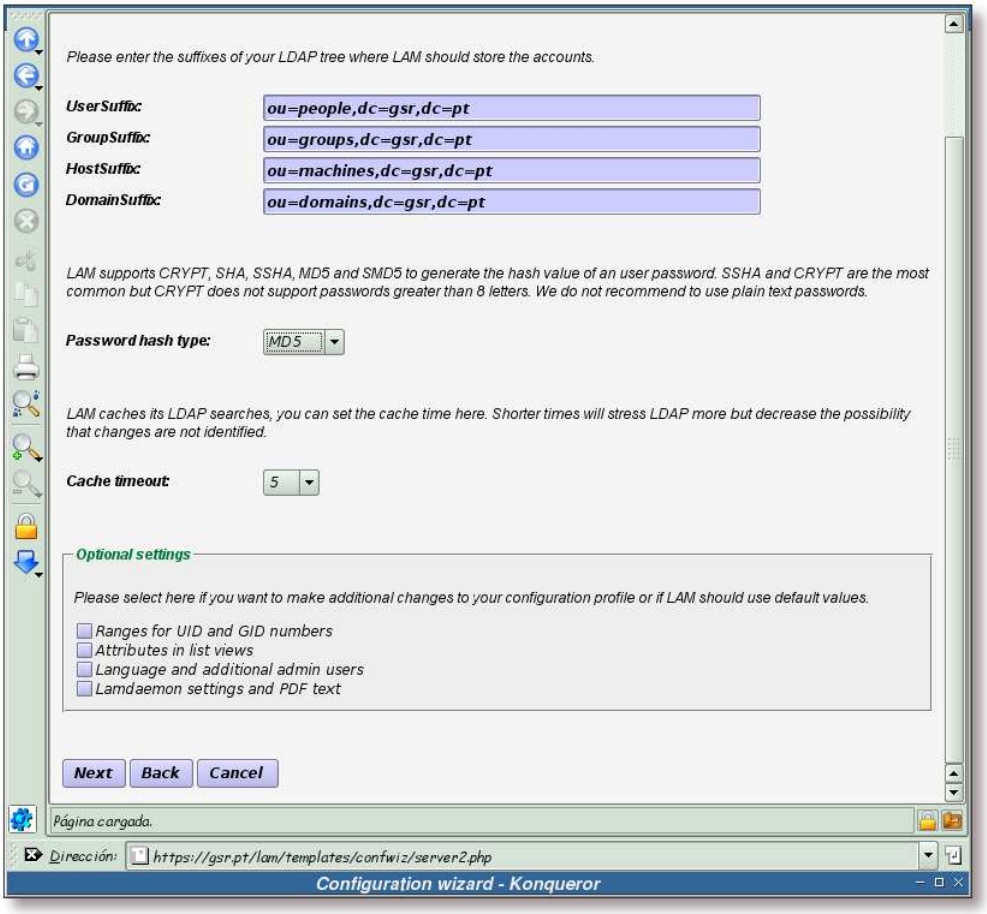
Pantalla dedicada a la localización del servidor LDAP y la versión de Samba:

- *Server address*: dirección del servidor LDAP que se va a utilizar.

Nota: Como no especifíca en ningún lugar la forma de activar el uso de TLS para las comunicaciones contra el servidor LDAP, si quiere asegurarse una conexión cifrada entre LAM y el servidor LDAP, especifique aquí la dirección mediante el protocolo *ldaps*, para utilizar SSL en las comunicaciones.

- *LDAP admin DN*: administrador del directorio LDAP.
- *Password*: clave para el administrador del directorio LDAP.
- *Samba version*: versión de Samba que se va a emplear, en este caso es la versión 3.*

Figura F-21. Asistente de configuración, creando la estructura para el directorio LDAP



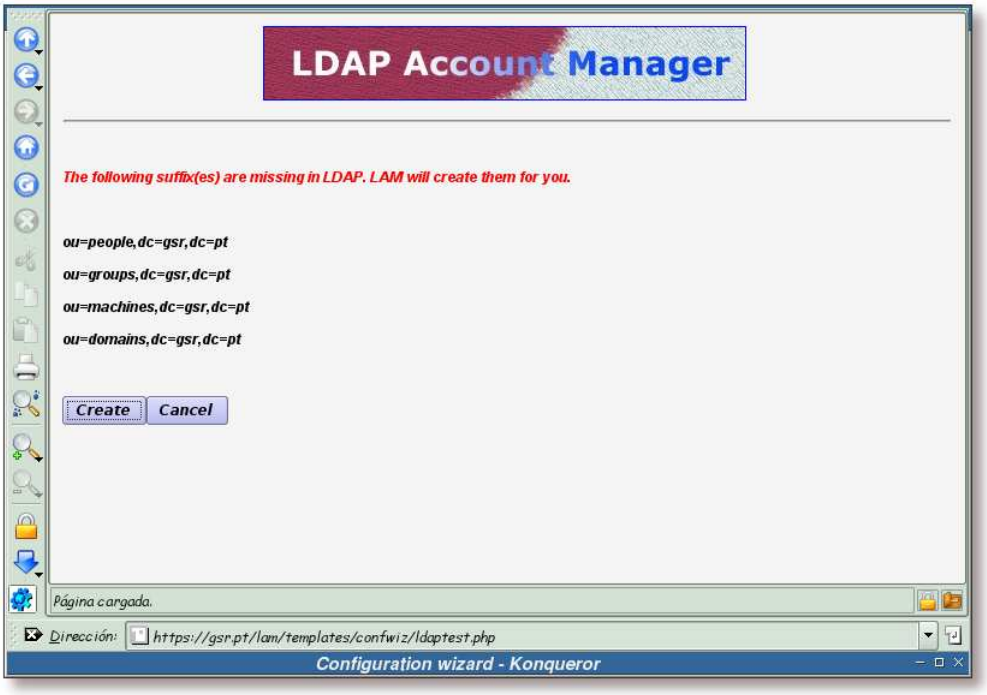
Las cuentas que se crearán a través de LAM se almacenarán en el directorio LDAP de la forma que se indique en este paso:

- *UserSuffix*: lugar donde se almacenarán las cuentas de los usuarios.
- *GroupSuffix*: lugar donde se almacenarán las cuentas de los grupos de usuarios.
- *HostSuffix*: lugar donde se almacenará la información sobre las máquinas Samba.
- *DomainSuffix*: lugar donde se almacenará la información sobre los dominios Samba.
- *Password hash type*: tipo de algoritmo de hash a utilizar para almacenar las claves, en este caso se ha elegido el tipo MD5.
- *Cache timeout*: tiempo que LAM mantendrá en su caché las búsquedas LDAP realizadas.
- *Optional settings*: las opciones por defecto se adaptan a las necesidades del proyecto, por lo que no se selecciona ninguna opción en este cuadro.

  La última opción: *Lamdaemon settings and PDF text* sirve para ajustar, entre otras cosas, la ruta al script `lamdaemon.pl`. Este script permite la creación/eliminación de los directorios home de los usuarios y el establecimiento de quotas para los mismos.

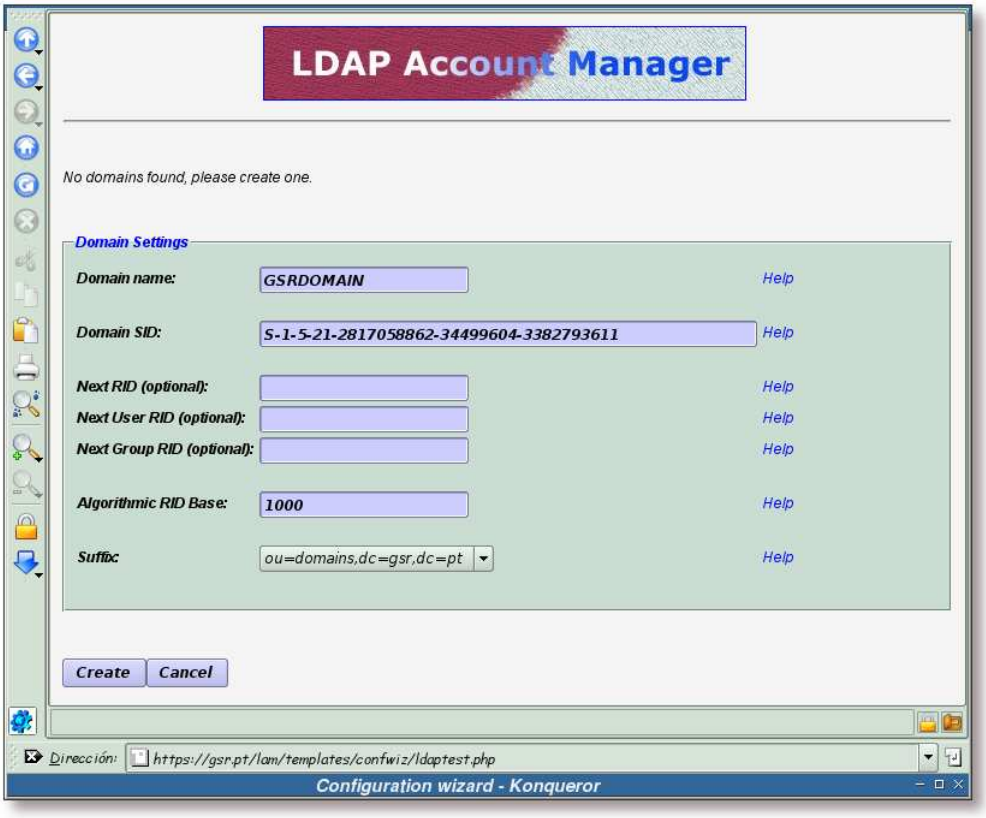
En esta documentación no se ha empleado dicho script, en su lugar se ha empleado el script del Apéndice K.

Figura F-22. Asistente de configuración, confirmación de la creación de entradas LDAP



Confirmación para la creación de las nuevas entradas en el directorio LDAP.

Figura F-23. Asistente de configuración, creación de un dominio



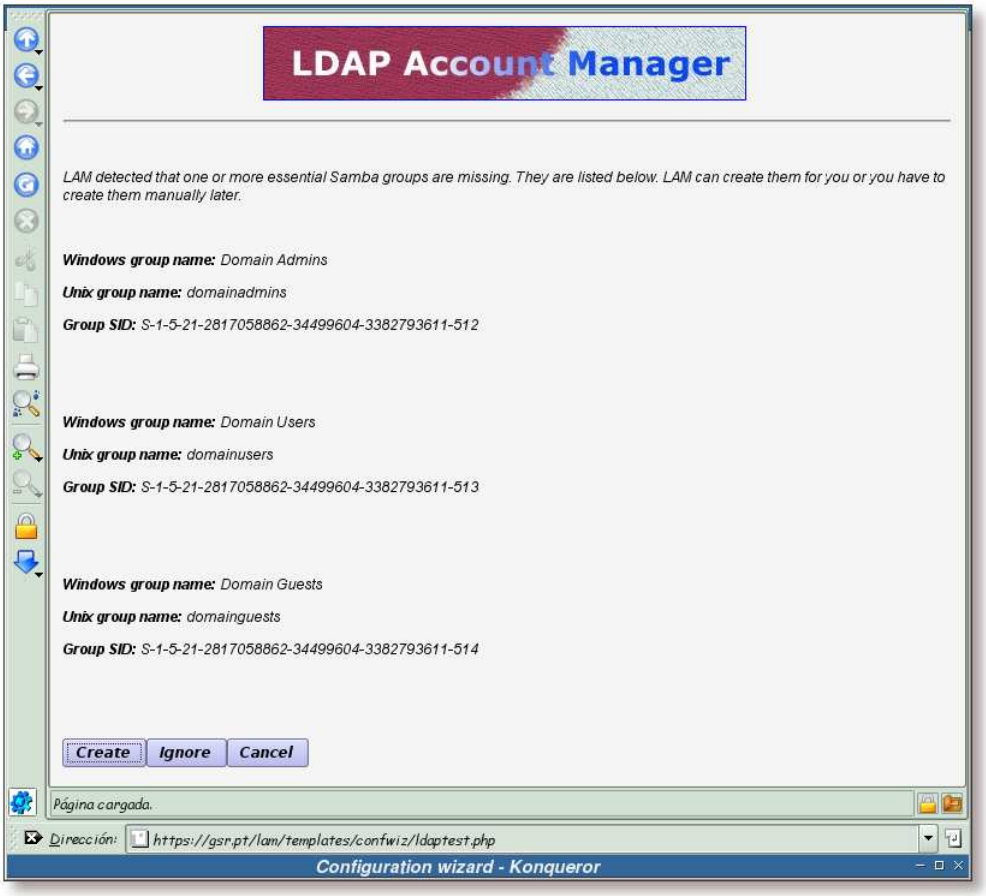
Aquí se introducirá el dominio que se va a utilizar en Samba así como el SID del servidor donde está alojado, las demás opciones se dejarán como están. De esta forma, en la opción *Domain name* se ha de teclear el dominio correspondiente (en este caso GSRDOMAIN).

La forma de obtener el SID se muestra en el Ejemplo F-7, su resultado se ha de introducir en la opción *Domain SID*.

Ejemplo F-7. Obtención del SID

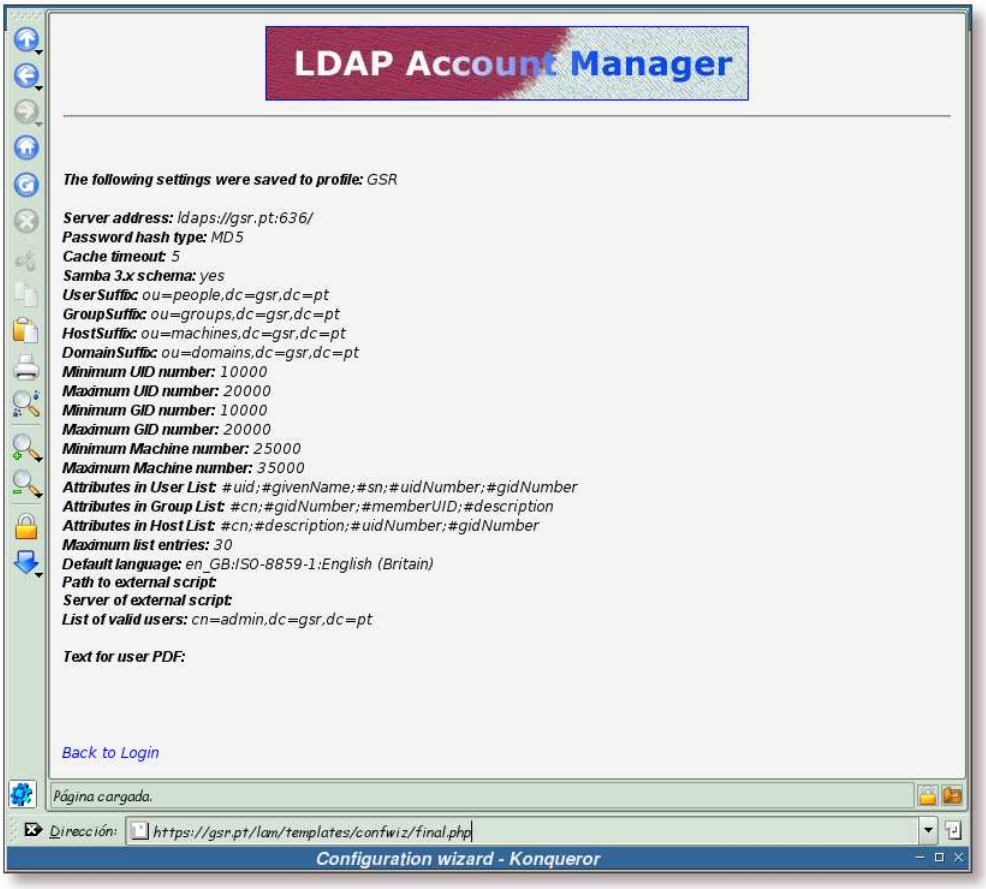
```
# /usr/bin/net getlocalsid
SID for domain TODOSCSI is: S-1-5-21-2817058862-34499604-3382793611
```

Figura F-24. Asistente de configuración, creación de grupos para Samba



El asistente pide confirmación para la creación de una serie de grupos esenciales para Samba, se pulsa sobre *Create* para continuar.

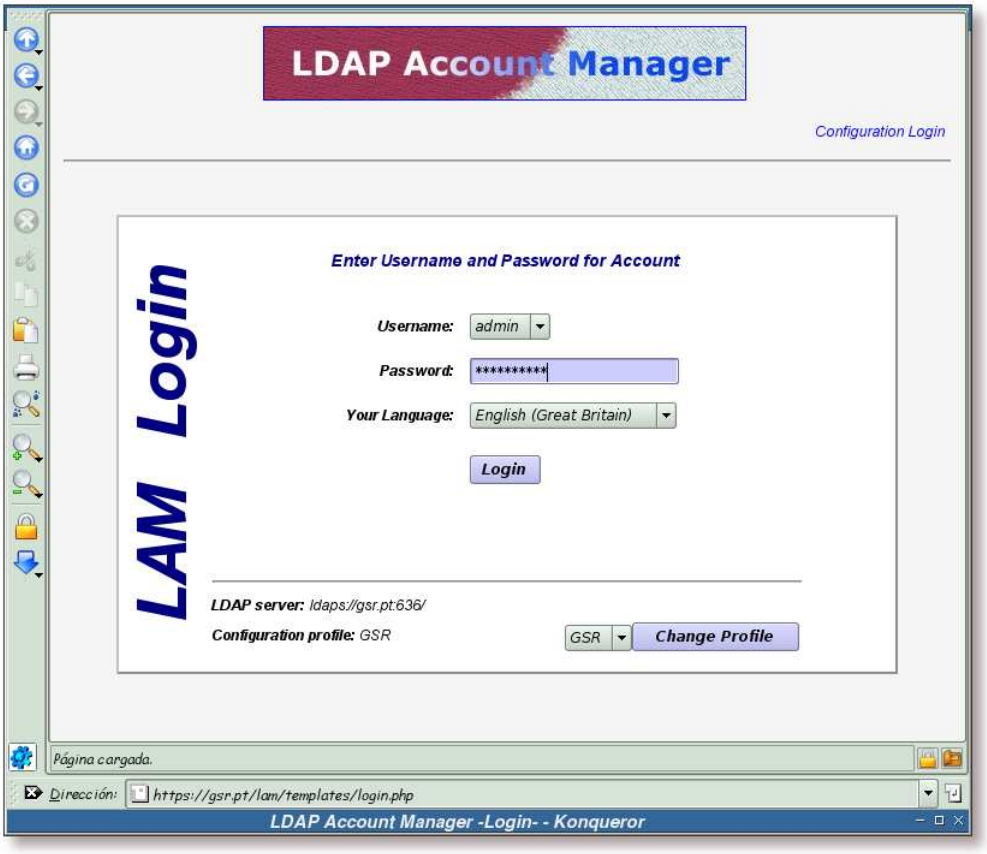
Figura F-25. Información sobre el nuevo perfil creado



Esta pantalla muestra la información que se a almacenado para el perfil *GSR* que se acaba de crear. A continuación se regresará a la pantalla de ingreso, pulsando sobre el enlace *Back to Login*.

Como se ha creado un nuevo perfil adaptado a las necesidades del sistema, *GSR*, sería recomendable modificar el archivo `/etc/ldap-account-manager/config.cfg` para indicar que el perfil por defecto pasa a ser *GSR* y no *lam*. Para ello, se ha de asignar el valor *GSR* a la variable: *default*.

Figura F-26. Ingreso en LAM



En estos momentos, ya se puede ingresar al sistema con el perfil que se acaba de añadir. Para ello, si no está seleccionado, elija el perfil *GSR* y pulse sobre: *Change Profile*. Una vez seleccionado el perfil adecuado, se ha de teclear la clave del administrador del directorio LDAP y pulsar sobre *Login*.

Figura F-27. Pantalla principal de LAM

Nada más ingresar en la herramienta, se muestran los usuarios que posee el directorio LDAP bajo la unidad organizacional *people* (en estos momentos no hay ningún usuario, ya que se acaba de crear la estructura y todavía no se ha añadido ningún usuario).

Figura F-28. Dominios existentes

Si se pulsa sobre el enlace *Domains*, se listan los dominios existentes bajo la unidad organizacional *domains*. En estos momentos, sólo hay un dominio: *GSRDOMAIN*, creado en el proceso de configuración.

Figura F-29. Grupos existentes

Bajo el enlace *Groups*, se listan los grupos existentes bajo la unidad organizacional *groups*. Actualmente los grupos existentes únicamente son tres, los que se han creado durante el proceso de configuración.

Nota: Si no ha cambiado el grupo del directorio `/home/samba/netlogon/`, este sería un buen momento para hacerlo. Más detalles en el Ejemplo 10-4.

Figura F-30. Hosts existentes

Al pulsar sobre *Hosts*, se muestran las máquinas de Samba existentes bajo la unidad organizacional *machines*. Como se puede ver, todavía no se ha introducido ninguna máquina.

Figura F-31. Saliendo de la herramienta

Una vez se ha finalizado el uso de la herramienta, se ha de salir de la misma, para ello se ha de pulsar sobre el enlace *Logout*.

LAM ya se encuentra completamente instalado y adaptado a las necesidades del sistema, por lo que ya se puede comenzar a utilizar para la administración de usuarios y demás aspectos relativos.

En las secciones la sección de nombre *Adición de un usuario al sistema* en Capítulo 11 y la sección de nombre *Creación de cuentas para las máquinas* en Capítulo 12 tiene un ejemplo sobre como crear cuentas de usuario y máquina, respectivamente.

Apéndice G. Instalación y configuración de *phpLDAPadmin*

Instalación

phpLDAPadmin es una interfaz web destinada a la administración de un directorio LDAP. Antes de proceder con la instalación de phpLDAPadmin, se verá la descripción del paquete *phpldapadmin*, que provee dicha herramienta dentro de Debian:

Ejemplo G-1. Descripción de phpLDAPadmin

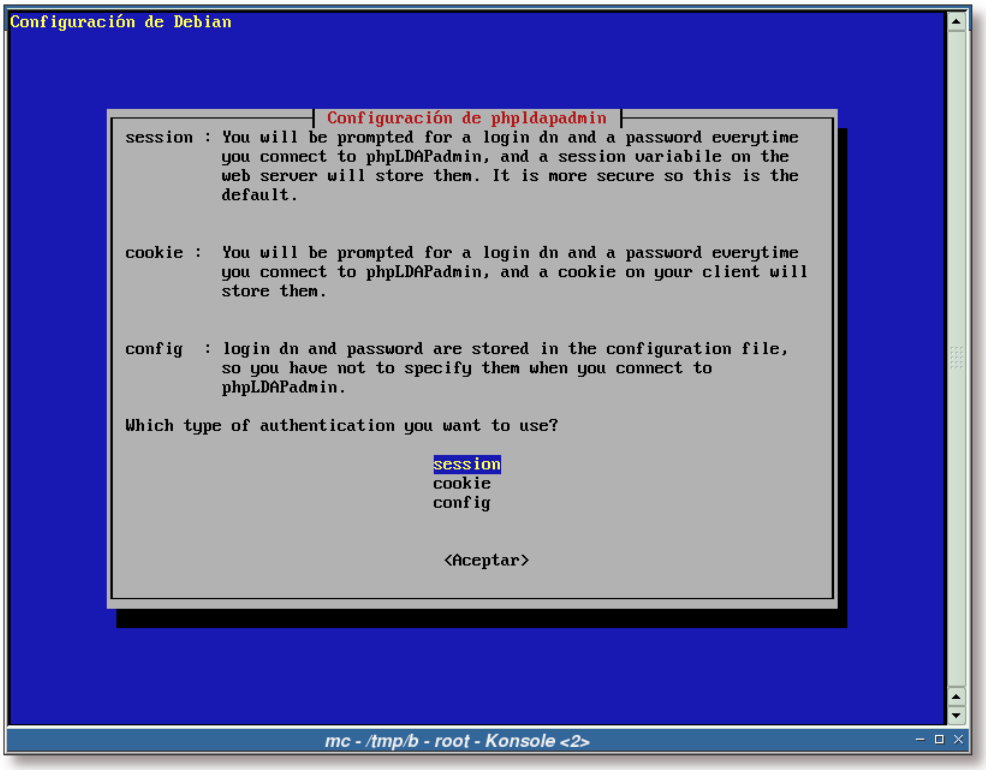
```
$ /usr/bin/apt-cache show phpldapadmin
Package: phpldapadmin
Priority: extra
Section: admin
Installed-Size: 1716
Maintainer: Fabio Tranchitella <kobold@kobold.it>
Architecture: all
Version: 0.9.4-9
Depends: apache | httpd, php4-ldap,
php4 (>= 4.1.0) | php4-cgi (>= 4.1.0) | libapache2-mod-php4, debconf (>= 0.2.26)
Filename: pool/main/p/phpldapadmin/phpldapadmin_0.9.4-9_all.deb
Size: 374178
MD5sum: eea7c0c0bc601462e999a5207c530846
Description: Web based interface for administering LDAP servers
 phpLDAPadmin is a web-based LDAP client. It provides easy,
 anywhere-accessible, multi-language administration for your LDAP
 server. Its hierarchical tree-viewer and advanced search functionality
 make it intuitive to browse and administer your LDAP directory. Since it
 is a web application, this LDAP browser works on many platforms, making
 your LDAP server easily manageable from any location.
```

El proceso de instalación de esta herramienta se muestra en el siguiente ejemplo:

Ejemplo G-2. Instalación del paquete *phpldapadmin* (primera parte)

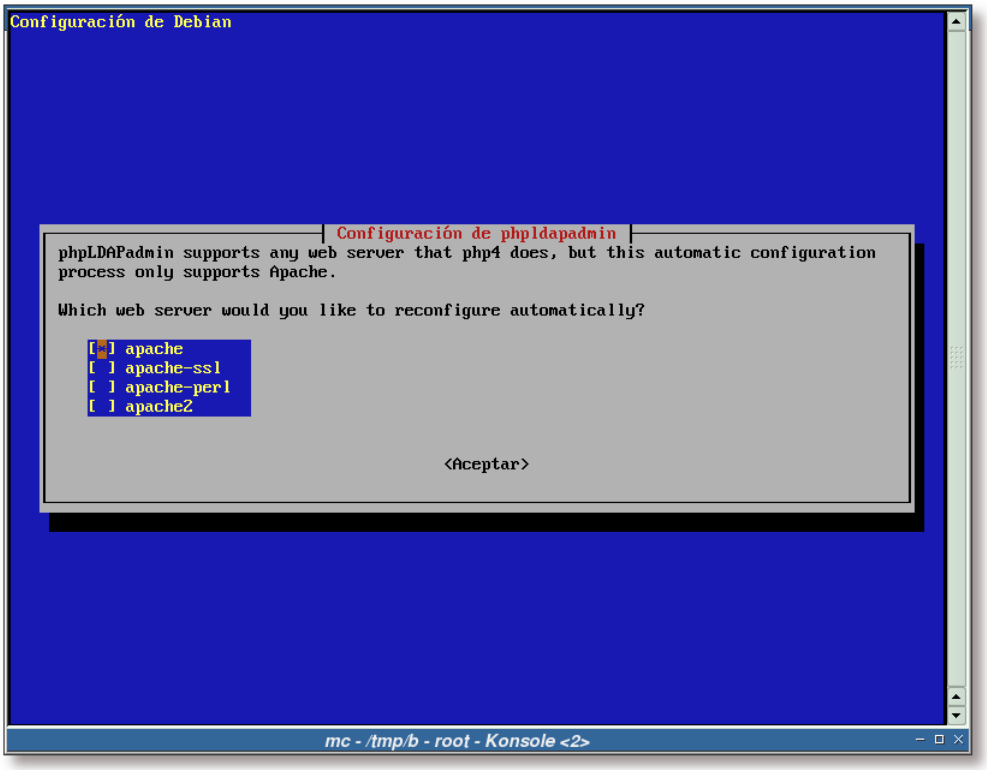
```
# /usr/bin/apt-get install phpldapadmin
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  phpldapadmin
0 actualizados, 1 se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 0B/374kB de archivos.
Se utilizarán 1757kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...
```

Figura G-1. ¿Qué tipo de autentificación desea?



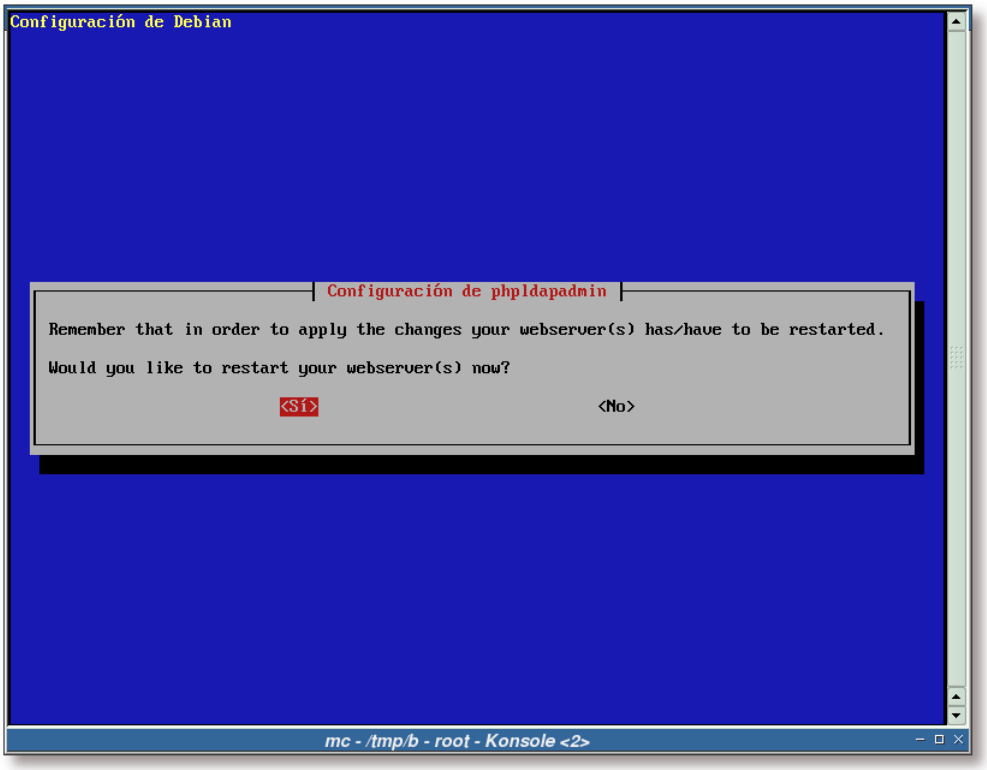
Seleccione aquí el tipo de autentificación que más se ajuste a sus necesidades, en esta documentación se ha seleccionado la opción “session”.

Figura G-2. ¿Qué servidor web reconfigurar?



Elija la versión(es) de Apache que tenga instalada(s) o aquella(s) para la(s) cual(es) quiera configurar el acceso a phpldapadmin.

Figura G-3. ¿Reiniciar el servidor web?



Sería recomendable reiniciar el servidor web, para que relea la nueva configuración.

Ejemplo G-3. Instalación del paquete *phpldapadmin* (segunda parte)

```
Seleccionando el paquete phpldapadmin previamente no seleccionado.
(Leyendo la base de datos ...
135022 ficheros y directorios instalados actualmente.)
Desempaquetando phpldapadmin (de .../phpldapadmin_0.9.4-9_all.deb) ...
Configurando phpldapadmin (0.9.4-9) ...
Restarting apache.

localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

Configuración

Configuración relativa a Apache

> **Nota:** Si desea ver como se configura Apache para el soporte SSL, vea el Apéndice I.

Antes de proceder a la configuración de la herramienta, se va a obligar al servidor web Apache a servir las páginas relacionadas con *phpLDAPadmin* en modo SSL. Para ello, edite el archivo `/etc/phpldapadmin/apache.conf` y añada las siguientes líneas al final del archivo:

```
# redirect to https when available (thanks omen@descolada.dartmouth.edu)
<IfModule mod_rewrite.c>
    <IfModule mod_ssl.c>
        <Location /phpldapadmin>
            RewriteEngine on
            RewriteCond %{HTTPS} !=on
            RewriteRule . https://%{HTTP_HOST}%{REQUEST_URI}  [L]
        </Location>
    </IfModule>
</IfModule>
```

El siguiente paso será hacer que el servidor Apache relea su configuración:

Ejemplo G-4. Releyendo la configuración de Apache

```
# /etc/init.d/apache reload
Reloading apache configuration.
```

Ajustes en la configuración

El último paso antes de tener *phpLDAPadmin* completamente instalado y configurado, es retocar varios archivos de configuración del mismo. Las siguientes secciones mostrarán dichos cambios.

`/etc/phpldapadmin/config.php`

Las siguientes líneas mostrarán las opciones más importantes del archivo de configuración `/etc/phpldapadmin/config.php` y los valores adoptados en esta documentación.

> **Nota:** En el Apéndice AI posee un ejemplo completo de este archivo de configuración.

1. Nombre del equipo donde está alojado el servidor LDAP:

   ```
   $servers[$i]['name'] = 'TodoSCSI';
   ```

2. URL del servidor LDAP. Si quiere utilizar TLS en la conexión contra el servidor LDAP (como es el caso de esta documentación), asegúrese de indicar aquí la dirección del servidor LDAP por el protocolo *ldap*.

   ```
   $servers[$i]['host'] = 'ldap://gsr.pt';
   ```

3. La base DN del servidor LDAP.

   ```
   $servers[$i]['base'] = 'dc=gsr,dc=pt';
   ```

4. Puerto del servidor LDAP. Al igual que se indicaba anteriormente, especifique aquí el puerto del servidor LDAP que no utilice cifrado SSL, esto es necesario para realizar las conexiones por TLS.

   ```
   $servers[$i]['port'] = 389;
   ```

5. Tipo de autentificación que se utilizará. Esta opción ya se definió en el proceso de instalación de *phpldapadmin* (vea la Figura G-1 para más datos).

   ```
   $servers[$i]['auth_type'] = 'session';
   ```

6. Usuario con el que se desea ingresar en *phpLDAPadmin* por defecto. El DN que aquí se teclee, aparecerá por defecto siempre que trate de ingresar en la herramienta.

   ```
   $servers[$i]['login_dn'] = 'cn=admin,dc=gsr,dc=pt';
   ```

7. Se activa la conexión por TLS entre la aplicación *phpLDAPadmin* y el servidor LDAP.

   ```
   $servers[$i]['tls'] = true;
   ```

8. Seleccione el algoritmo de hash que desee utilizar por defecto para el cifrado de las claves.

   ```
   $servers[$i]['default_hash'] = 'crypt';
   ```

9. Si se quiere que *phpLDAPadmin* busque y asigne automáticamente el *uid* para las nuevas entradas, active esta opción.

   ```
   $servers[$i]['enable_auto_uid_numbers'] = true;
   ```

10. Método para buscar el primer *uid* disponible en el sistema.

    ```
    $servers[$i]['auto_uid_number_mechanism'] = 'search';
    ```

11. Base de la búsqueda para encontrar el siguiente *uid* libre en el sistema.

    ```
    $servers[$i]['auto_uid_number_search_base'] = 'ou=people,dc=gsr,dc=pt';
    ```

12. Si se ha seleccionado la opción "search" para encontrar automáticamente los *uids* de las nuevas entradas, indique aquí el valor mínimo que un UID puede tener.

    ```
    $servers[$i]['auto_uid_number_min'] = 1000;
    ```

/etc/phpldapadmin/templates/template_config.php

En este archivo se configuran algunos aspectos relativos a Samba y la forma de añadir cuentas al sistema. A continuación se verán las partes que se han modificado de este archivo, en relación al archivo original distribuido con la herramienta:

> **Nota:** En el Apéndice AJ posee un archivo de configuración completo.

Ejemplo G-5. Modificaciones realizadas al archivo `template_config.php`

```
--- template_config.php.orig    2004-10-01 18:22:34.000000000 +0200
+++ template_config.php 2004-10-01 22:10:18.000000000 +0200
@@ -101,7 +101,7 @@

 // uncomment to set the base dn of posix groups
 // default is set to the base dn of the server
-//$base_posix_groups="ou=People,dc=example,dc=com";
+$base_posix_groups="ou=groups,dc=gsr,dc=pt"; ❶



@@ -117,29 +117,30 @@
 ##############################################################################*/

 // path 2 the mkntpwd utility (Customize)
-$mkntpwdCommand = "./templates/creation/mkntpwd";
+$mkntpwdCommand = "/usr/sbin/smbldap-passwd"; ❷

 // Default domains definition (Customize)
 //   (use 'net getlocalsid' on samba server)
 $default_samba3_domains = array();
 $default_samba3_domains[] =
-        array(  'name'   => 'My Samba domain Name',
-                'sid' => 'S-1-5-21-479559372-1547523452-3818884970' );
+        array(  'name'   => 'GSRDOMAIN', ❸
+                'sid' => 'S-1-5-21-2817058862-34499604-3382793611' ); ❹

 // The base dn of samba group. (CUSTOMIZE)
-//$samba_base_groups = "ou=Groups,ou=samba,dc=example,dc=org";
+$samba_base_groups = "ou=groups,dc=gsr,dc=pt"; ❺


 //Definition of built-in local groups
-$built_in_local_groups = array( "S-1-5-32-544" => "Administrators",
-                                "S-1-5-32-545" => "Users",
-                                "S-1-5-32-546" => "Guests",
-                                "S-1-5-32-547" => "Power Users",
-                                "S-1-5-32-548" => "Account Operators",
-                                "S-1-5-32-549" => "Server Operators",
-                                "S-1-5-32-550" => "Print Operators",
-                                "S-1-5-32-551" => "backup Operators",
-                                "S-1-5-32-552" => "Replicator" );
+$built_in_local_groups = array(
+               "S-1-5-21-2817058862-34499604-3382793611-512" => "Administrators", ❻
+               "S-1-5-21-2817058862-34499604-3382793611-513" => "Users",
+               "S-1-5-21-2817058862-34499604-3382793611-514" => "Guests",
+               "S-1-5-21-2817058862-34499604-3382793611-21007" => "Power Users",
+               "S-1-5-21-2817058862-34499604-3382793611-21009" => "Account Operators",
+               "S-1-5-21-2817058862-34499604-3382793611-21011" => "Server Operators",
+               "S-1-5-21-2817058862-34499604-3382793611-21013" => "Print Operators",
+               "S-1-5-21-2817058862-34499604-3382793611-21015" => "backup Operators",
```

```
+                "S-1-5-21-2817058862-34499604-3382793611-21017" => "Replicator" );

 /*##############################################################################################
```

❶ Base de la unidad organizacional destinada al almacén de los grupos de usuarios.

❷ Localización de la herramienta mkntpwd. Esta herramienta la proveía IDEALX (http://samba.idealx.org/) con el paquete smbldap-tools (versión <=0.8.4).

Desde la versión 0.8.5 esta herramienta se ha sustituído por el módulo de perl *Crypt::SmbHash*. Por este motivo, a partir de ahora se puede hacer uso de la herramienta smbldap-passwd en su lugar.

> **Nota:** En el Apéndice H podrá ver la forma de instalar y configurar este conjunto de herramientas.

❸ Dominio que administra el servidor Samba.

❹ SID de la máquina donde se ejecuta Samba. (Vea el Ejemplo F-7 para saber como obtener este número).

❺ Base de la unidad organizacional destinada al almacén de los grupos de usuarios.

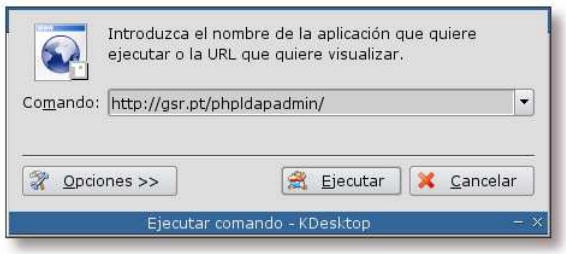
❻ Se modifican los gids que tienen por defecto los grupos listados y se adaptan a los gids de los grupos ya existentes en el sistema (si no existe algún grupo, puede crearlos en este momento, si lo desea).

El valor que se ha de añadir en cada uno de los grupos, es el valor del atributo *sambaSID* de los grupos en cuestión.

Acceso a la aplicación

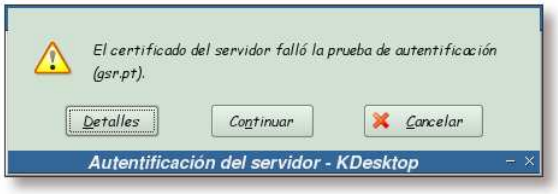
Realizadas las modificaciones de las secciones anteriores, ya se puede acceder a la aplicación, para ello puede teclear en su navegador favorito la URL: http://gsr.pt/phpldapadmin/ (sustituya el dominio por el que se adapte a su configuración).

Figura G-4. URL donde está instalado *phpLDAPadmin*



Si se encuentra en un entorno de escritorio con KDE, teclee **Alt**+**F2** e introduzca la dirección donde se encuentre instalado *phpLDAPadmin*.

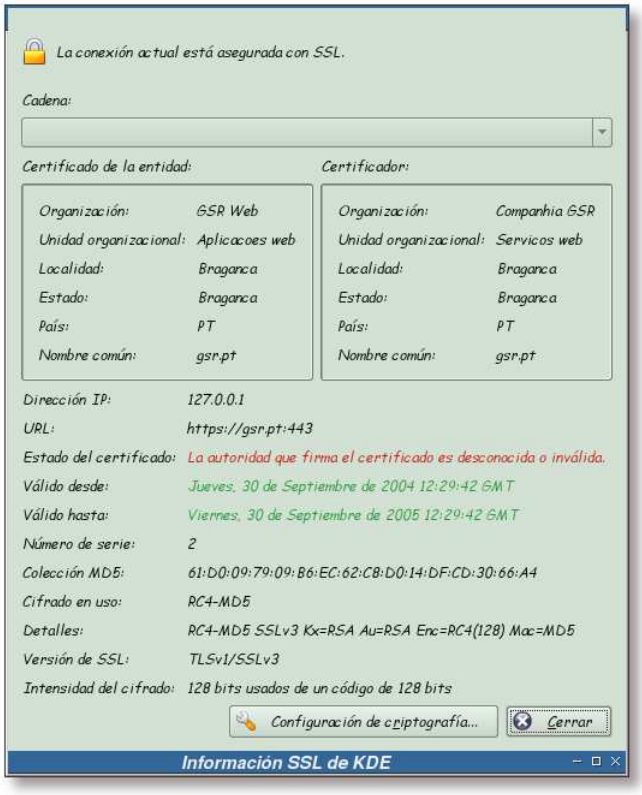
Figura G-5. Aviso acerca del certificado del servidor web I



Si ha configurado correctamente el servidor web, a la hora de acceder a la aplicación *phpLDAPadmin* por el protocolo *http*, Apache le tendría que redireccionar a la misma dirección, pero bajo el protocolo *https*.

Esto es lo que ha ocurrido en esta pantalla, Apache ha redirigido la petición realizada (http://gsr.pt/phpldapadmin/) hacia el protocolo *https*. Por este motivo, y debido a que la entidad certificadora que se ha creado es desconocida, sale este aviso. Pulse sobre el botón *Detalles* para obtener más información.

Figura G-6. Información SSL



En esta pantalla se muestra la información del certificado y la entidad certificadora que ha creado dicho certificado. Si se fija, aquí aparecerán los datos tecleados en el Apéndice I. Pulse sobre el botón *Cerrar* para continuar.

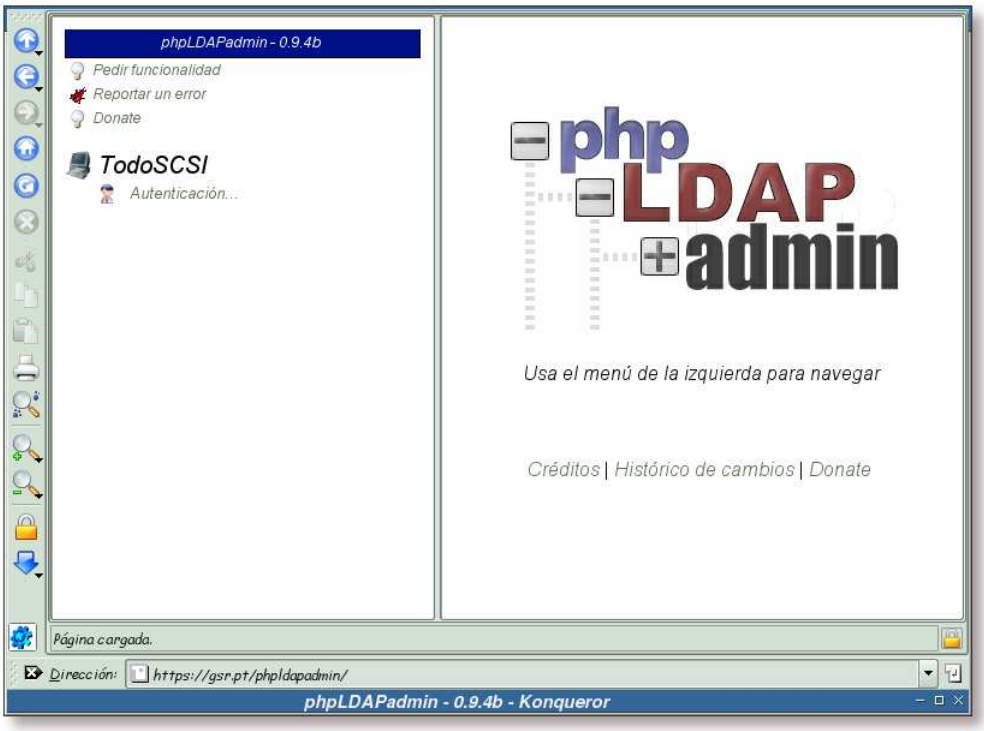
Figura G-7. Aviso acerca del certificado del servidor web II

Pulse ahora sobre el botón *Continuar* para seguir con la carga de la página.

Figura G-8. Período de aceptación del certificado

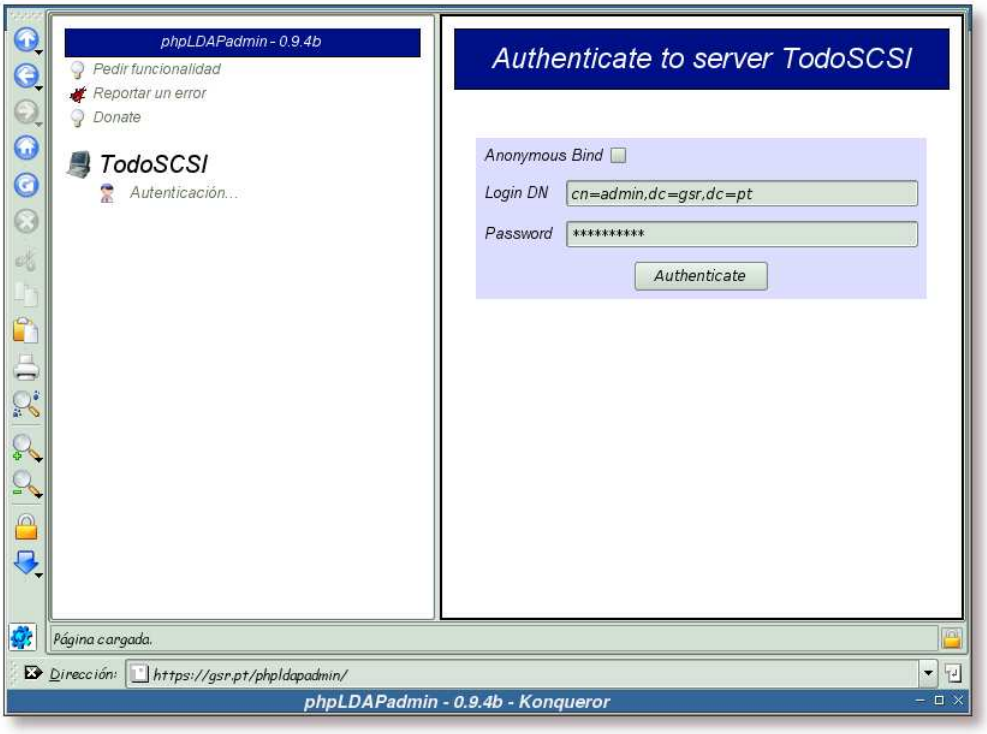
Seleccione la opción deseada y pulse sobre ella.

Figura G-9. Pantalla principal de *phpLDAPadmin*



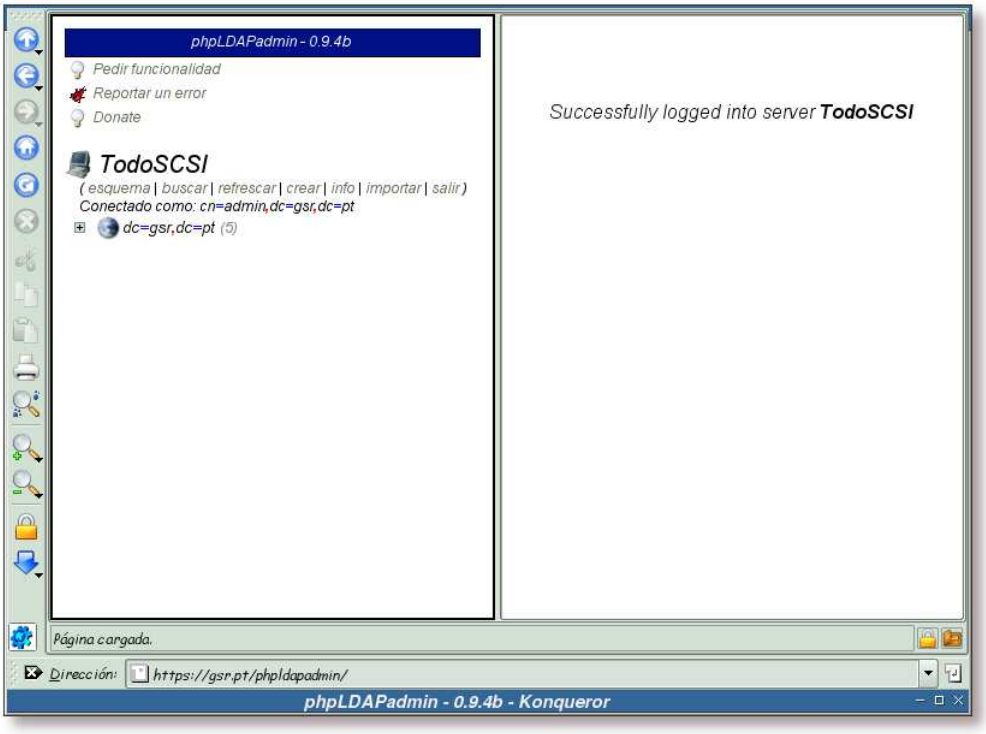
Pantalla principal de *phpLDAPadmin*, para poder administrar el directorio LDAP se ha de efectuar la autentificación. Esto se consigue pulsando sobre el enlace *Autenticación...*

Figura G-10. Autentificándose en *phpLDAPadmin*



Se teclea en el campo correspondiente el DN del usuario con el que quiera acceder al directorio LDAP (recuerde que por defecto aparecerá el usuario que haya tecleado en el archivo de configuración de *phpLDAPadmin*. En el siguiente enlace puede ver la opción referida anteriormente:
Usuario por defecto para el ingreso de phpLDAPadmin) y la clave para dicho usuario. Luego se procede a la autentificación, pulsando sobre el botón *Authenticate*.

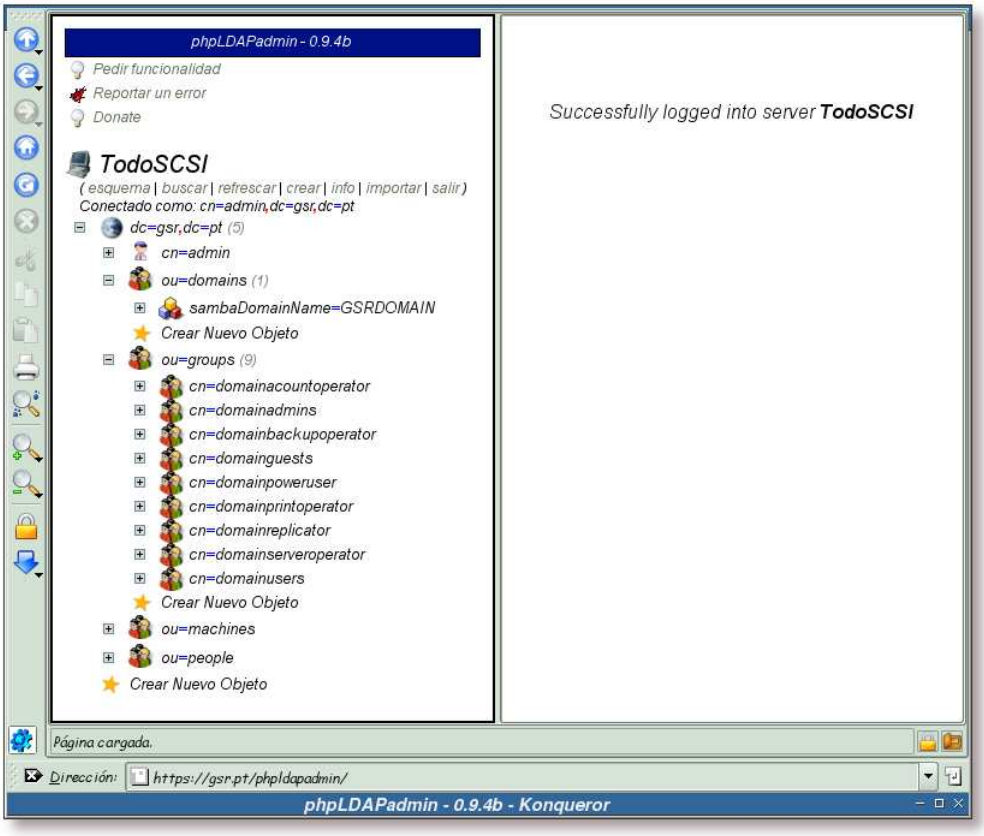
Figura G-11. Autentificación realizada con éxito



La aplicación informa de la correcta autentificación en el servidor LDAP.

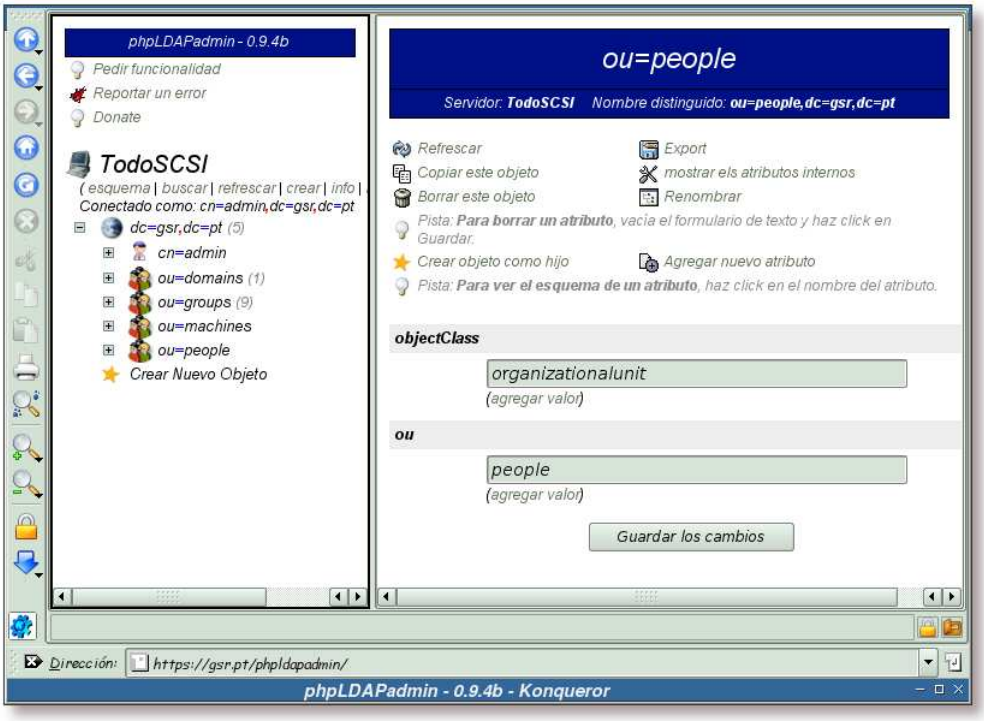
Como se puede ver en la imagen, una vez autentificado, la aplicación provee una serie de herramientas para la administración de un directorio LDAP. Estas comprenden desde el listado de los esquemas disponibles en el servidor LDAP, búsquedas, creación de nuevas entradas, información sobre el servidor hasta la posibilidad de importar archivos LDIF.

Figura G-12. Árbol de contenidos del directorio



Si se pulsa sobre el signo “+” que está a la izquierda de cada objeto, se puede ver los objetos hijos que este posee.

Figura G-13. Información sobre un objeto

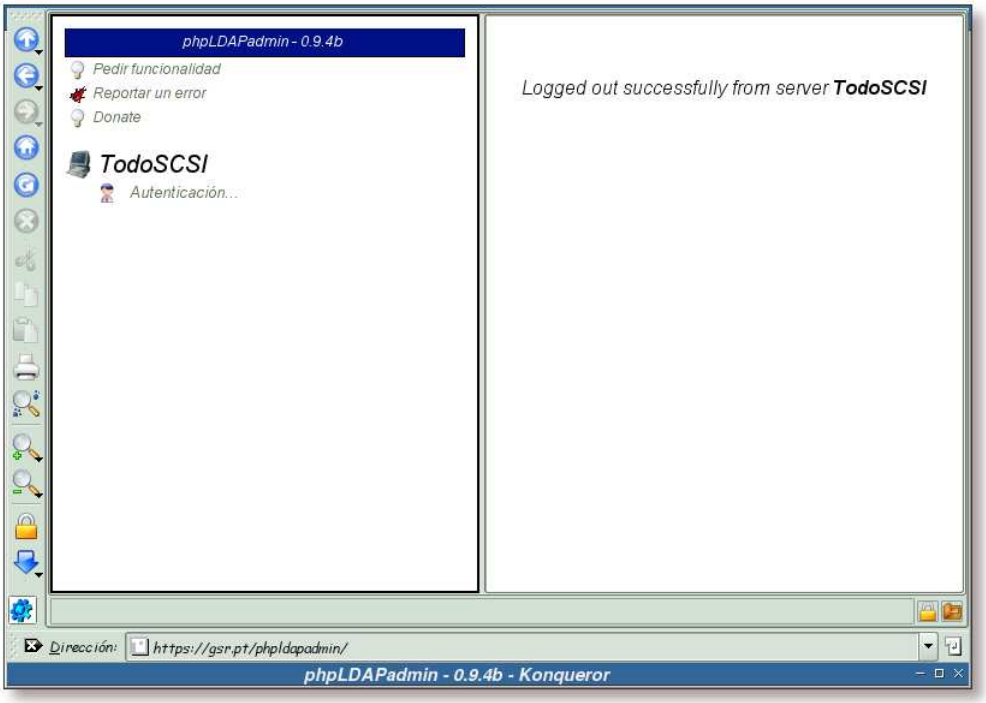


Si se pulsa sobre el nombre de un objeto, por ejemplo sobre *ou=people*, se puede ver la información almacenada en el mismo, así como proceder a su modificación.

Figura G-14. Creación de un nuevo objeto

phpLDAPadmin da la posibilidad de crear una serie de objetos predefinidos, ayudando sobremanera a la hora de administrar un servidor LDAP. En esta pantalla se pueden observar aquellos objetos para los que *phpLDAPadmin* posee plantillas.

Figura G-15. Finalizando la sesión



Una vez finalizado el trabajo con *phpLDAPadmin* se ha de finalizar la sesión, para ello se ha de pulsar sobre el enlace *salir*.

Apéndice H. Instalación y configuración de *smbldap-tools*

Introducción

Las herramientas que provee el paquete *smbldap-tools*, son un conjunto de scripts que se ejecutan sobre las herramientas de sistema *user{add,del,mod}* y *group{add,del,mod}* para permitir la manipulación de usuarios y grupos almacenados en un directorio LDAP, destinadas a sistemas DEN como Samba-LDAP y pam/nss_ldap.

Adicionalmente, se han diseñado algunos scripts para facilitar la migración de servidores PDC Windows NT 4.0 a servidores PDC Samba-LDAP. Estas son: smbldap-populate, smbldap-migrate-groups y smbldap-migrate-accounts.

La última versión de estas herramientas se encuentra en: http://samba.idealx.org/. La versión utilizada para realizar esta documentación ha sido la 0.8.5.

Instalación

Las herramientas diseñadas por *idealx* se encuentran en el paquete *smbldap-tools*, por lo que tendrá que teclear la siguiente orden para instalarlas:

Ejemplo H-1. Instalación del paquete *smbldap-tools*

```
# /usr/bin/apt-get install smbldap-tools
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  libconvert-asn1-perl libcrypt-smbhash-perl libdigest-md4-perl libnet-ldap-perl
Paquetes sugeridos:
  libio-socket-ssl-perl libxml-parser-perl libauthen-sasl-perl libxml-sax-perl
Se instalarán los siguientes paquetes NUEVOS:
  libconvert-asn1-perl libcrypt-smbhash-perl libdigest-md4-perl libnet-ldap-perl smbldap-tools
0 actualizados, 5 se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 0B/624kB de archivos.
Se utilizarán 1794kB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n]
Seleccionando el paquete libconvert-asn1-perl previamente no seleccionado.
(Leyendo la base de datos ...
133905 ficheros y directorios instalados actualmente.)
Desempaquetando libconvert-asn1-perl (de .../libconvert-asn1-perl_0.18-1_all.deb) ...
Seleccionando el paquete libdigest-md4-perl previamente no seleccionado.
Desempaquetando libdigest-md4-perl (de .../libdigest-md4-perl_1.1-2_i386.deb) ...
Seleccionando el paquete libnet-ldap-perl previamente no seleccionado.
Desempaquetando libnet-ldap-perl (de .../libnet-ldap-perl_0.3202-2_all.deb) ...
Seleccionando el paquete libcrypt-smbhash-perl previamente no seleccionado.
Desempaquetando libcrypt-smbhash-perl (de .../libcrypt-smbhash-perl_0.02-6_all.deb) ...
```

```
Seleccionando el paquete smbldap-tools previamente no seleccionado.
Desempaquetando smbldap-tools (de .../smbldap-tools_0.8.5-1_all.deb) ...
Configurando libconvert-asn1-perl (0.18-1) ...
Configurando libdigest-md4-perl (1.1-2) ...
Configurando libnet-ldap-perl (0.3202-2) ...
Configurando libcrypt-smbhash-perl (0.02-6) ...
Configurando smbldap-tools (0.8.5-1) ...

localepurge: checking system for new locale ...
localepurge: processing locale files ...
localepurge: processing man pages ...
```

Si desea ver la descripción del paquete que se acaba de instalar, teclee la orden:

Ejemplo H-2. Descripción del paquete *smbldap-tools*

```
# /usr/bin/apt-cache show smbldap-tools
Package: smbldap-tools
Priority: optional
Section: admin
Installed-Size: 600
Maintainer: Sergio Talens-Oliag <sto@debian.org>
Architecture: all
Version: 0.8.5-1
Depends: perl, libnet-ldap-perl, libcrypt-smbhash-perl
Filename: pool/main/s/smbldap-tools/smbldap-tools_0.8.5-1_all.deb
Size: 291454
MD5sum: 87dd4028958d8ef9f9e4bafdf1b4ae6d
Description: Scripts to manage Unix and Samba accounts stored on LDAP
 Set of scripts to manage data relative to users and groups stored in an LDAP
 server. The tools manage POSIX, shadow and Samba (3.0 series) accounts and
 groups.
 .
 This package is used to add/del/mod users and groups in the Linux
 Samba-OpenLDAP Howto <http://samba.idealx.org/smbldap-howto.en.html>.
```

Con la siguiente orden se observarán las herramientas que provee este paquete:

Ejemplo H-3. Herramientas que provee el paquete *smbldap-tools*

```
$ /usr/bin/dpkg -L smbldap-tools | /bin/grep bin
/usr/sbin/smbldap-groupadd
/usr/sbin/smbldap-groupdel
/usr/sbin/smbldap-groupmod
/usr/sbin/smbldap-groupshow
/usr/sbin/smbldap-passwd
/usr/sbin/smbldap-populate
/usr/sbin/smbldap-useradd
/usr/sbin/smbldap-userdel
/usr/sbin/smbldap-usermod
/usr/sbin/smbldap-usershow
```

Configuración

El primer paso para configurar estas herramientas, es copiar los archivos de configuración al directorio `/etc/smbldap-tools`. En el directorio `/usr/share/doc/smbldap-tools/examples/` hay archivos de configuración de ejemplo, y a partir de ellos se realizará la configuración. El siguiente ejemplo muestra como hacerlo.

Ejemplo H-4. Copiando los archivos de configuración de *smbldap-tools* a `/etc/smbldap-tools`

```
# /bin/cp -v \
            /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf /etc/smbldap-tools/
«/usr/share/doc/smbldap-tools/examples/smbldap_bind.conf» -> \
            «/etc/smbldap-tools/smbldap_bind.conf»
# /bin/zcat -v /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz > \
             /etc/smbldap-tools/smbldap.conf
/usr/share/doc/smbldap-tools/examples/smbldap.conf.gz:   62.8%
```

Ahora que ya están los archivos de configuración necesarios, sólo queda adaptarlos al sistema. En las siguientes secciones se verán las opciones más importantes de ambos archivos.

> **Nota:** En los apéndices: Apéndice AK y Apéndice AL posee un ejemplo de estos archivos ya configurados.

`/etc/smbldap-tools/smbldap_bind.conf`

- Usuario administrador del directorio LDAP.

  `masterDN="cn=admin,dc=gsr,dc=pt"`
- Clave del usuario administrador del servidor LDAP.

  `masterPw="**********"`

`/etc/smbldap-tools/smbldap.conf`

Sección general

- SID del servidor (en el siguiente enlace tiene un ejemplo de como obtenerlo: Ejemplo F-7).

  `SID="S-1-5-21-2817058862-34499604-3382793611"`

Sección LDAP

- Dirección del servidor LDAP.

```
masterLDAP="gsr.pt"
```

- Puerto por el que conectarse al servidor LDAP.

  ```
  masterPort="389"
  ```

- Se activa la conexión por TLS.

  ```
  ldapTLS="1"
  ```

- Se obliga a que el servidor LDAP provea un certificado y además, este certificado ha de ser válido.

  ```
  verify="require"
  ```

- Archivo del certificado de la CA.

  ```
  cafile="/etc/ldap/ssl/cacert.pem"
  ```

- Certificado que se utilizará para conectarse con el servidor LDAP.

  ```
  clientcert="/home/certs/ldap.cliente.cert.pem"
  ```

- Llave del certificado que se utilizará para conectarse con el servidor LDAP.

  ```
  clientkey="/home/certs/ldap.cliente.key.pem"
  ```

- Base del servidor LDAP.

  ```
  suffix="dc=gsr,dc=pt"
  ```

- Entidad bajo la cual se almacenarán los usuarios.

  ```
  usersdn="ou=people,${suffix}"
  ```

- Entidad bajo la cual se almacenarán los equipos.

  ```
  computersdn="ou=machines,${suffix}"
  ```

- Entidad bajo la cual se almacenarán los grupos.

  ```
  groupsdn="ou=groups,${suffix}"
  ```

- Algoritmo de hash para cifrar las claves.

  ```
  hash_encrypt="MD5"
  ```

Sección para las cuentas unix

- Shell por defecto para los nuevos usuarios.

  ```
  userLoginShell="/bin/bash"
  ```

- Directorio «home» de los usuarios (la variable *%U* se sustituirá por el nombre del usuario).

  ```
  userHome="/home/samba/users/%U"
  ```

- GID por defecto al que pertenecerán los nuevos usuarios (en este caso se ha elegido el grupo *domainusers*).

  ```
  defaultUserGid="1001"
  ```

- GID por defecto al que pertenecerán los nuevos equipos (en este caso se ha elegido el grupo *domainadmins*).

  ```
  defaultComputerGid="1000"
  ```

- Directorio desde el cual se copiarán los archivos de configuración por defecto de los nuevos usuarios (*directorio skel*).

  ```
  skeletonDir="/etc/skel"
  ```

Sección Samba

- Localización del *home* de los usuarios a través de Samba (la variable *%U* sustituye al nombre del usuario).

  > **Nota:** Si se quiere hacer uso de la directiva “logon home” del archivo de configuración de Samba, `smb.conf` y/o se quiere deshabilitar los perfiles móviles, deje esta variable en blanco.

  ```
  userSmbHome="\\TODOSCSI\%U"
  ```

- Localización de los perfiles de los usuarios a través de Samba (la variable *%U* sustituye al nombre del usuario).

  > **Nota:** Si se quiere hacer uso de la directiva “logon home” del archivo de configuración de Samba, `smb.conf` y/o se quiere deshabilitar los perfiles móviles, deje esta variable en blanco.

  ```
  userProfile="\\TODOSCSI\profiles\%U"
  ```

- Letra para mapear el directorio *home* del usuario.

  ```
  userHomeDrive="H:"
  ```

- Script *netlogon* por defecto (la variable *%U* sustituye al nombre del usuario).

  > **Nota:** Si la variable se deja en blanco, se utilizará automáticamente el script bajo el archivo `nombreusuario.cmd`.

  ```
  userScript=""
  ```

- Dominio que se añadirá al atributo “mail” de los usuarios, cuando se utiliza la orden **smbldap-useradd -M**.

  ```
  mailDomain="gsr.pt"
  ```

Apéndice I. Preparación de Apache para el uso de SSL

Introducción

En los ejemplos Ejemplo F-2, Ejemplo F-3, Ejemplo F-4 y Ejemplo F-5 se ha visto el proceso de instalación de Apache junto con el módulo “mod_ssl”, entre otros. Este apéndice abordará la creación de los certificados necesarios así como la configuración relativa al servidor web, para permitir conexiones SSL contra el servidor Apache.

Generación de la entidad certificadora y los certificados

A continuación se mostrará el proceso que se ha de seguir para la creación de la entidad certificadora y el certificado necesario para que el servidor Apache pueda servir páginas a través de SSL:

Ejemplo I-1. Creación del certificado para el servidor Apache

```
# /usr/bin/dpkg-reconfigure libapache-mod-ssl
What type of certificate do you want to create?

  1. dummy     (dummy self-signed Snake Oil cert)
  2. test      (test cert signed by Snake Oil CA)
  3. custom    (custom cert signed by own CA)
  4. existing  (existing cert)


Use  dummy     when you are a vendor package maintainer,
     test      when you are an admin but want to do tests only,
     custom    when you are an admin willing to run a real server
     existing  when you are an admin who upgrades a server.

Normally you would choose 2.

your choice: 3
Which algorithm should be used to generate required key(s)?

  1. RSA
  2. DSA

Normally you would choose 1.

your choice: 1
SSL Certificate Generation Utility (mkcert.sh)
Copyright (c) 1998-2000 Ralf S. Engelschall, All Rights Reserved.

Generating custom certificate signed by own CA [CUSTOM]
```

```
STEP 1: Generating RSA private key for CA (1024 bit) [ca.key]
2477870 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....++++++
.......................................++++++
e is 65537 (0x10001)
```

```
STEP 2: Generating X.509 certificate signing request for CA [ca.csr]
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
1. Country Name             (2 letter code) [XY]:PT
2. State or Province Name   (full name)     [Snake Desert]:Braganca
3. Locality Name            (eg, city)      [Snake Town]:Braganca
4. Organization Name        (eg, company)   [Snake Oil, Ltd]:Companhia GSR
5. Organizational Unit Name (eg, section)   [Certificate Authority]:Servicos web
6. Common Name              (eg, CA name)   [Snake Oil CA]:gsr.pt
7. Email Address            (eg, name@FQDN) [ca@snakeoil.dom]:sergio@gsr.pt
8. Certificate Validity     (days)          [365]: [Enter]
```

```
STEP 3: Generating X.509 certificate for CA signed by itself [ca.crt]
Certificate Version (1 or 3) [3]:3
Signature ok
subject=/C=PT/ST=Braganca/L=Braganca/O=Companhia \
                                GSR/OU=Servicos web/CN=gsr.pt/emailAddress=sergio@gsr.pt
Getting Private key
Verify: matching certificate & key modulus
Verify: matching certificate signature
/etc/apache/ssl.crt/ca.crt: /C=PT/ST=Braganca/L=Braganca/O=Companhia \
                                GSR/OU=Servicos web/CN=gsr.pt/emailAddress=sergio@gsr.pt
error 18 at 0 depth lookup:self signed certificate
OK
```

```
STEP 4: Generating RSA private key for SERVER (1024 bit) [server.key]
2477870 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
........++++++
......++++++
e is 65537 (0x10001)
```

```
STEP 5: Generating X.509 certificate signing request for SERVER [server.csr]
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
1. Country Name             (2 letter code) [XY]:PT
2. State or Province Name   (full name)     [Snake Desert]:Braganca
3. Locality Name            (eg, city)      [Snake Town]:Braganca
4. Organization Name        (eg, company)   [Snake Oil, Ltd]:GSR Web
5. Organizational Unit Name (eg, section)   [Webserver Team]:Aplicacoes web
6. Common Name              (eg, FQDN)      [www.snakeoil.dom]:gsr.pt
7. Email Address            (eg, name@fqdn) [www@snakeoil.dom]:sergio@gsr.pt
8. Certificate Validity     (days)          [365]:[Enter]
```

```
STEP 6: Generating X.509 certificate signed by own CA [server.crt]
Certificate Version (1 or 3) [3]:3
Signature ok
subject=/C=PT/ST=Braganca/L=Braganca/O=GSR Web/OU=Aplicacoes \
                                        web/CN=gsr.pt/emailAddress=sergio@gsr.pt
Getting CA Private Key
Verify: matching certificate & key modulus
Verify: matching certificate signature
/etc/apache/ssl.crt/server.crt: OK
```

```
STEP 7: Enrypting RSA private key of CA with a pass phrase for security [ca.key]
The contents of the ca.key file (the generated private key) has to be
kept secret. So we strongly recommend you to encrypt the server.key file
with a Triple-DES cipher and a Pass Phrase.
Encrypt the private key now? [Y/n]: n ❶
Warning, you're using an unencrypted private key.
Please notice this fact and do this on your own risk.
```

```
STEP 8: Enrypting RSA private key of SERVER with a pass phrase for security [server.key]
The contents of the server.key file (the generated private key) has to be
kept secret. So we strongly recommend you to encrypt the server.key file
with a Triple-DES cipher and a Pass Phrase.
Encrypt the private key now? [Y/n]: n ❷
Warning, you're using an unencrypted RSA private key.
Please notice this fact and do this on your own risk.
```

```
RESULT: CA and Server Certification Files

o  /etc/apache/ssl.key/ca.key
   The PEM-encoded RSA private key file of the CA which you can
   use to sign other servers or clients. KEEP THIS FILE PRIVATE!

o  /etc/apache/ssl.crt/ca.crt
   The PEM-encoded X.509 certificate file of the CA which you use to
   sign other servers or clients. When you sign clients with it (for
```

```
   SSL client authentication) you can configure this file with the
   'SSLCACertificateFile' directive.

o  /etc/apache/ssl.key/server.key
   The PEM-encoded RSA private key file of the server which you configure
   with the 'SSLCertificateKeyFile' directive (automatically done
   when you install via APACI). KEEP THIS FILE PRIVATE!

o  /etc/apache/ssl.crt/server.crt
   The PEM-encoded X.509 certificate file of the server which you configure
   with the 'SSLCertificateFile' directive (automatically done
   when you install via APACI).

o  /etc/apache/ssl.csr/server.csr
   The PEM-encoded X.509 certificate signing request of the server file which
   you can send to an official Certificate Authority (CA) in order
   to request a real server certificate (signed by this CA instead
   of our own CA) which later can replace the /etc/apache/ssl.crt/server.crt
   file.

Congratulations that you establish your server with real certificates.

./snakeoil-ca-rsa.crt ... e52d41d0.0
./ca-bundle.crt ... Skipped
./gsr-ca-rsa.crt ... c43c023d.0
./snakeoil-dsa.crt ... 5d8360e1.0
./snakeoil-rsa.crt ... 82ab5372.0
./ca.crt ... 458c23d7.0
./server.crt ... 6219a630.0
./snakeoil-ca-dsa.crt ... 0cf14d7d.0
```

❶❷ Como se está trabajando sobre un equipo destinado a pruebas, se ha decidido no cifrar las llaves generadas, de esta forma se evitará el teclear la clave empleada en el cifrado cada vez que se reinicie el servidor Apache. ¡Esto es un problema muy grabe de seguridad! si está trabajando sobre un servidor en producción, es más que recomendable hacer uso del cifrado en estos puntos.

Configuración de Apache

Para añadir soporte SSL a Apache, no basta únicamente con crear el certificado, también hay que indicar a Apache donde se encuentra dicho certificado.

En primer lugar, se copiará un archivo de ejemplo de configuración del módulo *mod_ssl*, distribuído con el paquete *libapache-mod-ssl*, y se personalizará. Siga las siguientes indicaciones:

Ejemplo I-2. Preparación para la configuración del módulo *mod_ssl* de Apache

```
# /bin/cp -v /usr/share/doc/libapache-mod-ssl/examples/mod-ssl.conf \
/etc/apache/conf.d/mod_ssl-00-global.conf
«/usr/share/doc/libapache-mod-ssl/examples/mod-ssl.conf» -> «/etc/apache/conf.d/mod_ssl-00-global.c
# /bin/chmod -v 644 mod_ssl-00-global.conf
```

```
el modo de «mod_ssl-00-global.conf» cambia a 0644 (rw-r--r--)
```

Ahora edite el archivo `/etc/apache/conf.d/mod_ssl-00-global.conf` y comente las siguientes líneas:

```
Listen   80

SSLSessionCache   none
```

y descomente estas otras:

```
#SSLSessionCache         dbm:/var/run/mod_ssl_scache
#SSLSessionCacheTimeout  300

#SSLLog /var/log/apache/ssl_engine.log
#SSLLogLevel info
```

> **Nota:** En el Apéndice AM se encuentra un archivo de configuración completo.

Configuración de los *virtual host*

Ahora se creará la configuración personalizada para cada “virtual host”. En la actualidad existen dos “virtual host” en el equipo: uno denominado *gsr.pt:80* y otro *gsr.pt:443*.

La configuración de los “virtual host” se almacenará en el archivo `/etc/apache/conf.d/vhost.conf`. Aquí no se tratará el contenido de este archivo, ya que posee un archivo de configuración completo en el Apéndice AN.

Esto es suficiente para habilitar el soporte SSL en Apache. Ahora se ha de reiniciar Apache, para ello teclee:

Ejemplo I-3. Reinicio del servidor Apache

```
# /etc/init.d/apache restart
Restarting apache.
```

Apéndice J. Cambio para el registro de Windows XP (miembro de un dominio Samba)

Para poder añadir un cliente Windows XP a un dominio administrado por Samba, es necesario aplicar el siguiente cambio en el registro de Windows:

```
Windows Registry Editor Version 5.00

;
; This registry key is needed for a Windows XP Client to join
; and logon to a Samba domain. Note: Samba 2.2.3a contained
; this key in a broken format which did nothing to the registry -
; however XP reported "registry key imported". If in doubt
; check the key by hand with regedit.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
"requiresignorseal"=dword:00000000
```

> **Nota:** El cambio a realizar se ha obtenido de los archivos suministrados con el paquete *samba-doc*, más concretamente el archivo `/usr/share/doc/samba-doc/registry/WinXP_SignOrSeal.reg`

Apéndice K. Script para la creación/eliminación de los homes de los usuarios

Cuando se añaden/borran usuarios en la base de datos de LDAP no se crea el directorio destinado a almacenar sus archivos personales (el directorio *HOME*). La aplicación LDAP Account Manager (ver el Apéndice F para más información) adjunta un script destinado a la creación/eliminación de los directorios home de los usuarios: lamdaemon.pl; pero en esta documentación no se hará uso del mismo.

En su lugar se ha creado el siguiente script, que ha de ser ejecutado como usuario root cada vez que se cree un nuevo usuario, sobre todo si este está destinado a hacer uso de Samba (la creación del directorio home cuando se accede a la shell ya está solucionado: vea la la sección de nombre `/etc/pam.d/common-session` en Capítulo 5 para más detalles):

Nota: El script no está pensado para sistemas en producción, simplemente es un ejemplo utilizado para facilitar la creación de esta documentación.

Aviso

Tenga mucho cuidado con el uso del siguiente script, ya que añade y borra, ¡sin preguntar!, los homes de los usuarios en relación al estado de la base de datos de usuarios LDAP.

Su comportamiento es el siguiete:

- Crea el directorio home y copia el contenido del directorio `/etc/skel`, de aquellos usuarios que no tengan creado su directorio home.
- Borra, sin preguntar ni hacer una copia de seguridad, los homes de los usuarios que ya no existan en la base de datos LDAP, pero aun posean un directorio home en el sistem.

Nota: Este script se ha basado en los scripts creados por J. Vriesman y Jesús Roncero Franco para la elaboración de los siguientes documentos, respectivamente:

- http://jeroen.protheus.com/postfix-courier-ldap-howto.html
- http://bulma.net/body.phtml?nIdNoticia=2013

```
#!/bin/sh
#
# Copyright (C) 2004 Sergio González González <sergio.gonzalez@hispalinux.es>
#
# Depends on:
#               - ldapsearch
#
# Based on http://jeroen.protheus.com/postfix-courier-ldap-howto.html
```

```
# (c) J.Vriesman
#
# and
#
# Based on http://bulma.net/body.phtml?nIdNoticia=2013
# (c) Jesús Roncero Franco
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
#
#
# This script manage the home directories of LDAP users (make the new users home
# directory and delete the non-existent users home directory)



# Password to bind to ldap server
systempass="********"
# Bind dn
binddn="cn=admin,dc=gsr,dc=pt"
# Acount leave
accountleave="ou=people,dc=gsr,dc=pt"
# ldap host
ldaphost="gsr.pt"
# skel directory
skel="/etc/skel/"
# Home leave (without final slash: '/')
homeleave="/home/samba/users"


usernames=‘ldapsearch -h $ldaphost -x -w $systempass -D "$binddn" \
                      -b "$accountleave" uid | grep "^[^#]" | grep "^[^dn]" \
                      | grep uid | awk '{ print $2 }''

# create personal home directories

for username in $usernames
do
  homedirectory=‘ldapsearch -h $ldaphost -x -w $systempass -D "$binddn" \
                            -b "$accountleave" "(uid=$username)" homeDirectory \
                            | grep "^[^#]" | grep homeDirectory \
                            | awk '{ print $2 }''
```

```
  group=‘ldapsearch -h $ldaphost -x -w $systempass -D "$binddn" \
                    -b "$accountleave" "(uid=$username)" gidNumber \
                    | grep "^[^#]" | grep gidNumber \
                    | awk ’{ print $2 }’‘

  if [ ! -d $homedirectory ] && [ ! -z $homedirectory ]
  then

    cp -a $skel $homedirectory
    chown -R $username.$group $homedirectory
  fi

done

# delete personal home directories

for username in ‘ls $homeleave‘
do
  name=‘ldapsearch -h $ldaphost -x -w $systempass -D "$binddn" \
                   -b "$accountleave" "(homeDirectory=$homeleave/$username)" uid \
                   | grep "^[^#]" | grep "uid:" | awk ’{ print $2 }’‘

  if [ -z $name ]
  then
    rm -rf $homeleave/$username
  fi
done
```

Apéndice L. Script para convertir a mayúsculas el archivo pasado como argumento

El script que se lista a continuación, convierte el archivo pasado como argumento a mayúsculas.

> **Nota:** Este script se ha adaptado a partir del archivo de ejemplo `/usr/share/doc/bash/examples/scripts.v2/lowercase` que se distribuye con el paquete *bash*.

```
#! /bin/bash
#
# original from
# @(#) lowercase.ksh 1.0 92/10/08
# 92/10/08 john h. dubois iii (john@armory.com)
#
# conversion to bash v2 syntax done by Chet Ramey
#
# Convert to uppercase by Sergio González González
#

Usage="Usage: $name file ..."
phelp()
{
echo "$name: change filenames to upper case.
$Usage
Each file is moved to a name with the same directory component, if any,
and with a filename component that is the same as the original but with
any lower case letters changed to upper case."
}

name=${0##*/}

while getopts "h" opt; do
 case "$opt" in
 h) phelp; exit 0;;
 *) echo "$Usage" 1>&2; exit 2;;
 esac
done

shift $((OPTIND - 1))

for file; do
    filename=${file##*/}
    case "$file" in
    */*)    dirname=${file%/*} ;;
    *)    dirname=. ;;
    esac
    nf=$(echo $filename | tr a-z A-Z)
    newname="${dirname}/${nf}"
    if [ "$nf" != "$filename" ]; then
```

```
 mv "$file" "$newname"
 echo "$0: $file -> $newname"
    else
 echo "$0: $file not changed."
    fi
done
```

Apéndice M. Script para mover los controladores PostScript de Adobe al directorio `/usr/share/cups/drivers`

El script que se lista a continuación, mueve los controladores PostScript de Adobe necesarios al directorio `/usr/share/cups/drivers`.

```
#!/bin/bash

ARCHIVOS="ADFONTS.MFM
ADOBEPS4.DRV
ADOBEPS4.HLP
DEFPRTR2.PPD
ICONLIB.DLL
PSMON.DLL
ADOBEPS5.DLL
ADOBEPSU.DLL
ADOBEPSU.HLP"

for x in $ARCHIVOS
do
 find ‘pwd‘ -name "$x" -exec /bin/cp -vf {} /usr/share/cups/drivers \;
done

chmod -v 644 /usr/share/cups/drivers/*
```

Apéndice N. Salida de la ejecución de la orden /usr/sbin/cupsaddsmb -v -U root -a

Nota: Las líneas se han cortado para aumentar la legibilidad

```
$ /usr/sbin/cupsaddsmb -v -U root -a
Password for root required to access localhost via SAMBA: [Clave]

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                         -c 'mkdir W32X86;put /var/tmp/40d05d8c7eb4b \
                         W32X86/InyeccionBN.ppd;put \
                         /usr/share/cups/drivers/cupsdrv5.dll \
                         W32X86/cupsdrv5.dll;put \
                         /usr/share/cups/drivers/cupsui5.dll \
                         W32X86/cupsui5.dll;put \
                         /usr/share/cups/drivers/cups5.hlp \
                         W32X86/cups5.hlp'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \W32X86
putting file /var/tmp/40d05d8c7eb4b as \W32X86/InyeccionBN.ppd \
                           (1571,5 kb/s) (average 1571,5 kb/s)
putting file /usr/share/cups/drivers/cupsdrv5.dll as \W32X86/cupsdrv5.dll \
                           (3041,1 kb/s) (average 2963,8 kb/s)
putting file /usr/share/cups/drivers/cupsui5.dll as \W32X86/cupsui5.dll \
                           (2646,8 kb/s) (average 2817,9 kb/s)
putting file /usr/share/cups/drivers/cups5.hlp as \W32X86/cups5.hlp \
                           (3475,0 kb/s) (average 2832,5 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                         -c 'adddriver "Windows NT x86" \
                         "InyeccionBN:cupsdrv5.dll:InyeccionBN.ppd:\
                          cupsui5.dll:cups5.hlp:NULL:RAW:NULL"'
Printer Driver InyeccionBN successfully installed.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                         -c 'mkdir WIN40;put /var/tmp/40d05d8c7eb4b \
                         WIN40/InyeccionBN.PPD;put \
                         /usr/share/cups/drivers/ADFONTS.MFM \
                         WIN40/ADFONTS.MFM;put \
                         /usr/share/cups/drivers/ADOBEPS4.DRV \
                         WIN40/ADOBEPS4.DRV;put \
                         /usr/share/cups/drivers/ADOBEPS4.HLP \
                         WIN40/ADOBEPS4.HLP;put \
                         /usr/share/cups/drivers/DEFPRTR2.PPD \
                         WIN40/DEFPRTR2.PPD;put \
                         /usr/share/cups/drivers/ICONLIB.DLL \
                         WIN40/ICONLIB.DLL;put \
                         /usr/share/cups/drivers/PSMON.DLL \
```

```
                          WIN40/PSMON.DLL;'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \WIN40
putting file /var/tmp/40d05d8c7eb4b as \WIN40/InyeccionBN.PPD \
                           (1571,5 kb/s) (average 1571,5 kb/s)
putting file /usr/share/cups/drivers/ADFONTS.MFM as \WIN40/ADFONTS.MFM \
                           (3722,4 kb/s) (average 3653,5 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.DRV as \WIN40/ADOBEPS4.DRV \
                           (4838,3 kb/s) (average 4396,1 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.HLP as \WIN40/ADOBEPS4.HLP \
                           (3019,2 kb/s) (average 4161,2 kb/s)
putting file /usr/share/cups/drivers/DEFPRTR2.PPD as \WIN40/DEFPRTR2.PPD \
                           (4389,2 kb/s) (average 4162,5 kb/s)
putting file /usr/share/cups/drivers/ICONLIB.DLL as \WIN40/ICONLIB.DLL \
                           (1774,8 kb/s) (average 3891,2 kb/s)
putting file /usr/share/cups/drivers/PSMON.DLL as \WIN40/PSMON.DLL \
                           (1098,0 kb/s) (average 3662,5 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'adddriver "Windows 4.0" \
                          "InyeccionBN:ADOBEPS4.DRV:InyeccionBN.PPD:NULL:\
                           ADOBEPS4.HLP:PSMON.DLL:RAW:ADOBEPS4.DRV,\
                           InyeccionBN.PPD,ADOBEPS4.HLP,PSMON.DLL, \
                           ADFONTS.MFM,DEFPRTR2.PPD,ICONLIB.DLL"'
Printer Driver InyeccionBN successfully installed.

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'setdriver InyeccionBN InyeccionBN'
Succesfully set InyeccionBN to driver InyeccionBN.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                          -c 'mkdir W32X86;put /var/tmp/40d05d92939de \
                          W32X86/InyeccionColor.ppd;put \
                          /usr/share/cups/drivers/cupsdrv5.dll \
                          W32X86/cupsdrv5.dll;put \
                          /usr/share/cups/drivers/cupsui5.dll \
                          W32X86/cupsui5.dll;put \
                          /usr/share/cups/drivers/cups5.hlp \
                          W32X86/cups5.hlp'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \W32X86
putting file /var/tmp/40d05d92939de as \W32X86/InyeccionColor.ppd \
                             (982,2 kb/s) (average 982,2 kb/s)
putting file /usr/share/cups/drivers/cupsdrv5.dll as \W32X86/cupsdrv5.dll \
                            (3146,0 kb/s) (average 2963,8 kb/s)
putting file /usr/share/cups/drivers/cupsui5.dll as \W32X86/cupsui5.dll \
                            (2713,9 kb/s) (average 2850,3 kb/s)
putting file /usr/share/cups/drivers/cups5.hlp as \W32X86/cups5.hlp \
                            (2316,7 kb/s) (average 2832,5 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'adddriver "Windows NT x86" \
                          "InyeccionColor:cupsdrv5.dll:\
```

```
                            InyeccionColor.ppd:cupsui5.dll:\
                            cups5.hlp:NULL:RAW:NULL"'
Printer Driver InyeccionColor successfully installed.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                           -c 'mkdir WIN40;put /var/tmp/40d05d92939de \
                           WIN40/InyeccionColor.PPD;put \
                           /usr/share/cups/drivers/ADFONTS.MFM \
                           WIN40/ADFONTS.MFM;put \
                           /usr/share/cups/drivers/ADOBEPS4.DRV \
                           WIN40/ADOBEPS4.DRV;put \
                           /usr/share/cups/drivers/ADOBEPS4.HLP \
                           WIN40/ADOBEPS4.HLP;put \
                           /usr/share/cups/drivers/DEFPRTR2.PPD \
                           WIN40/DEFPRTR2.PPD;put \
                           /usr/share/cups/drivers/ICONLIB.DLL \
                           WIN40/ICONLIB.DLL;put \
                           /usr/share/cups/drivers/PSMON.DLL \
                           WIN40/PSMON.DLL;'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \WIN40
putting file /var/tmp/40d05d92939de as \WIN40/InyeccionColor.PPD \
                              (1964,3 kb/s) (average 1964,4 kb/s)
putting file /usr/share/cups/drivers/ADFONTS.MFM as \WIN40/ADFONTS.MFM \
                              (4043,8 kb/s) (average 3985,6 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.DRV as \WIN40/ADOBEPS4.DRV \
                              (4432,3 kb/s) (average 4283,4 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.HLP as \WIN40/ADOBEPS4.HLP \
                              (2917,5 kb/s) (average 4048,7 kb/s)
putting file /usr/share/cups/drivers/DEFPRTR2.PPD as \WIN40/DEFPRTR2.PPD \
                              (2633,5 kb/s) (average 4035,2 kb/s)
putting file /usr/share/cups/drivers/ICONLIB.DLL as \WIN40/ICONLIB.DLL \
                              (1831,1 kb/s) (average 3798,2 kb/s)
putting file /usr/share/cups/drivers/PSMON.DLL as \WIN40/PSMON.DLL \
                              (5090,9 kb/s) (average 3822,0 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                           -c 'adddriver "Windows 4.0" \
                           "InyeccionColor:ADOBEPS4.DRV:InyeccionColor.PPD:\
                            NULL:ADOBEPS4.HLP:PSMON.DLL:RAW:ADOBEPS4.DRV,\
                            InyeccionColor.PPD,ADOBEPS4.HLP,PSMON.DLL,\
                            ADFONTS.MFM,DEFPRTR2.PPD,ICONLIB.DLL"'
Printer Driver InyeccionColor successfully installed.

Running command: rpcclient localhost -N -U'root%1' \
                           -c 'setdriver InyeccionColor InyeccionColor'
Succesfully set InyeccionColor to driver InyeccionColor.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                           -c 'mkdir W32X86;put /var/tmp/40d05d96c0f3a \
                           W32X86/LaserBN.ppd;put \
                           /usr/share/cups/drivers/cupsdrv5.dll \
                           W32X86/cupsdrv5.dll;put \
```

```
                          /usr/share/cups/drivers/cupsui5.dll \
                          W32X86/cupsui5.dll;put \
                          /usr/share/cups/drivers/cups5.hlp \
                          W32X86/cups5.hlp'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \W32X86
putting file /var/tmp/40d05d96c0f3a as \W32X86/LaserBN.ppd \
                          (1571,5 kb/s) (average 1571,5 kb/s)
putting file /usr/share/cups/drivers/cupsdrv5.dll as \W32X86/cupsdrv5.dll \
                          (2975,0 kb/s) (average 2902,6 kb/s)
putting file /usr/share/cups/drivers/cupsui5.dll as \W32X86/cupsui5.dll \
                          (2614,6 kb/s) (average 2770,7 kb/s)
putting file /usr/share/cups/drivers/cups5.hlp as \W32X86/cups5.hlp \
                          (3475,0 kb/s) (average 2786,1 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'adddriver "Windows NT x86" \
                          "LaserBN:cupsdrv5.dll:LaserBN.ppd:\
                           cupsui5.dll:cups5.hlp:NULL:RAW:NULL"'
Printer Driver LaserBN successfully installed.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                          -c 'mkdir WIN40;put /var/tmp/40d05d96c0f3a \
                          WIN40/LaserBN.PPD;put \
                          /usr/share/cups/drivers/ADFONTS.MFM \
                          WIN40/ADFONTS.MFM;put \
                          /usr/share/cups/drivers/ADOBEPS4.DRV \
                          WIN40/ADOBEPS4.DRV;put \
                          /usr/share/cups/drivers/ADOBEPS4.HLP \
                          WIN40/ADOBEPS4.HLP;put \
                          /usr/share/cups/drivers/DEFPRTR2.PPD \
                          WIN40/DEFPRTR2.PPD;put \
                          /usr/share/cups/drivers/ICONLIB.DLL \
                          WIN40/ICONLIB.DLL;put \
                          /usr/share/cups/drivers/PSMON.DLL \
                          WIN40/PSMON.DLL;'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \WIN40
putting file /var/tmp/40d05d96c0f3a as \WIN40/LaserBN.PPD \
                          (1964,3 kb/s) (average 1964,4 kb/s)
putting file /usr/share/cups/drivers/ADFONTS.MFM as \WIN40/ADFONTS.MFM \
                          (4043,8 kb/s) (average 3985,6 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.DRV as \WIN40/ADOBEPS4.DRV \
                          (4282,5 kb/s) (average 4185,8 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.HLP as \WIN40/ADOBEPS4.HLP \
                          (2596,6 kb/s) (average 3890,9 kb/s)
putting file /usr/share/cups/drivers/DEFPRTR2.PPD as \WIN40/DEFPRTR2.PPD \
                          (2633,5 kb/s) (average 3879,4 kb/s)
putting file /usr/share/cups/drivers/ICONLIB.DLL as \WIN40/ICONLIB.DLL \
                          (1774,8 kb/s) (average 3654,8 kb/s)
putting file /usr/share/cups/drivers/PSMON.DLL as \WIN40/PSMON.DLL \
                          (1076,9 kb/s) (average 3452,0 kb/s)
```

```
Running command: rpcclient localhost -N -U'root%1' \
                          -c 'adddriver "Windows 4.0" \
                          "LaserBN:ADOBEPS4.DRV:LaserBN.PPD:NULL:\
                           ADOBEPS4.HLP:PSMON.DLL:RAW:ADOBEPS4.DRV,\
                           LaserBN.PPD,ADOBEPS4.HLP,PSMON.DLL,\
                           ADFONTS.MFM,DEFPRTR2.PPD,ICONLIB.DLL"'
Printer Driver LaserBN successfully installed.

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'setdriver LaserBN LaserBN'
Succesfully set LaserBN to driver LaserBN.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                          -c 'mkdir W32X86;put /var/tmp/40d05d9b3e1a0 \
                          W32X86/LaserColor.ppd;put \
                          /usr/share/cups/drivers/cupsdrv5.dll \
                          W32X86/cupsdrv5.dll;put \
                          /usr/share/cups/drivers/cupsui5.dll \
                          W32X86/cupsui5.dll;put \
                          /usr/share/cups/drivers/cups5.hlp \
                          W32X86/cups5.hlp'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \W32X86
putting file /var/tmp/40d05d9b3e1a0 as \W32X86/LaserColor.ppd \
                          (1309,5 kb/s) (average 1309,6 kb/s)
putting file /usr/share/cups/drivers/cupsdrv5.dll as \W32X86/cupsdrv5.dll \
                          (2709,9 kb/s) (average 2631,4 kb/s)
putting file /usr/share/cups/drivers/cupsui5.dll as \W32X86/cupsui5.dll \
                          (2614,6 kb/s) (average 2624,1 kb/s)
putting file /usr/share/cups/drivers/cups5.hlp as \W32X86/cups5.hlp \
                          (3475,0 kb/s) (average 2641,7 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'adddriver "Windows NT x86" \
                          "LaserColor:cupsdrv5.dll:LaserColor.ppd:\
                           cupsui5.dll:cups5.hlp:NULL:RAW:NULL"'
Printer Driver LaserColor successfully installed.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                          -c 'mkdir WIN40;put /var/tmp/40d05d9b3e1a0 \
                          WIN40/LaserColor.PPD;put \
                          /usr/share/cups/drivers/ADFONTS.MFM \
                          WIN40/ADFONTS.MFM;put \
                          /usr/share/cups/drivers/ADOBEPS4.DRV \
                          WIN40/ADOBEPS4.DRV;put \
                          /usr/share/cups/drivers/ADOBEPS4.HLP \
                          WIN40/ADOBEPS4.HLP;put \
                          /usr/share/cups/drivers/DEFPRTR2.PPD \
                          WIN40/DEFPRTR2.PPD;put \
                          /usr/share/cups/drivers/ICONLIB.DLL \
                          WIN40/ICONLIB.DLL;put \
                          /usr/share/cups/drivers/PSMON.DLL \
                          WIN40/PSMON.DLL;'
```

```
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \WIN40
putting file /var/tmp/40d05d9b3e1a0 as \WIN40/LaserColor.PPD \
                          (1964,3 kb/s) (average 1964,4 kb/s)
putting file /usr/share/cups/drivers/ADFONTS.MFM as \WIN40/ADFONTS.MFM \
                          (4043,8 kb/s) (average 3985,6 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.DRV as \WIN40/ADOBEPS4.DRV \
                          (4694,9 kb/s) (average 4449,3 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.HLP as \WIN40/ADOBEPS4.HLP \
                          (2950,6 kb/s) (average 4186,1 kb/s)
putting file /usr/share/cups/drivers/DEFPRTR2.PPD as \WIN40/DEFPRTR2.PPD \
                          (3291,9 kb/s) (average 4179,0 kb/s)
putting file /usr/share/cups/drivers/ICONLIB.DLL as \WIN40/ICONLIB.DLL \
                          (1860,6 kb/s) (average 3925,5 kb/s)
putting file /usr/share/cups/drivers/PSMON.DLL as \WIN40/PSMON.DLL \
                          (5090,9 kb/s) (average 3947,7 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                           -c 'adddriver "Windows 4.0" \
                           "LaserColor:ADOBEPS4.DRV:LaserColor.PPD:\
                            NULL:ADOBEPS4.HLP:PSMON.DLL:RAW:\
                            ADOBEPS4.DRV,LaserColor.PPD,ADOBEPS4.HLP,\
                            PSMON.DLL,ADFONTS.MFM,DEFPRTR2.PPD,\
                            ICONLIB.DLL"'
Printer Driver LaserColor successfully installed.

Running command: rpcclient localhost -N -U'root%1' \
                           -c 'setdriver LaserColor LaserColor'
Succesfully set LaserColor to driver LaserColor.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                           -c 'mkdir W32X86;put /var/tmp/40d05d9f9895e \
                           W32X86/Multifuncion.ppd;put \
                           /usr/share/cups/drivers/cupsdrv5.dll \
                           W32X86/cupsdrv5.dll;put \
                           /usr/share/cups/drivers/cupsui5.dll \
                           W32X86/cupsui5.dll;put \
                           /usr/share/cups/drivers/cups5.hlp \
                           W32X86/cups5.hlp'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \W32X86
putting file /var/tmp/40d05d9f9895e as \W32X86/Multifuncion.ppd \
                             (982,2 kb/s) (average 982,2 kb/s)
putting file /usr/share/cups/drivers/cupsdrv5.dll as \W32X86/cupsdrv5.dll \
                            (3041,1 kb/s) (average 2873,0 kb/s)
putting file /usr/share/cups/drivers/cupsui5.dll as \W32X86/cupsui5.dll \
                            (2821,0 kb/s) (average 2850,3 kb/s)
putting file /usr/share/cups/drivers/cups5.hlp as \W32X86/cups5.hlp \
                            (3475,0 kb/s) (average 2864,3 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                           -c 'adddriver "Windows NT x86" \
                           "Multifuncion:cupsdrv5.dll:\
```

```
                            Multifuncion.ppd:cupsui5.dll:\
                            cups5.hlp:NULL:RAW:NULL"'
Printer Driver Multifuncion successfully installed.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                           -c 'mkdir WIN40;put /var/tmp/40d05d9f9895e \
                           WIN40/Multifuncion.PPD;put \
                           /usr/share/cups/drivers/ADFONTS.MFM \
                           WIN40/ADFONTS.MFM;put \
                           /usr/share/cups/drivers/ADOBEPS4.DRV \
                           WIN40/ADOBEPS4.DRV;put \
                           /usr/share/cups/drivers/ADOBEPS4.HLP \
                           WIN40/ADOBEPS4.HLP;put \
                           /usr/share/cups/drivers/DEFPRTR2.PPD \
                           WIN40/DEFPRTR2.PPD;put \
                           /usr/share/cups/drivers/ICONLIB.DLL \
                           WIN40/ICONLIB.DLL;put \
                           /usr/share/cups/drivers/PSMON.DLL \
                           WIN40/PSMON.DLL;'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \WIN40
putting file /var/tmp/40d05d9f9895e as \WIN40/Multifuncion.PPD \
                           (1964,3 kb/s) (average 1964,4 kb/s)
putting file /usr/share/cups/drivers/ADFONTS.MFM as \WIN40/ADFONTS.MFM \
                           (3747,2 kb/s) (average 3700,9 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.DRV as \WIN40/ADOBEPS4.DRV \
                           (4932,4 kb/s) (average 4471,0 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.HLP as \WIN40/ADOBEPS4.HLP \
                           (2950,6 kb/s) (average 4202,8 kb/s)
putting file /usr/share/cups/drivers/DEFPRTR2.PPD as \WIN40/DEFPRTR2.PPD \
                           (2633,5 kb/s) (average 4187,3 kb/s)
putting file /usr/share/cups/drivers/ICONLIB.DLL as \WIN40/ICONLIB.DLL \
                           (1538,1 kb/s) (average 3844,1 kb/s)
putting file /usr/share/cups/drivers/PSMON.DLL as \WIN40/PSMON.DLL \
                           (1037,0 kb/s) (average 3604,7 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                           -c 'adddriver "Windows 4.0" \
                           "Multifuncion:ADOBEPS4.DRV:Multifuncion.PPD:\
                            NULL:ADOBEPS4.HLP:PSMON.DLL:RAW:\
                            ADOBEPS4.DRV,Multifuncion.PPD,ADOBEPS4.HLP,\
                            PSMON.DLL,ADFONTS.MFM,DEFPRTR2.PPD,\
                            ICONLIB.DLL"'
Printer Driver Multifuncion successfully installed.

Running command: rpcclient localhost -N -U'root%1' \
                           -c 'setdriver Multifuncion Multifuncion'
Succesfully set Multifuncion to driver Multifuncion.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                           -c 'mkdir W32X86;put /var/tmp/40d05da3c1a90 \
                           W32X86/Plotter.ppd;put \
                           /usr/share/cups/drivers/cupsdrv5.dll \
```

```
                          W32X86/cupsdrv5.dll;put \
                          /usr/share/cups/drivers/cupsui5.dll \
                          W32X86/cupsui5.dll;put \
                          /usr/share/cups/drivers/cups5.hlp \
                          W32X86/cups5.hlp'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \W32X86
putting file /var/tmp/40d05da3c1a90 as \W32X86/Plotter.ppd \
                       (1964,3 kb/s) (average 1964,4 kb/s)
putting file /usr/share/cups/drivers/cupsdrv5.dll as \W32X86/cupsdrv5.dll \
                       (2943,0 kb/s) (average 2902,6 kb/s)
putting file /usr/share/cups/drivers/cupsui5.dll as \W32X86/cupsui5.dll \
                       (3633,8 kb/s) (average 3179,2 kb/s)
putting file /usr/share/cups/drivers/cups5.hlp as \W32X86/cups5.hlp \
                       (2780,0 kb/s) (average 3166,8 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                       -c 'adddriver "Windows NT x86" \
                       "Plotter:cupsdrv5.dll:Plotter.ppd:\
                        cupsui5.dll:cups5.hlp:NULL:RAW:NULL"'
Printer Driver Plotter successfully installed.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                          -c 'mkdir WIN40;put /var/tmp/40d05da3c1a90 \
                          WIN40/Plotter.PPD;put \
                          /usr/share/cups/drivers/ADFONTS.MFM \
                          WIN40/ADFONTS.MFM;put \
                          /usr/share/cups/drivers/ADOBEPS4.DRV \
                          WIN40/ADOBEPS4.DRV;put \
                          /usr/share/cups/drivers/ADOBEPS4.HLP \
                          WIN40/ADOBEPS4.HLP;put \
                          /usr/share/cups/drivers/DEFPRTR2.PPD \
                          WIN40/DEFPRTR2.PPD;put \
                          /usr/share/cups/drivers/ICONLIB.DLL \
                          WIN40/ICONLIB.DLL;put \
                          /usr/share/cups/drivers/PSMON.DLL \
                          WIN40/PSMON.DLL;'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \WIN40
putting file /var/tmp/40d05da3c1a90 as \WIN40/Plotter.PPD \
                      (1571,5 kb/s) (average 1571,5 kb/s)
putting file /usr/share/cups/drivers/ADFONTS.MFM as \WIN40/ADFONTS.MFM \
                      (3557,5 kb/s) (average 3496,6 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.DRV as \WIN40/ADOBEPS4.DRV \
                      (4712,4 kb/s) (average 4253,6 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.HLP as \WIN40/ADOBEPS4.HLP \
                      (3054,8 kb/s) (average 4056,5 kb/s)
putting file /usr/share/cups/drivers/DEFPRTR2.PPD as \WIN40/DEFPRTR2.PPD \
                      (2194,6 kb/s) (average 4035,2 kb/s)
putting file /usr/share/cups/drivers/ICONLIB.DLL as \WIN40/ICONLIB.DLL \
                      (1860,6 kb/s) (average 3804,7 kb/s)
putting file /usr/share/cups/drivers/PSMON.DLL as \WIN40/PSMON.DLL \
                      (848,5 kb/s) (average 3505,0 kb/s)
```

```
Running command: rpcclient localhost -N -U'root%1' \
                          -c 'adddriver "Windows 4.0" \
                          "Plotter:ADOBEPS4.DRV:Plotter.PPD:NULL:\
                           ADOBEPS4.HLP:PSMON.DLL:RAW:ADOBEPS4.DRV,\
                           Plotter.PPD,ADOBEPS4.HLP,PSMON.DLL,\
                           ADFONTS.MFM,DEFPRTR2.PPD,ICONLIB.DLL"'
Printer Driver Plotter successfully installed.

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'setdriver Plotter Plotter'
Succesfully set Plotter to driver Plotter.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                          -c 'mkdir W32X86;put /var/tmp/40d05da9be1dc \
                          W32X86/Sublimacion.ppd;put \
                          /usr/share/cups/drivers/cupsdrv5.dll \
                          W32X86/cupsdrv5.dll;put \
                          /usr/share/cups/drivers/cupsui5.dll \
                          W32X86/cupsui5.dll;put \
                          /usr/share/cups/drivers/cups5.hlp \
                          W32X86/cups5.hlp'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \W32X86
putting file /var/tmp/40d05da9be1dc as \W32X86/Sublimacion.ppd \
                           (1122,5 kb/s) (average 1122,5 kb/s)
putting file /usr/share/cups/drivers/cupsdrv5.dll as \W32X86/cupsdrv5.dll \
                           (4414,5 kb/s) (average 4080,5 kb/s)
putting file /usr/share/cups/drivers/cupsui5.dll as \W32X86/cupsui5.dll \
                           (5229,1 kb/s) (average 4508,6 kb/s)
putting file /usr/share/cups/drivers/cups5.hlp as \W32X86/cups5.hlp \
                           (3475,0 kb/s) (average 4472,4 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'adddriver "Windows NT x86" \
                          "Sublimacion:cupsdrv5.dll:Sublimacion.ppd:\
                           cupsui5.dll:cups5.hlp:NULL:RAW:NULL"'
Printer Driver Sublimacion successfully installed.

Running command: smbclient //localhost/print\$ -N -U'root%1' \
                          -c 'mkdir WIN40;put /var/tmp/40d05da9be1dc \
                          WIN40/Sublimacion.PPD;put \
                          /usr/share/cups/drivers/ADFONTS.MFM \
                          WIN40/ADFONTS.MFM;put \
                          /usr/share/cups/drivers/ADOBEPS4.DRV \
                          WIN40/ADOBEPS4.DRV;put \
                          /usr/share/cups/drivers/ADOBEPS4.HLP \
                          WIN40/ADOBEPS4.HLP;put \
                          /usr/share/cups/drivers/DEFPRTR2.PPD \
                          WIN40/DEFPRTR2.PPD;put \
                          /usr/share/cups/drivers/ICONLIB.DLL \
                          WIN40/ICONLIB.DLL;put \
                          /usr/share/cups/drivers/PSMON.DLL \
```

```
                          WIN40/PSMON.DLL;'
Domain=[GSRDOMAIN] OS=[Unix] Server=[Samba 3.0.7-Debian]
NT_STATUS_OBJECT_NAME_COLLISION making remote directory \WIN40
putting file /var/tmp/40d05da9be1dc as \WIN40/Sublimacion.PPD \
                         (1571,5 kb/s) (average 1571,5 kb/s)
putting file /usr/share/cups/drivers/ADFONTS.MFM as \WIN40/ADFONTS.MFM \
                         (5620,8 kb/s) (average 5428,0 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.DRV as \WIN40/ADOBEPS4.DRV \
                         (5174,0 kb/s) (average 5250,2 kb/s)
putting file /usr/share/cups/drivers/ADOBEPS4.HLP as \WIN40/ADOBEPS4.HLP \
                         (2297,8 kb/s) (average 4529,6 kb/s)
putting file /usr/share/cups/drivers/DEFPRTR2.PPD as \WIN40/DEFPRTR2.PPD \
                         (731,5 kb/s) (average 4387,5 kb/s)
putting file /usr/share/cups/drivers/ICONLIB.DLL as \WIN40/ICONLIB.DLL \
                         (5015,6 kb/s) (average 4416,2 kb/s)
putting file /usr/share/cups/drivers/PSMON.DLL as \WIN40/PSMON.DLL \
                         (3294,1 kb/s) (average 4379,6 kb/s)

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'adddriver "Windows 4.0" \
                          "Sublimacion:ADOBEPS4.DRV:Sublimacion.PPD:\
                           NULL:ADOBEPS4.HLP:PSMON.DLL:RAW:ADOBEPS4.DRV,\
                           Sublimacion.PPD,ADOBEPS4.HLP,PSMON.DLL,\
                           ADFONTS.MFM,DEFPRTR2.PPD,ICONLIB.DLL"'
Printer Driver Sublimacion successfully installed.

Running command: rpcclient localhost -N -U'root%1' \
                          -c 'setdriver Sublimacion Sublimacion'
Succesfully set Sublimacion to driver Sublimacion.
```

Apéndice O. Ejemplo de certificado para un servidor

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDHrnH1k+2Iae/5jC0mia+LiJTLJj9KVI7t0/vj5Nu7cLTsQJEi
71bGHq23TQDuwCwaAK12aIbaXUk1m1C/pl3BCTm1h5mlHMZXZrMyikNeh+3Fq33a
xSAn71pbm5iRp9EJjoDXggWIJwZrGoCG4wXDZAT9iXtEI5y/jP4xV7s8HwIDAQAB
AoGBAIaPo/QeD8ARw8mjEPobZtTc4YhU6empOfhDFkfo/bo+pW1fxW6JYyx3mBEi
LzK1BgMv2bUlk1qr6p3ZYH0GG768ZBr3Vola0W1H9pNx2/Cm/7wt3Dkv5cjG5STk
qYHIsfTyvyGdE0Gr5OLl84ayHh6Bv7AU2FGC/1ybABNYiUqBAkEA89uJpTXzNC/7
RKARHqmPjwTAVoJAbIwefNT5KyOysCYe0oa3U0pW/Q5aWEgkTJ1KOD6/oPKZHCbW
xgu6BbSNTwJBANGfytpVx3bF2Emnkp0Dr4+edVvj16xPWuuK25PHTqqTHkX7Qn9A
kSMRXmSmQuHf8uBt6iIUd8Sn4MmQMF3k0DECQHokims//JM1PUwASNLs50Uhgh1S
nGZCQLsSCcP723KzhVi5tXV4lN2npMT3TYc6eYR2mZFKMjqRkZ4dHY3iA60CQQCN
i8WxCm0GkW+LxKBmb5+zbb83TjFKw8bT985vCgzfdzng7VmojZOzRz4i3nWZCdx5
mR6Y5pM88lMCJ9/Q9vlxAkApzw9xI0gjLp0TD7fqocbrcDf8RNatRZlN2J9ciVBn
jWos3xjqtpSjXISCjUUh3k6vLGAxBvXFdN6nM8fQFnM7
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDZTCCAs6gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBhDELMAkGA1UEBhMCUFQx
ETAPBgNVBAgUCEJyYWdhbudhMREwDwYDVQQHFAhCcmFnYW7nYTEPMA0GA1UEChMG
Z3NyLnB0MQ8wDQYDVQQLEwZnc3IucHQxDzANBgNVBAMTBmdzci5wdDEcMBoGCSqG
SIb3DQEJARYNc2VyZ2lvQGdzci5wdDAeFw0wNDAzMDkyMTI5MTVaFw0wNTAzMDky
MTI5MTVaMIGEMQswCQYDVQQGEwJQVDERMA8GA1UECBQIQnJhZ2Fu52ExETAPBgNV
BAcUCEJyYWdhbudhMQ8wDQYDVQQKEwZnc3IucHQxDzANBgNVBAsTBmdzci5wdDEP
MA0GA1UEAxMGZ3NyLnB0MRwwGgYJKoZIhvcNAQkBFg1zZXJnaW9AZ3NyLnB0MIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDHrnH1k+2Iae/5jC0mia+LiJTLJj9K
VI7t0/vj5Nu7cLTsQJEi71bGHq23TQDuwCwaAK12aIbaXUk1m1C/pl3BCTm1h5ml
HMZXZrMyikNeh+3Fq33axSAn71pbm5iRp9EJjoDXggWIJwZrGoCG4wXDZAT9iXtE
I5y/jP4xV7s8HwIDAQABo4HkMIHhMB0GA1UdDgQWBBRvONFfdt9EbYzVcOgfHeaa
jBToHDCBsQYDVR0jBIGpMIGmgBRvONFfdt9EbYzVcOgfHeaajBToHKGBiqSBhzCB
hDELMAkGA1UEBhMCUFQxETAPBgNVBAgUCEJyYWdhbudhMREwDwYDVQQHFAhCcmFn
YW7nYTEPMA0GA1UEChMGZ3NyLnB0MQ8wDQYDVQQLEwZnc3IucHQxDzANBgNVBAMT
Bmdzci5wdDEcMBoGCSqGSIb3DQEJARYNc2VyZ2lvQGdzci5wdIIBADAMBgNVHRME
BTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAIhp8yRnTK8IYnMyPyvvjEId3sv/D6M9
RgkG7T1M7MovJn9EHwn3c2rcexrZeCP8viomGGuyuN7/nr9rmTZ1fi/z0tjpXCdt
D7UMsEKA8lzzWldrm2sv9xUQfuwZivU9SFXQ8Q+PLAFRquTnRiE+SvOAKYumaa8I
UM7tOAK2EvQv
-----END CERTIFICATE-----
```

VI. Archivos de configuración

Apéndice P. Opciones de compilación de OpenLDAP en Debian GNU/Linux

```
# Copyright 1998-2003 The OpenLDAP Foundation,  All Rights Reserved.
#  Restrictions apply, see COPYRIGHT and LICENSE files.
# Usage: configure [options] [host]
# Options: [defaults in brackets after descriptions]
# Configuration:
#   --cache-file=FILE       cache test results in FILE
#   --help                  print this message
#   --no-create             do not create output files
#   --quiet, --silent       do not print ‘checking...’ messages
#   --version               print the version of autoconf that created configure
# Directory and file names:
#   --prefix=PREFIX         install architecture-independent files in PREFIX
#                           [/usr/local]
--prefix=/usr
#   --exec-prefix=EPREFIX   install architecture-dependent files in EPREFIX
#                           [same as prefix]
#   --bindir=DIR            user executables in DIR [EPREFIX/bin]
#   --sbindir=DIR           system admin executables in DIR [EPREFIX/sbin]
#   --libexecdir=DIR        program executables in DIR [EPREFIX/libexec]
--libexecdir=’${prefix}/lib’
#   --datadir=DIR           read-only architecture-independent data in DIR
#                           [PREFIX/share]
#   --sysconfdir=DIR        read-only single-machine data in DIR [PREFIX/etc]
--sysconfdir=/etc
#   --sharedstatedir=DIR    modifiable architecture-independent data in DIR
#                           [PREFIX/com]
#   --localstatedir=DIR     modifiable single-machine data in DIR [PREFIX/var]
--localstatedir=/var/run
#   --libdir=DIR            object code libraries in DIR [EPREFIX/lib]
#   --includedir=DIR        C header files in DIR [PREFIX/include]
#   --oldincludedir=DIR     C header files for non-gcc in DIR [/usr/include]
#   --infodir=DIR           info documentation in DIR [PREFIX/info]
#   --mandir=DIR            man documentation in DIR [PREFIX/man]
--mandir=’${prefix}/share/man’
#   --srcdir=DIR            find the sources in DIR [configure dir or ..]
#   --program-prefix=PREFIX prepend PREFIX to installed program names
#   --program-suffix=SUFFIX append SUFFIX to installed program names
#   --program-transform-name=PROGRAM
#                           run sed PROGRAM on installed program names
# Host type:
#   --build=BUILD           configure for building on BUILD [BUILD=HOST]
#   --host=HOST             configure for HOST [guessed]
#   --target=TARGET         configure for TARGET [TARGET=HOST]
# Features and packages:
#   --disable-FEATURE       do not include FEATURE (same as --enable-FEATURE=no)
#   --enable-FEATURE[=ARG]  include FEATURE [ARG=yes]
#   --with-PACKAGE[=ARG]    use PACKAGE [ARG=yes]
#   --without-PACKAGE       do not use PACKAGE (same as --with-PACKAGE=no)
```

```
#   --x-includes=DIR        X include files are in DIR
#   --x-libraries=DIR       X library files are in DIR
# --enable and --with options recognized:
#   --with-subdir=DIR       change default subdirectory used for installs
--with-subdir=ldap
#   --enable-debug    enable debugging [yes]
## Our users might want to use the -d option
--enable-debug
#   --enable-syslog   enable syslog support [auto]
--enable-syslog
#   --enable-proctitle   enable proctitle support [yes]
--enable-proctitle
#   --enable-cache   enable caching (experimental) [no]
#--enable-cache
#   --enable-referrals   enable LDAPv2+ Referrals (experimental) [no]
## Better support this standard ldap feature
--enable-referrals
#   --enable-ipv6    enable IPv6 support [auto]
## Debian tries to fully support IPv6 so we need this
--enable-ipv6
#   --enable-local   enable AF_LOCAL (AF_UNIX) socket support [auto]
--enable-local
#   --enable-x-compile   enable cross compiling [no]
#   --with-cyrus-sasl   with Cyrus SASL support [auto]
--with-cyrus-sasl
#   --with-fetch    with freeBSD fetch URL support [auto]
#   --with-kerberos   with Kerberos support [auto]
#   --with-readline   with readline support [auto]
--with-readline
#   --with-threads   with threads [auto]
--with-threads
#   --with-tls    with TLS/SSL support [auto]
--with-tls
#   --with-yielding-select  with implicitly yielding select [auto]
#
# SLAPD (Standalone LDAP Daemon) Options:
#   --enable-slapd   enable building slapd [yes]
--enable-slapd
#     --enable-aci   enable per-object ACIs (experimental) [no]
#--enable-aci
#     --enable-cleartext   enable cleartext passwords [yes]
--enable-cleartext
#     --enable-crypt   enable crypt(3) passwords [no]
--enable-crypt
#     --enable-dynamic   enable linking built binaries with dynamic libs [no]
--enable-dynamic
#     --enable-kpasswd   enable Kerberos password verification [no]
#     --enable-lmpasswd   enable LAN Manager passwords [no]
#     --enable-spasswd   enable (Cyrus) SASL password verification [no]
--enable-spasswd
#     --enable-modules   enable dynamic module support [no]
--enable-modules
#     --enable-phonetic   enable phonetic/soundex [no]
```

```
--enable-phonetic
#     --enable-rewrite   enable DN rewriting in back-ldap and back-meta [no]
--enable-rewrite
#     --enable-rlookups   enable reverse lookups of client hostnames [no]
--enable-rlookups
#     --enable-slp          enable SLPv2 support [no]
--enable-slp
#     --enable-wrappers   enable tcp wrapper support [no]
--enable-wrappers
#     --enable-bdb   enable Berkeley DB backend [yes]
--enable-bdb
#     --with-bdb-module     module type static|dynamic [static]
--with-bdb-module=dynamic
#     --enable-dnssrv   enable dnssrv backend [no]
--enable-dnssrv
#     --with-dnssrv-module  module type static|dynamic [static]
--with-dnssrv-module=dynamic
#     --enable-ldap   enable ldap backend [no]
--enable-ldap
#     --with-ldap-module   module type static|dynamic [static]
--with-ldap-module=dynamic
#     --enable-ldbm   enable ldbm backend [no]
--enable-ldbm
#     --with-ldbm-api       with LDBM API auto|berkeley|bcompat|mdbm|gdbm [auto]
--with-ldbm-api=berkeley
#     --with-ldbm-module   module type static|dynamic [static]
--with-ldbm-module=dynamic
#     --with-ldbm-type   use LDBM type auto|btree|hash [auto]
#     --enable-meta   enable metadirectory backend [no]
--enable-meta
#     --with-meta-module   module type static|dynamic [static]
--with-meta-module=dynamic
#     --enable-monitor   enable monitor backend [no]
--enable-monitor
#     --with-monitor-module module type static|dynamic [static]
--with-monitor-module=dynamic
#     --enable-null   enable null backend [no]
--enable-null
#     --with-null-module   module type static|dynamic [static]
--with-null-module=dynamic
#     --enable-passwd   enable passwd backend [no]
--enable-passwd
#     --with-passwd-module  module type static|dynamic [static]
--with-passwd-module=dynamic
#     --enable-perl   enable perl backend [no]
## This does not currently build with Perl 5.8 - disable it
--disable-perl
#     --with-perl-module   module type static|dynamic [static]
#     --enable-shell   enable shell backend [no]
--enable-shell
#     --with-shell-module   module type static|dynamic [static]
--with-shell-module=dynamic
#     --enable-sql   enable sql backend [no]
```

```
--enable-sql
#     --with-sql-module   module type static|dynamic [static]
--with-sql-module=dynamic
#
# SLURPD (Replication Daemon) Options:
#   --enable-slurpd   enable building slurpd [auto]
--enable-slurpd
#
# Library Generation & Linking Options
#   --enable-static[=PKGS]  build static libraries [default=yes]
#   --enable-shared[=PKGS]  build shared libraries [default=yes]
--enable-shared
#   --enable-fast-install[=PKGS]  optimize for fast installation [default=yes]
#   --with-gnu-ld           assume the C compiler uses GNU ld [default=no]
#   --disable-libtool-lock  avoid locking (might break parallel builds)
#   --with-pic              try to use only PIC/non-PIC objects [default=use both]
#
# See INSTALL file for further details.
```

Apéndice Q. Archivo de configuración `/etc/ldap/slapd.conf`

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

########################################################################
# Global Directives:

# Features to permit
#allow bind_v2

# Schema and objectClass definitions
include     /etc/ldap/schema/core.schema
include     /etc/ldap/schema/cosine.schema
include     /etc/ldap/schema/nis.schema
include     /etc/ldap/schema/inetorgperson.schema
include     /etc/ldap/schema/openldap.schema
include     /etc/ldap/schema/misc.schema
include     /etc/ldap/schema/samba.schema
include     /etc/ldap/schema/pykota.schema

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck  on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile      /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile     /var/run/slapd.args

# Read slapd.conf(5) for possible values
loglevel     -1

# Where the dynamically loaded modules are stored
modulepath  /usr/lib/ldap
moduleload  back_ldbm

########################################################################
# Specific Backend Directives for ldbm:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend     ldbm

########################################################################
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
#backend    <other>
```

```
#######################################################################
# Specific Directives for database #1, of type ldbm:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database    ldbm

# The base of your directory in database #1
suffix      "dc=gsr,dc=pt"

# Where the database file are physically stored for database #1
directory   "/var/lib/ldap"

# Indexing options for database #1
#
# Requerido por OpenLDAP
index objectclass   eq

index default       sub
index cn            pres,sub,eq
index sn            pres,sub,eq
index mail          eq,subinitial
index givenname     eq,subinitial

# Requerido para soportar pdb_getsampwnam
index uid           pres,sub,eq

# Requerido para soportar pdb_getsambapwrid()
index displayName   pres,sub,eq

# Descomente las siguientes líneas si está almacenando entradas
# posixAccount y posixGroup en el directorio
index uidNumber     eq
index gidNumber     eq
index memberUid     eq

# Samba 3.*
index sambaSID              eq
index sambaPrimaryGroupSID  eq
index sambaDomainName       eq

# PyKota
index pykotaUserName        pres,eq,sub
index pykotaGroupName       pres,eq,sub
index pykotaPrinterName     pres,eq,sub
index pykotaLastJobIdent    eq

# Save the time that the entry gets modified, for database #1
lastmod       on

# Where to store the replica logs for database #1
# replogfile     /var/lib/ldap/replog
```

```
# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attribute=userPassword
    by dn="cn=admin,dc=gsr,dc=pt" write
    by dn="cn=readadmin,dc=gsr,dc=pt" read
    by dn="cn=pykotaadmin,dc=gsr,dc=pt" write
    by dn="cn=pykotauser,dc=gsr,dc=pt" read
    by self write
    by anonymous auth
    by * none

# allow the "ldap admin dn" access, but deny everyone else
# (Samba related)
access to attribute=sambaLMPassword,sambaNTPassword
    by dn="cn=admin,dc=gsr,dc=pt" write
    by dn="cn=readadmin,dc=gsr,dc=pt" read
    by dn="cn=pykotaadmin,dc=gsr,dc=pt" write
    by dn="cn=pykotauser,dc=gsr,dc=pt" read
    by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms.  Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
    by dn="cn=admin,dc=gsr,dc=pt" write
    by dn="cn=readadmin,dc=gsr,dc=pt" read
    by dn="cn=pykotaadmin,dc=gsr,dc=pt" write
    by dn="cn=pykotauser,dc=gsr,dc=pt" read
    by self write
    by users read
    by anonymous auth


# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
#access to dn=".*,ou=Roaming,o=morsnet"
#        by dn="cn=admin,dc=gsr,dc=pt" write
#        by dnattr=owner write

# User Limits
```

```
limits dn="cn=pykotauser,dc=gsr,dc=pt" size.soft=-1 size.hard=soft
limits dn="cn=pykotaadmin,dc=gsr,dc=pt" size.soft=-1 size.hard=soft

# CA signed certificate and server cert entries:

TLSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCACertificateFile /etc/ldap/ssl/cacert.pem
TLSCertificateFile /etc/ldap/ssl/certs/servidorcert.pem
TLSCertificateKeyFile /etc/ldap/ssl/private/servidorkey.pem

# Use the following if client authentication is required
TLSVerifyClient demand
# ... or not desired at all
#TLSVerifyClient try
#TLSVerifyClient allow
#TLSVerifyClient never

#TLSCipherSuite ALL

#######################################################################
# Specific Directives for database #2, of type 'other' (can be ldbm too):
# Database specific directives apply to this databasse until another
# 'database' directive occurs
#database        <other>

# The base of your directory for database #2
#suffix  "dc=debian,dc=org"
```

Apéndice R. Archivo de configuración `/etc/ldap/ldap.conf`

```
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.9 2000/09/04 19:57:01 kurt Exp $
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

HOST gsr.pt
BASE dc=gsr, dc=pt
PORT 636

TLS_CACERT /etc/ldap/ssl/cacert.pem
TLS_REQCERT demand
```

Apéndice S. Archivo de configuración `/etc/default/slapd`

```
# Default location of the slapd.conf file
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="slapd"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="slapd"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.conf)
SLAPD_PIDFILE=

# Configure if the slurpd daemon should be started. Possible values:
# - yes:   Always start slurpd
# - no:    Never start slurpd
# - auto:  Start slurpd if a replica option is found in slapd.conf (default)
SLURPD_START=auto

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
SLAPD_SERVICES="ldap://gsr.pt:389/ ldaps://gsr.pt:636/"

# Additional options to pass to slapd and slurpd
SLAPD_OPTIONS=""
SLURPD_OPTIONS=""
```

Apéndice T. Archivo de configuración `/etc/nsswitch.conf`

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the ‘glibc-doc’ and ‘info’ packages installed, try:
# ‘info libc "Name Service Switch"’ for information about this file.

passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap

hosts:          files ldap dns
networks:       files

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

netgroup:       nis
```

Apéndice U. Archivo de configuración `/etc/pam_ldap.conf`

```
###DEBCONF###
# the configuration of this file will be done by debconf as long as the
# first line of the file says '###DEBCONF###'
#
# you should use dpkg-reconfigure to configure this file
#
# @(#)$Id: ldap.conf,v 1.28 2003/05/29 13:01:04 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# PADL Software
# http://www.padl.com
#

# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host gsr.pt

# The distinguished name of the search base.
base dc=gsr,dc=pt

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://gsr.pt/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn cn=readadmin,dc=gsr,dc=pt

# The credentials to bind with.
# Optional: default is no credential.
bindpw 1

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
```

```
rootbinddn cn=admin,dc=gsr,dc=pt

# The port.
# Optional: default is 389.
#port 389

# The search scope.
#scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30

# Bind timelimit
#bind_timelimit 30

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid

# Search the root DSE for the password policy (works
# with Netscape Directory Server)
#pam_lookup_policy yes

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
#pam_check_host_attr yes

# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=padl,dc=com

# Group member attribute
#pam_member_attribute uniquemember
```

```
# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.

# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
pam_password exop

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password nds

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad

# Use the OpenLDAP password change
# extended operation to update the password.
#pam_password exop

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change your password.

# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX  base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
```

```
# nss_base_passwd ou=People,
# to append the default base DN but this
# may incur a small performance impact.
#nss_base_passwd ou=People,dc=padl,dc=com?one
#nss_base_shadow ou=People,dc=padl,dc=com?one
#nss_base_group  ou=Group,dc=padl,dc=com?one
#nss_base_hosts  ou=Hosts,dc=padl,dc=com?one
#nss_base_services ou=Services,dc=padl,dc=com?one
#nss_base_networks ou=Networks,dc=padl,dc=com?one
#nss_base_protocols ou=Protocols,dc=padl,dc=com?one
#nss_base_rpc  ou=Rpc,dc=padl,dc=com?one
#nss_base_ethers ou=Ethers,dc=padl,dc=com?one
#nss_base_netmasks ou=Networks,dc=padl,dc=com?ne
#nss_base_bootparams ou=Ethers,dc=padl,dc=com?one
#nss_base_aliases ou=Aliases,dc=padl,dc=com?one
#nss_base_netgroup ou=Netgroup,dc=padl,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute rfc2307attribute mapped_attribute
#nss_map_objectclass rfc2307objectclass mapped_objectclass

# configure --enable-nds is no longer supported.
# For NDS now do:
#nss_map_attribute uniqueMember member

# configure --enable-mssfu-schema is no longer supported.
# For MSSFU now do:
#nss_map_objectclass posixAccount User
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# For authPassword support, now do:
#nss_map_attribute userPassword authPassword
#pam_password nds

# For IBM SecureWay support, do:
#nss_map_objectclass posixAccount aixAccount
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
```

```
#pam_filter objectclass=aixAccount
#pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs/cert7.db

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
ssl start_tls
#ssl on

# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is "no"
tls_checkpeer yes

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
tls_cacertfile /etc/ldap/ssl/cacert.pem
#tls_cacertdir /etc/ssl/certs

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
tls_cert /home/certs/ldap.cliente.cert.pem
tls_key /home/certs/ldap.cliente.key.pem
```

Apéndice V. Archivo de configuración `/etc/libnss-ldap.conf`

Una vez instalado y configurado el paquete libnss-ldap (vea el Ejemplo 5-2 para más detalles), el archivo de configuración para el mismo quedaría de la siguiente manera:

```
###DEBCONF###
# the configuration of this file will be done by debconf as long as the
# first line of the file says '###DEBCONF###'
#
# you should use dpkg-reconfigure libnss-ldap to configure this file.
#
# @(#)$Id: ldap.conf,v 2.35 2004/03/03 21:06:34 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# PADL Software
# http://www.padl.com
#

# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host gsr.pt

# The distinguished name of the search base.
base dc=gsr,dc=pt

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://gsr.pt/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn cn=readadmin,dc=gsr,dc=pt

# The credentials to bind with.
# Optional: default is no credential.
bindpw 1
```

```
# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=gsr,dc=pt

# The port.
# Optional: default is 389.
#port 389

# The search scope.
#scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30

# Bind/connect timelimit
#bind_timelimit 30

# Reconnect policy: hard (default) will retry connecting to
# the software with exponential backoff, soft will fail
# immediately.
#bind_policy hard

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid

# Search the root DSE for the password policy (works
# with Netscape Directory Server)
#pam_lookup_policy yes

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
#pam_check_host_attr yes

# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
```

```
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=padl,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.

# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password nds

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad

# Use the OpenLDAP password change
# extended operation to update the password.
#pam_password exop

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change your password.
```

```
# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX  base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd ou=People,
# to append the default base DN but this
# may incur a small performance impact.
#nss_base_passwd ou=People,dc=padl,dc=com?one
#nss_base_shadow ou=People,dc=padl,dc=com?one
#nss_base_group  ou=Group,dc=padl,dc=com?one
#nss_base_hosts  ou=Hosts,dc=padl,dc=com?one
#nss_base_services ou=Services,dc=padl,dc=com?one
#nss_base_networks ou=Networks,dc=padl,dc=com?one
#nss_base_protocols ou=Protocols,dc=padl,dc=com?one
#nss_base_rpc  ou=Rpc,dc=padl,dc=com?one
#nss_base_ethers ou=Ethers,dc=padl,dc=com?one
#nss_base_netmasks ou=Networks,dc=padl,dc=com?ne
#nss_base_bootparams ou=Ethers,dc=padl,dc=com?one
#nss_base_aliases ou=Aliases,dc=padl,dc=com?one
#nss_base_netgroup ou=Netgroup,dc=padl,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute rfc2307attribute mapped_attribute
#nss_map_objectclass rfc2307objectclass mapped_objectclass

# configure --enable-nds is no longer supported.
# NDS mappings
#nss_map_attribute uniqueMember member

# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid msSFU30Name
#nss_map_attribute uniqueMember msSFU30PosixMember
#nss_map_attribute userPassword msSFU30Password
#nss_map_attribute homeDirectory msSFU30HomeDirectory
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFU30Name
#pam_filter objectclass=User
#pam_password ad

# configure --enable-mssfu-schema is no longer supported.
# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
```

```
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# RFC 2307 (AD) mappings
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs/cert7.db

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
ssl start_tls
#ssl on

# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
```

```
# Default is "no"
tls_checkpeer yes

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
tls_cacertfile /etc/ldap/ssl/cacert.pem
#tls_cacertdir /etc/ssl/certs

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
tls_cert /home/certs/ldap.cliente.cert.pem
tls_key /home/certs/ldap.cliente.key.pem

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache
```

Apéndice W. Archivo de configuración /etc/pamd.d/common-account

```
#
# /etc/pam.d/common-account - authorization settings common to all services
#
# This module performs non-authentication based account management. It is
# typically used to restrict/permit access to a service based on the time of day,
# currently available system resources (maximum number of users) or perhaps
# the location of the applicant user---‘root’ login only on the console.
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system.  The default is to
# only deny service to users whose accounts are expired in /etc/shadow.
#
account required pam_unix.so
account sufficient pam_ldap.so
```

Apéndice X. Archivo de configuración `/etc/pamd.d/common-auth`

```
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This module type provides two aspects of authenticating the user.
# Firstly, it establishes that the user is who they claim to be, by
# instructing the application to prompt the user for a password or other
# means of identification. Secondly, the module can grant group membership
# (independently of the /etc/groups file) or other privileges through
# its credential granting properties.
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#

auth sufficient pam_unix.so
auth sufficient pam_ldap.so try_first_pass
auth required pam_env.so
auth required pam_securetty.so
auth required pam_unix_auth.so

# Se escribe un aviso en el archivo designado por
# syslog para la autentificación, en este caso:
# /var/log/auth.log
#
auth required pam_warn.so

auth required pam_deny.so
```

Apéndice Y. Archivo de configuración /etc/pamd.d/common-password

```
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This module type is required for updating the authentication token associated
# with the user. Typically, there is one module for each ‘challenge/response’
# based authentication (auth) module-type.
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define  the services to be
# used to change user passwords.  The default is pam_unix

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

Apéndice Z. Archivo de configuración `/etc/pamd.d/common-session`

```
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This module is associated with doing things that need to be done for the
# user before/after they can be given service. Such things include the
# logging of information concerning the opening/closing of some data exchange
# with a user, mounting directories, etc. .
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).  The default is pam_unix.
#
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
session required pam_limits.so
session required pam_unix.so
session optional pam_ldap.so
```

Apéndice AA. Archivo de configuración `/etc/nscd.conf`

```
#
# /etc/nscd.conf
#
# An example Name Service Cache config file.  This file is needed by nscd.
#
# Legal entries are:
#
#   logfile         <file>
#   debug-level     <level>
#   threads         <#threads to use>
#   server-user     <user to run server as instead of root>
#       server-user is ignored if nscd is started with -S parameters
#       stat-user               <user who is allowed to request statistics>
#
#   enable-cache            <service> <yes|no>
#   positive-time-to-live   <service> <time in seconds>
#   negative-time-to-live   <service> <time in seconds>
#   suggested-size          <service> <prime number>
#   check-files             <service> <yes|no>
#
# Currently supported cache names (services): passwd, group, hosts
#


    logfile         /var/log/nscd.log
#   threads         6
    server-user     nscd
#   stat-user       somebody
    debug-level     0

    enable-cache            passwd       yes
    positive-time-to-live   passwd       600
    negative-time-to-live   passwd       20
    suggested-size          passwd       211
    check-files             passwd       yes

    enable-cache            group       yes
    positive-time-to-live   group       3600
    negative-time-to-live   group       60
    suggested-size          group       211
    check-files             group       yes

    enable-cache            hosts       yes
    positive-time-to-live   hosts       3600
    negative-time-to-live   hosts       20
    suggested-size          hosts       211
    check-files             hosts       yes
```

Apéndice AB. Archivo de configuración `/etc/default/samba`

```
# Defaults for samba initscript
# sourced by /etc/init.d/samba
# installed at /etc/default/samba by the maintainer scripts
#

#
# This is a POSIX shell fragment
#

# How should Samba (smbd) run? Possible values are "daemons"
# or "inetd".
RUN_MODE="daemons"
```

Apéndice AC. Archivo de configuración `/etc/samba/smb.conf` - por defecto -

```
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentary and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not many any basic syntactic
# errors.
#

#======================= Global Settings =======================

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = GSRDOMAIN

# server string is the equivalent of the NT Description field
   server string = %h server (Samba %v)

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
;   wins support = no

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
   dns proxy = no

# What naming service and in what order should we use to resolve host names
# to IP addresses
;   name resolve order = lmhosts host wins bcast


#### Debugging/Accounting ####
```

```
# This tells Samba to use a separate log file for each machine
# that connects
   log file = /var/log/samba/log.%m

# Put a capping on the size of the log files (in Kb).
   max log size = 1000

# If you want Samba to only log through syslog then set the following
# parameter to 'yes'.
;   syslog only = no

# We want Samba to log a minimum amount of information to syslog. Everything
# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log
# through syslog you should set the following parameter to something higher.
   syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace
   panic action = /usr/share/samba/panic-action %d


####### Authentication #######

# "security = user" is always a good idea. This will require a Unix account
# in this server for every user accessing the server. See
# /usr/share/doc/samba-doc/htmldocs/ServerType.html in the samba-doc
# package for details.
;   security = user

# You may wish to use password encryption.  See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
   encrypt passwords = true

# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
   passdb backend = tdbsam guest

   obey pam restrictions = yes

;   guest account = nobody
   invalid users = root

# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
;   unix password sync = no

# For Unix password sync to work on a Debian GNU/Linux system, the following
# parameters must be set (thanks to Augustin Luton <aluton@hybrigenics.fr> for
# sending the correct chat script for the passwd program in Debian Potato).
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n
```

```
# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
;   pam password change = no


########## Printing ##########

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
;   load printers = yes

# lpr(ng) printing. You may wish to override the location of the
# printcap file
;   printing = bsd
;   printcap name = /etc/printcap

# CUPS printing.  See also the cupsaddsmb(8) manpage in the
# cupsys-client package.
;   printing = cups
;   printcap name = cups

# When using [print$], root is implicitly a 'printer admin', but you can
# also give this right to other users to add drivers and set printer
# properties
;   printer admin = @ntadmin


######## File sharing ########

# Name mangling options
;   preserve case = yes
;   short preserve case = yes


############ Misc ############

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /home/samba/etc/smb.conf.%m

# Most people will find that this option gives better performance.
# See smb.conf(5) and /usr/share/doc/samba-doc/htmldocs/speed.html
# for details
# You may want to add the following on a Linux system:
#         SO_RCVBUF=8192 SO_SNDBUF=8192
   socket options = TCP_NODELAY

# The following parameter is useful only if you have the linpopup package
# installed. The samba maintainer and the linpopup maintainer are
# working to ease installation and configuration of linpopup and samba.
;   message command = /bin/sh -c '/usr/bin/linpopup "%f" "%m" %s; rm %s' &
```

```
# Domain Master specifies Samba to be the Domain Master Browser. If this
# machine will be configured as a BDC (a secondary logon server), you
# must set this to 'no'; otherwise, the default behavior is recommended.
;   domain master = auto

# Some defaults for winbind (make sure you're not using the ranges
# for something else.)
;   idmap uid = 10000-20000
;   idmap gid = 10000-20000
;   template shell = /bin/bash

#======================= Share Definitions =======================

[homes]
   comment = Home Directories
   browseable = no

# By default, the home directories are exported read-only. Change next
# parameter to 'yes' if you want to be able to write to them.
   writable = no

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
   directory mask = 0700

# Un-comment the following and create the netlogon directory for Domain Logons
# (you need to configure Samba to act as a domain controller too.)
;[netlogon]
;   comment = Network Logon Service
;   path = /home/samba/netlogon
;   guest ok = yes
;   writable = no
;   share modes = no

[printers]
   comment = All Printers
   browseable = no
   path = /tmp
   printable = yes
   public = no
   writable = no
   create mode = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
```

```
   browseable = yes
   read only = yes
   guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# Replace 'ntadmin' with the name of the group your admin users are
# members of.
;   write list = root, @ntadmin

# A sample share for sharing your CD-ROM with others.
;[cdrom]
;   comment = Samba server's CD-ROM
;   writable = no
;   locking = no
;   path = /cdrom
;   public = yes

# The next two parameters show how to auto-mount a CD-ROM when the
# cdrom share is accesed. For this to work /etc/fstab must contain
# an entry like this:
#
#       /dev/scd0   /cdrom  iso9660 defaults,noauto,ro,user   0 0
#
# The CD-ROM gets unmounted automatically after the connection to the
#
# If you don't want to use auto-mounting/unmounting make sure the CD
# is mounted on /cdrom
#
;   preexec = /bin/mount /cdrom
;   postexec = /bin/umount /cdrom
```

Apéndice AD. Archivo de configuración `/etc/samba/smb.conf` - Completo -

```
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentary and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not many any basic syntactic
# errors.
#

#======================= Global Settings =======================

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = GSRDOMAIN

# This sets the NetBIOS name by which a Samba server is known.
netbios name = TODOSCSI

# server string is the equivalent of the NT Description field
server string = SAMBA-LDAP PDC server

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
wins support = no

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
dns proxy = no

# What naming service and in what order should we use to resolve host names
# to IP addresses
name resolve order = lmhosts host wins bcast
```

```
#### Debugging/Accounting ####

# This tells Samba to use a separate log file for each machine
# that connects
log file = /var/log/samba/log.%m

# The value of the parameter (a astring) allows the debug level
# (logging level) to be specified in  the  smb.conf file.
# (passdb:5 auth:10 winbind:2)
log level = 0

# Put a capping on the size of the log files (in Kb).
# (0 means no limit)
max log size = 1000

# If you want Samba to only log through syslog then set the following
# parameter to 'yes'.
syslog only = no

# We want Samba to log a minimum amount of information to syslog. Everything
# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log
# through syslog you should set the following parameter to something higher.
syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace
panic action = /usr/share/samba/panic-action %d


####### Authentication #######

# "security = user" is always a good idea. This will require a Unix account
# in this server for every user accessing the server. See
# /usr/share/doc/samba-doc/htmldocs/ServerType.html in the samba-doc
# package for details.
security = user

# You may wish to use password encryption.  See the section on
# 'encrypt passwords' in the smb.conf(5) manpage before enabling.
encrypt passwords = true

# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
passdb backend = ldapsam:ldap://gsr.pt

# This parameter control whether or not Samba should obey PAM's
# account and session management directives. The default
# behavior is to use PAM for clear text authentication only and
# to ignore any account or session management. Note that Samba
# always ignores PAM for authentication in the  case  of
# encrypt passwords = yes.
obey pam restrictions = yes
```

```
# This is a username which will be used for access to services which
# are specified as "guest ok"
guest account = guest

# This is a list of users that should not be allowed to login to this service.
#   invalid users = root

# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
unix password sync = yes

# For Unix password sync to work on a Debian GNU/Linux system, the following
# parameters must be set (thanks to Augustin Luton <aluton@hybrigenics.fr> for
# sending the correct chat script for the passwd program in Debian Potato).
;   passwd program = /usr/bin/passwd %u
passwd program = /usr/sbin/smbldap-passwd -o %u
passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n .

# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
pam password change = no


####### LDAP-specific settings ########

# The ldap admin dn defines the Distinguished Name (DN) name used by Samba
# to contact the ldap server when retreiving user account information.
# The ldap admin dn is used in conjunction
# with the admin dn password stored in the private/secrets.tdb file.
# See the smbpasswd(8) man page for more information on how to accmplish this.
ldap admin dn = cn=admin,dc=gsr,dc=pt

# This parameter should contain the FQDN of the ldap directory server which
# should be queried to locate user account information.
;    ldap server = gsr.pt

# This option is used to control the tcp port number used to contact the
# ldap server. The default is to use the stand LDAPS port 636.
;   ldap port = 389

# This option is used to define whether or not Samba should use SSL when
# connecting to the ldap server. ('off', 'start_tls', or 'on' (default))
ldap ssl = star_tls

# This parameter specifies whether a delete operation in the ldapsam deletes
# the complete entry or only the attributes specific to Samba.
ldap delete dn = no

# This parameter specifies the RFC 2254 compliant LDAP search filter.
# The default is to match the login name with the uid attribute for
```

```
# all entries matching the sambaSamAccount objectclass.
# Note that this filter should only return one entry.
;   ldap filter = (&(uid=%u)(objectclass=sambaSamAccount))

# Specifies where user and machine accounts are added to the tree.
# Can be overriden by ldap user suffix and ldap machine suffix.
# It also used as the base dn for all ldap searches.
ldap suffix = dc=gsr,dc=pt

# This parameter specifies where users are added to the tree.
ldap user suffix = ou=people

# This parameters specifies the suffix that is used for groups when these
# are added to the LDAP directory.
ldap group suffix = ou=groups

# It specifies where machines should be added to the ldap tree.
ldap machine suffix = ou=machines


########## Printing ##########

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
load printers = yes

# lpr(ng) printing. You may wish to override the location of the
# printcap file
;   printing = bsd
;   printcap name = /etc/printcap

# CUPS printing.  See also the cupsaddsmb(8) manpage in the
# cupsys-client package.
printing = cups

# When using [print$], root is implicitly a 'printer admin', but you can
# also give this right to other users to add drivers and set printer
# properties
printer admin = @domainprintoperator


######## File sharing ########

# Name mangling options
preserve case = yes


#### Domain Controller #######


# This integer value controls what level Samba advertises itself as for browse
# elections. The value of this parameter determines whether nmbd(8) has a
# chance of becoming a local master browser for the WORKGROUP in the
```

```
# local broadcast area.
os level = 80

# This boolean parameter controls if nmbd(8) is a preferred master browser
# for its workgroup.
preferred master = yes

# Domain Master specifies Samba to be the Domain Master Browser. If this
# machine will be configured as a BDC (a secondary logon server), you
# must set this to 'no'; otherwise, the default behavior is recommended.
domain master = yes

# This option allows nmbd(8) to try and become a local master browser
# on a subnet.
local master = yes

# If set to yes, the Samba server will act as a Primary Domain Controller
# (PDC) for  the  workgroup  it  is  in.
domain logons = yes

# This  parameter specifies the home directory where roaming profiles
# (NTuser.dat etc files for Windows NT) are stored.
logon path = \\%L\profiles\%u

# This parameter specifies the local path to which the home directory
# will be connected and is only used by NT Workstations.
logon drive = H:

# This  parameter  specifies the home directory location when a Win95/98
# or NT Workstation logs into a Samba PDC.
logon home = \\%L\%u\.profile

# This parameter specifies the batch file (.bat) or NT command file
# (.cmd) to be downloaded and run  on a machine when a user successfully
# logs in.
;   logon script = logon.cmd
logon script =

# Users and groups allowed to be 'Domain Admins'
;   domain admin group = @domainadmins


############ Misc ############

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /home/samba/etc/smb.conf.%m

# Most people will find that this option gives better performance.
# See smb.conf(5) and /usr/share/doc/samba-doc/htmldocs/speed.html
# for details
# You may want to add the following on a Linux system:
```

```
#         SO_RCVBUF=8192 SO_SNDBUF=8192
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
winbind uid = 10000-20000
winbind gid = 10000-20000

# When filling out the user information for a Windows NT user,
# the winbindd(8) daemon uses this parameter to fill in the login
# shell for that user.
template shell = /bin/bash

# This parameter specifies what OS ACL semantics should be
# compatible with. Possible values are winnt for Windows NT 4,
# win2k for Windows 2000 and above and auto. If you specify auto,
# the value for this parameter will be based upon the version
# of the client. There should be no reason to change this
# parameter from the default.
acl compatibility = Auto

# Using smbldap-tools to add machines
add user script = /usr/sbin/smbldap-useradd.pl -w %u


#======================= Share Definitions =======================

[homes]
comment = Home Directories

# This controls whether this share is seen in the list of
# available shares in a net view and in the browse list.
browseable = no
read only = no

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
directory mask = 0700

[netlogon]
comment = Network Logon Service
path = /home/samba/netlogon
share modes = no
guest ok = yes
write list = @domainadmins

[profiles]
comment = User’s Profiles
path = /home/samba/profiles
read only = no
browseable = no
create mask = 0600
```

```
directory mask = 0700
guest ok = yes

[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
printable = yes
printer admin = root, @domainprintoperator
;   create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
write list = root, @domainprintoperator

[tmp]
comment = Temporal
read only = no
path = /tmp

[cdrom]
comment = Samba server’s CD-ROM
locking = no
path = /cdrom
guest ok = yes
```

Apéndice AE. Archivo de configuración /etc/cups/client.conf

```
#
# "$Id: client.conf,v 1.8 2004/02/25 20:15:27 mike Exp $"
#
#   Sample client configuration file for the Common UNIX Printing System
#   (CUPS).
#
#   Copyright 1997-2004 by Easy Software Products, all rights reserved.
#
#   These coded instructions, statements, and computer programs are the
#   property of Easy Software Products and are protected by Federal
#   copyright law.  Distribution and use rights are outlined in the file
#   "LICENSE.txt" which should have been included with this file.  If this
#   file is missing or damaged please contact Easy Software Products
#   at:
#
#       Attn: CUPS Licensing Information
#       Easy Software Products
#       44141 Airport View Drive, Suite 204
#       Hollywood, Maryland 20636-3111 USA
#
#       Voice: (301) 373-9603
#       EMail: cups-info@cups.org
#         WWW: http://www.cups.org
#

##############################################################################
#                                                                            #
# This is the CUPS client configuration file.  This file is used to    #
# define client-specific parameters, such as the default server or     #
# default encryption settings.                                               #
#                                                                            #
##############################################################################

#
# ServerName: the hostname of your server.  By default CUPS will use the
# hostname of the system or the value of the CUPS_SERVER environment
# variable.  ONLY ONE SERVER NAME MAY BE SPECIFIED AT A TIME.  To use
# more than one server you must use a local scheduler with browsing
# and possibly polling.
#

ServerName gsr.pt

#
# Encryption: whether or not to use encryption; this depends on having
# the OpenSSL library linked into the CUPS library.
#
# Possible values:
```

```
#
#     Always       - Always use encryption (SSL)
#     Never        - Never use encryption
#     Required     - Use TLS encryption upgrade
#     IfRequested  - Use encryption if the server requests it
#
# The default value is "IfRequested".  This parameter can also be set
# using the CUPS_ENCRYPTION environment variable.
#

#Encryption Always
#Encryption Never
#Encryption Required
#Encryption IfRequested


#
# End of "$Id: client.conf,v 1.8 2004/02/25 20:15:27 mike Exp $".
#
```

Apéndice AF. Archivo de configuración /etc/cups/cupsd.conf

```
#
# "$Id: cupsd.conf.in,v 1.14 2004/02/25 20:14:51 mike Exp $"
#
#   Sample configuration file for the Common UNIX Printing System (CUPS)
#   scheduler.
#
#   Copyright 1997-2004 by Easy Software Products, all rights reserved.
#
#   These coded instructions, statements, and computer programs are the
#   property of Easy Software Products and are protected by Federal
#   copyright law.  Distribution and use rights are outlined in the file
#   "LICENSE.txt" which should have been included with this file.  If this
#   file is missing or damaged please contact Easy Software Products
#   at:
#
#       Attn: CUPS Licensing Information
#       Easy Software Products
#       44141 Airport View Drive, Suite 204
#       Hollywood, Maryland 20636-3111 USA
#
#       Voice: (301) 373-9603
#       EMail: cups-info@cups.org
#         WWW: http://www.cups.org
#

##############################################################################
#                                                                            #
# This is the CUPS configuration file.  If you are familiar with       #
# Apache or any of the other popular web servers, we've followed the   #
# same format.  Any configuration variable used here has the same      #
# semantics as the corresponding variable in Apache.  If we need       #
# different functionality then a different name is used to avoid       #
# confusion...                                                               #
#                                                                            #
##############################################################################


########
######## Server Identity
########

#
# ServerName: the hostname of your server, as advertised to the world.
# By default CUPS will use the hostname of the system.
#
# To set the default server used by clients, see the client.conf file.
#
```

```
ServerName gsr.pt

#
# ServerAdmin: the email address to send all complaints/problems to.
# By default CUPS will use "root@hostname".
#

ServerAdmin sergio@gsr.pt


########
######## Server Options
########

#
# AccessLog: the access log file; if this does not start with a leading /
# then it is assumed to be relative to ServerRoot.  By default set to
# "/var/log/cups/access_log"
#
# You can also use the special name "syslog" to send the output to the
# syslog file or daemon.
#

AccessLog /var/log/cups/access_log

#
# Classification: the classification level of the server.  If set, this
# classification is displayed on all pages, and raw printing is disabled.
# The default is the empty string.
#

#Classification classified
#Classification confidential
#Classification secret
#Classification topsecret
#Classification unclassified

#
# ClassifyOverride: whether to allow users to override the classification
# on printouts. If enabled, users can limit banner pages to before or
# after the job, and can change the classification of a job, but cannot
# completely eliminate the classification or banners.
#
# The default is off.
#

#ClassifyOverride off

#
# DataDir: the root directory for the CUPS data files.
# By default "/usr/share/cups".
#
```

```
DataDir /usr/share/cups

#
# DefaultCharset: the default character set to use. If not specified,
# defaults to "utf-8".  Note that this can also be overridden in
# HTML documents...
#

DefaultCharset notused

#
# DefaultLanguage: the default language if not specified by the browser.
# If not specified, the current locale is used.
#

DefaultLanguage es

#
# DocumentRoot: the root directory for HTTP documents that are served.
# By default "/usr/share/cups/doc-root".
#

DocumentRoot /usr/share/cups/doc-root

#
# ErrorLog: the error log file; if this does not start with a leading /
# then it is assumed to be relative to ServerRoot.  By default set to
# "/var/log/cups/error_log"
#
# You can also use the special name "syslog" to send the output to the
# syslog file or daemon.
#

ErrorLog /var/log/cups/error_log

#
# FileDevice: determines whether the scheduler will allow new printers
# to be added using device URIs of the form "file:/foo/bar". The default
# is not to allow file devices due to the potential security vulnerability
# and due to the fact that file devices do not support raw printing.
#

FileDevice No


#
# FontPath: the path to locate all font files (currently only for pstoraster)
# By default "/usr/share/cups/fonts".
#

FontPath /usr/share/cups/fonts

#
```

```
# LogLevel: controls the number of messages logged to the ErrorLog
# file and can be one of the following:
#
#     debug2 Log everything.
#     debug Log almost everything.
#     info      Log all requests and state changes.
#     warn      Log errors and warnings.
#     error     Log only errors.
#     none      Log nothing.
#

LogLevel debug2

#
# MaxLogSize: controls the maximum size of each log file before they are
# rotated.  Defaults to 1048576 (1MB).  Set to 0 to disable log rotating.
#

MaxLogSize 0

#
# PageLog: the page log file; if this does not start with a leading /
# then it is assumed to be relative to ServerRoot.  By default set to
# "/var/log/cups/page_log"
#
# You can also use the special name "syslog" to send the output to the
# syslog file or daemon.
#

PageLog /var/log/cups/page_log

#
# PreserveJobHistory: whether or not to preserve the job history after a
# job is completed, cancelled, or stopped.  Default is Yes.
#

PreserveJobHistory Yes

#
# PreserveJobFiles: whether or not to preserve the job files after a
# job is completed, cancelled, or stopped.  Default is No.
#

PreserveJobFiles No

#
# AutoPurgeJobs: automatically purge jobs when not needed for quotas.
# Default is No.
#

AutoPurgeJobs No

#
```

```
# MaxCopies: maximum number of copies that a user can request. Default is
# 100.
#

MaxCopies 100

#
# MaxJobs: maximum number of jobs to keep in memory (active and completed.)
# Default is 500; the value 0 is used for no limit.
#

MaxJobs 500

#
# MaxJobsPerPrinter: maximum number of active jobs per printer. The default
# is 0 for no limit.
#

MaxJobsPerPrinter 0

#
# MaxJobsPerUser: maximum number of active jobs per user. The default
# is 0 for no limit.
#

MaxJobsPerUser 0

#
# MaxPrinterHistory: controls the maximum number of history collections
# in the printer-state-history attribute.  Set to 0 to disable history
# data.
#

MaxPrinterHistory 10

#
# Printcap: the name of the printcap file.  Default is /etc/printcap.
# Leave blank to disable printcap file generation.
#

Printcap /var/run/cups/printcap

#
# PrintcapFormat: the format of the printcap file, currently either
# BSD or Solaris.  The default is "BSD".
#

#PrintcapFormat BSD
#PrintcapFormat Solaris

#
# PrintcapGUI: the name of the GUI options panel program to associate
# with print queues under IRIX.  The default is "/usr/bin/glpoptions"
```

```
# from ESP Print Pro.
#
# This option is only used under IRIX; the options panel program
# must accept the "-d printer" and "-o options" options and write
# the selected printer options back to stdout on completion.
#

#PrintcapGUI /usr/bin/glpoptions

#
# RequestRoot: the directory where request files are stored.
# By default "/var/spool/cups".
#

RequestRoot /var/spool/cups

#
# RemoteRoot: the name of the user assigned to unauthenticated accesses
# from remote systems.  By default "remroot".
#

#RemoteRoot remroot

#
# ServerBin: the root directory for the scheduler executables.
# By default "/usr/lib/cups".
#

ServerBin /usr/lib/cups

#
# ServerRoot: the root directory for the scheduler.
# By default "/etc/cups".
#

ServerRoot /etc/cups


########
######## Fax Support
########

#
# FaxRetryLimit: the number of times a fax job is retried.
# The default is 5 times.
#

#FaxRetryLimit 5

#
# FaxRetryInterval: the number of seconds between fax job retries.
# The default is 300 seconds/5 minutes.
#
```

```
#FaxRetryInterval 300


########
######## Encryption Support
########

#
# ServerCertificate: the file to read containing the server's certificate.
# Defaults to "/etc/cups/ssl/server.crt".
#

ServerCertificate /etc/cups/ssl/certs/servidorcert.pem

#
# ServerKey: the file to read containing the server's key.
# Defaults to "/etc/cups/ssl/server.key".
#

ServerKey /etc/cups/ssl/private/servidorkey.pem


########
######## Filter Options
########

#
# User/Group: the user and group the server runs under.  Normally this
# must be lp and lpadmin, however you can configure things for another
# user or group as needed.
#
# Note: the server must be run initially as root to support the
# default IPP port of 631.  It changes users whenever an external
# program is run, or if the RunAsUser directive is specified...
#

User lp
Group lpadmin

#
# RIPCache: the amount of memory that each RIP should use to cache
# bitmaps.  The value can be any real number followed by "k" for
# kilobytes, "m" for megabytes, "g" for gigabytes, or "t" for tiles
# (1 tile = 256x256 pixels.)  Defaults to "8m" (8 megabytes).
#

RIPCache 8m

#
# TempDir: the directory to put temporary files in.  This directory must be
# writable by the user defined above!  Defaults to "/var/spool/cups/tmp" or
# the value of the TMPDIR environment variable.
```

```
#

TempDir /var/spool/cups/tmp

#
# FilterLimit: sets the maximum cost of all job filters that can be run
# at the same time.  A limit of 0 means no limit.  A typical job may need
# a filter limit of at least 200; limits less than the minimum required
# by a job force a single job to be printed at any time.
#
# The default limit is 0 (unlimited).
#

FilterLimit 0

########
######## Network Options
########

#
# Ports/addresses that we listen to.  The default port 631 is reserved
# for the Internet Printing Protocol (IPP) and is what we use here.
#
# You can have multiple Port/Listen lines to listen to more than one
# port or address, or to restrict access:
#
#    Port 80
#    Port 631
#    Listen hostname
#    Listen hostname:80
#    Listen hostname:631
#    Listen 1.2.3.4
#    Listen 1.2.3.4:631
#
# NOTE: Unfortunately, most web browsers don't support TLS or HTTP Upgrades
# for encryption.  If you want to support web-based encryption you'll
# probably need to listen on port 443 (the "https" port...)
#

#Port 80
#Port 443
#Port 631

Listen gsr.pt:631

SSLListen gsr.pt:6443

#
# HostNameLookups: whether or not to do lookups on IP addresses to get a
# fully-qualified hostname.  This defaults to Off for performance reasons...
#

HostNameLookups Off
```

```
#
# KeepAlive: whether or not to support the Keep-Alive connection
# option.  Default is on.
#

KeepAlive On

#
# KeepAliveTimeout: the timeout before Keep-Alive connections are
# automatically closed.  Default is 60 seconds.
#

KeepAliveTimeout 60

#
# MaxClients: controls the maximum number of simultaneous clients that
# will be handled.  Defaults to 100.
#

MaxClients 100

#
# MaxClientsPerHost: controls the maximum number of simultaneous clients that
# will be handled from a specific host.  Defaults to 10 or 1/10th of the
# MaxClients setting, whichever is larger.  A value of 0 specifies the
# automatic (10 or 1/10th) setting.
#

MaxClientsPerHost 0

#
# MaxRequestSize: controls the maximum size of HTTP requests and print files.
# Set to 0 to disable this feature (defaults to 0.)
#

MaxRequestSize 0

#
# Timeout: the timeout before requests time out.  Default is 300 seconds.
#

Timeout 300


########
######## Browsing Options
########

#
# Browsing: whether or not to broadcast and/or listen for CUPS printer
# information on the network.  Enabled by default.
#
```

```
#Browsing On

#
# BrowseProtocols: which protocols to use for browsing.  Can be
# any of the following separated by whitespace and/or commas:
#
#     all  - Use all supported protocols.
#     cups - Use the CUPS browse protocol.
#     slp  - Use the SLPv2 protocol.
#
# The default is "cups".
#
# NOTE: If you choose to use SLPv2, it is *strongly* recommended that
#       you have at least one SLP Directory Agent (DA) on your
#       network.  Otherwise, browse updates can take several seconds,
#       during which the scheduler will not respond to client
#       requests.
#

#BrowseProtocols cups

#
# BrowseAddress: specifies a broadcast address to be used.  By
# default browsing information is not sent!
#
# Note: HP-UX does not properly handle broadcast unless you have a
# Class A, B, C, or D netmask (i.e. no CIDR support).
#
# Note: Using the "global" broadcast address (255.255.255.255) will
# activate a Linux demand-dial link with the default configuration.
# If you have a LAN as well as the dial-up link, use the LAN's
# broadcast address.
#
# The @LOCAL address broadcasts to all non point-to-point interfaces.
# For example, if you have a LAN and a dial-up link, @LOCAL would
# send printer updates to the LAN but not to the dial-up link.
# Similarly, the @IF(name) address sends to the named network
# interface, e.g. @IF(eth0) under Linux.  Interfaces are refreshed
# automatically (no more than once every 60 seconds), so they can
# be used on dynamically-configured interfaces, e.g. PPP, 802.11, etc.
#

#BrowseAddress x.y.z.255
#BrowseAddress x.y.255.255
#BrowseAddress x.255.255.255
#BrowseAddress 255.255.255.255
#BrowseAddress @LOCAL
#BrowseAddress @IF(name)

#
# BrowseShortNames: whether or not to use "short" names for remote printers
# when possible (e.g. "printer" instead of "printer@host".)  Enabled by
```

```
# default.
#

#BrowseShortNames Yes

#
# BrowseAllow: specifies an address mask to allow for incoming browser
# packets. The default is to allow packets from all addresses.
#
# BrowseDeny: specifies an address mask to deny for incoming browser
# packets. The default is to deny packets from no addresses.
#
# Both "BrowseAllow" and "BrowseDeny" accept the following notations for
# addresses:
#
#     All
#     None
#     *.domain.com
#     .domain.com
#     host.domain.com
#     nnn.*
#     nnn.nnn.*
#     nnn.nnn.nnn.*
#     nnn.nnn.nnn.nnn
#     nnn.nnn.nnn.nnn/mm
#     nnn.nnn.nnn.nnn/mmm.mmm.mmm.mmm
#     @LOCAL
#     @IF(name)
#
# The hostname/domainname restrictions only work if you have turned hostname
# lookups on!
#

#BrowseAllow address
#BrowseDeny address

#
# BrowseInterval: the time between browsing updates in seconds.  Default
# is 30 seconds.
#
# Note that browsing information is sent whenever a printer's state changes
# as well, so this represents the maximum time between updates.
#
# Set this to 0 to disable outgoing broadcasts so your local printers are
# not advertised but you can still see printers on other hosts.
#

#BrowseInterval 30

#
# BrowseOrder: specifies the order of BrowseAllow/BrowseDeny comparisons.
#
```

```
#BrowseOrder allow,deny
#BrowseOrder deny,allow

#
# BrowsePoll: poll the named server(s) for printers
#

#BrowsePoll address:port

#
# BrowsePort: the port used for UDP broadcasts.  By default this is
# the IPP port; if you change this you need to do it on all servers.
# Only one BrowsePort is recognized.
#

#BrowsePort 631

#
# BrowseRelay: relay browser packets from one address/network to another.
#

#BrowseRelay source-address destination-address
#BrowseRelay @IF(src) @IF(dst)

#
# BrowseTimeout: the timeout for network printers - if we don't
# get an update within this time the printer will be removed
# from the printer list.  This number definitely should not be
# less the BrowseInterval value for obvious reasons.  Defaults
# to 300 seconds.
#

#BrowseTimeout 300

#
# ImplicitClasses: whether or not to use implicit classes.
#
# Printer classes can be specified explicitly in the classes.conf
# file, implicitly based upon the printers available on the LAN, or
# both.
#
# When ImplicitClasses is On, printers on the LAN with the same name
# (e.g. Acme-LaserPrint-1000) will be put into a class with the same
# name. This allows you to setup multiple redundant queues on a LAN
# without a lot of administrative difficulties.  If a user sends a
# job to Acme-LaserPrint-1000, the job will go to the first available
# queue.
#
# Enabled by default.
#

#ImplicitClasses On
```

```
#
# ImplicitAnyClasses: whether or not to create "AnyPrinter" implicit
# classes.
#
# When ImplicitAnyClasses is On and a local queue of the same name
# exists, e.g. "printer", "printer@server1", "printer@server1", then
# an implicit class called "Anyprinter" is created instead.
#
# When ImplicitAnyClasses is Off, implicit classes are not created
# when there is a local queue of the same name.
#
# Disabled by default.
#

#ImplicitAnyCLasses Off

#
# HideImplicitMembers: whether or not to show the members of an
# implicit class.
#
# When HideImplicitMembers is On, any remote printers that are
# part of an implicit class are hidden from the user, who will
# then only see a single queue even though many queues will be
# supporting the implicit class.
#
# Enabled by default.
#

#HideImplicitMembers On


########
######## Security Options
########

#
# SystemGroup: the group name for "System" (printer administration)
# access.  The default varies depending on the operating system, but
# will be "sys", "system", or "root" (checked for in that order.)
#
# Debian: The default CUPS group is "lpadmin".
#

#SystemGroup lpadmin

#
# RootCertDuration: How frequently the root certificate is regenerated.
# Defaults to 300 seconds.
#

#RootCertDuration 300

#
```

```
# Access permissions for each directory served by the scheduler.
# Locations are relative to DocumentRoot...
#
# AuthType: the authorization to use:
#
#    None   - Perform no authentication
#    Basic  - Perform authentication using the HTTP Basic method.
#    Digest - Perform authentication using the HTTP Digest method.
#
#    (Note: local certificate authentication can be substituted by
#           the client for Basic or Digest when connecting to the
#           localhost interface)
#
# AuthClass: the authorization class; currently only "Anonymous", "User",
# "System" (valid user belonging to group SystemGroup), and "Group"
# (valid user belonging to the specified group) are supported.
#
# AuthGroupName: the group name for "Group" authorization.
#
# Order: the order of Allow/Deny processing.
#
# Allow: allows access from the specified hostname, domain, IP address,
# network, or interface.
#
# Deny: denies access from the specified hostname, domain, IP address,
# network, or interface.
#
# Both "Allow" and "Deny" accept the following notations for addresses:
#
#     All
#     None
#     *.domain.com
#     .domain.com
#     host.domain.com
#     nnn.*
#     nnn.nnn.*
#     nnn.nnn.nnn.*
#     nnn.nnn.nnn.nnn
#     nnn.nnn.nnn.nnn/mm
#     nnn.nnn.nnn.nnn/mmm.mmm.mmm.mmm
#     @LOCAL
#     @IF(name)
#
# The host and domain address require that you enable hostname lookups
# with "HostNameLookups On" above.
#
# The @LOCAL address allows or denies from all non point-to-point
# interfaces.  For example, if you have a LAN and a dial-up link,
# @LOCAL could allow connections from the LAN but not from the dial-up
# link.  Similarly, the @IF(name) address allows or denies from the
# named network interface, e.g. @IF(eth0) under Linux.  Interfaces are
# refreshed automatically (no more than once every 60 seconds), so
# they can be used on dynamically-configured interfaces, e.g. PPP,
```

```
# 802.11, etc.
#
# Encryption: whether or not to use encryption; this depends on having
# the OpenSSL library linked into the CUPS library and scheduler.
#
# Possible values:
#
#     Always       - Always use encryption (SSL)
#     Never        - Never use encryption
#     Required     - Use TLS encryption upgrade
#     IfRequested  - Use encryption if the server requests it
#
# The default value is "IfRequested".
#

<Location />
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
</Location>

#<Location /classes>
#
# You may wish to limit access to printers and classes, either with Allow
# and Deny lines, or by requiring a username and password.
#
#</Location>

#<Location /classes/name>
#
# You may wish to limit access to printers and classes, either with Allow
# and Deny lines, or by requiring a username and password.
#
#</Location>

<Location /jobs>
#
# You may wish to limit access to job operations, either with Allow
# and Deny lines, or by requiring a username and password.
#
AuthType Basic
AuthClass User
#Encryption Required
</Location>

#<Location /printers>
#
# You may wish to limit access to printers and classes, either with Allow
# and Deny lines, or by requiring a username and password.
#
#</Location>

#<Location /printers/name>
```

```
#
# You may wish to limit access to printers and classes, either with Allow
# and Deny lines, or by requiring a username and password.
#

## Anonymous access (default)
#AuthType None

## Require a username and password (Basic authentication)
#AuthType Basic
#AuthClass User

## Require a username and password (Digest/MD5 authentication)
#AuthType Digest
#AuthClass User

## Restrict access to local domain
#Order Deny,Allow
#Deny From All
#Allow From .mydomain.com
#</Location>

<Location /admin>
#
# You definitely will want to limit access to the administration functions.
# The default configuration requires a local connection from a user who
# is a member of the system group to do any admin tasks.  You can change
# the group name using the SystemGroup directive.
#

AuthType Basic
AuthClass System

## Restrict access to local domain
Order Deny,Allow
Deny From All
Allow From 127.0.0.1

#Encryption Required
</Location>

#
# End of "$Id: cupsd.conf.in,v 1.14 2004/02/25 20:14:51 mike Exp $".
#
```

Apéndice AG. Archivo de configuración /etc/pykota/pykota.conf

```
# PyKota sample configuration file
#
# Copy this file into the /etc/pykota/ directory
# under the name /etc/pykota/pykota.conf
#
# PyKota - Print Quotas for CUPS and LPRng
#
# (c) 2003-2004 Jerome Alet <alet@librelogiciel.com>
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.
#
# $Id: pykota.conf.sample,v 1.104 2004/10/06 08:19:29 jalet Exp $
#

[global]
# Storage backend for quotas
# only PGStorage (PostgreSQL) and LDAPStorage (OpenLDAP) are supported.
# MySQL and BerkeleyDB are planned.

# the 'postgresql' value is deprecated, use 'pgstorage' instead.
storagebackend: ldapstorage

# Quota Storage Server hostname (and optional port)
# e.g. db.example.com:5432
storageserver: ldap://gsr.pt:389

#
# name of the Quota Storage Database
storagename: dc=gsr,dc=pt

#
# Quota Storage normal user's name and password
# These two fields contain a username and optional password
# which may give readonly access to your print quota database.
#
# PLEASE ENSURE THAT THIS USER CAN'T WRITE TO YOUR PRINT QUOTA
# DATABASE, OTHERWISE ANY USER WHO COULD READ THIS CONFIGURATION
```

```
# FILE COULD CHANGE HIS PRINT QUOTA.
#
storageuser: cn=pykotauser,dc=gsr,dc=pt
storageuserpw: **********

# Should the database caching mechanism be enabled or not ?
# If unset, caching is disabled. Possible values Y/N/YES/NO
# caching mechanism works with both PostgreSQL and OpenLDAP backends
# but may be really interesting only with OpenLDAP.
#
# ACTIVATING CACHE MAY CAUSE PRECISION PROBLEMS IN PRINT ACCOUNTING
# IF AN USER PRINTS ON SEVERAL PRINTERS AT THE SAME TIME.
# YOU MAY FIND IT INTERESTING ANYWAY, ESPECIALLY FOR LDAP.
#
# FYI, I ALWAYS SET IT TO YES !
#
storagecaching: No

# Should full job history be disabled ?
# If unset or set to No, full job history is kept in the database.
# This will be useful in the future when the report generator
# will be written.
# Disabling the job history can be useful with heavily loaded
# LDAP servers, to not make the LDAP tree grow out of control.
# Disabling the job history with the PostgreSQL backend works too
# but it’s probably less useful than with LDAP.
disablehistory: No

# LDAP example, uncomment and adapt it to your own configuration :
#storagebackend: ldapstorage
#storageserver: ldap://ldap.librelogiciel.com:389
#storagename: dc=librelogiciel,dc=com
#storageuser: cn=notadmin,dc=librelogiciel,dc=com
#storageuserpw: abc.123
#
# Here we define some helpers to know where
# to plug into an existing LDAP directory
userbase: ou=people,dc=gsr,dc=pt
userrdn: uid
balancebase: ou=people,dc=gsr,dc=pt
balancerdn: uid
groupbase: ou=groups,dc=gsr,dc=pt
grouprdn: cn
printerbase: ou=printers,ou=pykota,dc=gsr,dc=pt
printerrdn: cn
jobbase: ou=jobs,ou=pykota,dc=gsr,dc=pt
userquotabase: ou=uquotas,ou=pykota,dc=gsr,dc=pt
groupquotabase: ou=gquotas,ou=pykota,dc=gsr,dc=pt
lastjobbase: ou=lastjobs,ou=pykota,dc=gsr,dc=pt
#
# How to create new accounts and groups
# authorized values are "below" and "attach(objectclass name [, fail|warn])"
#
```

```
# "below" creates the new accounts/groups as standalone entries
# below the above defined 'userbase' ou
#
# attach(objectclass name [, action]) tries to find some existing user/group
# using the above defined 'userrdn' or 'grouprdn' and 'userbase'
# 'groupbase', and attach the PyKota specific entries to it.
# if action is "warn" and no entry exists to attach to, a new
# entry is created, and a message is logged.
# if action is "fail" and no entry exists to attach to, program
# logs an error message and aborts.
# if action is not set, the default value is "fail".
#
# a possible value:  newuser: attach(posixAccount, warn)
newuser : attach(posixAccount, warn)
newgroup : attach(posixGroup, warn)
#
# LDAP attribute which stores the user's email address
usermail : mail

#
# Choose what attribute contains the list of group members
# common values are : memberUid, uniqueMember, member
groupmembers: memberUid

# Activate low-level LDAP cache yes/no
# Nothing to do with "storagecaching" which is higher level
# and database independant.
# This saves some search queries and may help with heavily
# loaded LDAP servers.
# This is EXPERIMENTAL.
#
# BEWARE : SETTING THIS TO 'YES' CAUSES PROBLEMS FOR NOW
# BETTER TO LET IT SET TO 'NO'
# ldapcache: no

# Where to log ?
# supported values : stderr, system (system means syslog,
# but don't use 'syslog' here) if the value is not set
# then the default SYSTEM applies.
logger: system

# Enable debugging ? Put YES or NO there.
# From now on, YES is the default in this sample
# configuration file, so that debugging is activated
# when configuring PyKota. After all works, just
# put NO instead to save some disk space in your
# logs.
# Actually only database queries are logged.
debug : Yes

# Mail server to use to warn users
# If the value is not set then localhost is used.
smtpserver: localhost
```

```
# Crash messages' recipient : in addition to the log files
# each software crash can be sent to the author of PyKota
# or any other person of your choice. By default this
# is disabled. The recipient pykotacrashed@librelogiciel.com
# reaches PyKota's author.
# The 'adminmail' (defined a bit below) is CCed.
#
# Privacy concerns : what is sent is only :
#
#       - a copy of the software's traceback
#       - a copy of the software's command line arguments
#       - a copy of the software's environment variables
#
# suggested value
# crashrecipient: pykotacrashed@librelogiciel.com

# Email domain
# If the value is not set, and the mail attribute for the user
# is not set in the PyKota storage, be it LDAP (see usermail directive
# above) or PostgreSQL, then email messages are sent to
# username@smtpserver
#
# If the value is set, then email messages are sent to
# username@maildomain using the SMTP server defined above
#
# Set the appropriate value below, example.com set as per RFC2606.
maildomain: gsr.pt

# Should we force usernames to be all lowercase when printing ?
# Default is No.
# This is a global option only.
# Some people reported that WinXP sends mixed case usernames
# setting 'utolower: Yes' solves the problem.
# Of course you have to use lowercase only when adding
# users with edpykota, because ALL database accesses are
# still case sensitive.
#
# If utolower is Yes, the usernames received from the printing
# system is converted to lowercase at the start of the cupspykota
# backend or of the lprngpykota filter.
#
# If utolower is No, which is the default, strict case checking
# is done, this means that users 'Jerome' and 'jerome' are
# different. Printer and groups names are ALWAYS case sensitive.
utolower: No

# Should we split usernames on a specific separator when printing ?
# Default is No, i.e. if the value is unset.
# This is a global option only.
# This option adds support for Samba's Winbind utility, which
# prefixes usernames with domain name and separator character.
# Of course if you set this then you have to use NO separator when
```

```
# adding users with edpykota.
#
# If winbind_separator is set, the usernames received from the printing
# system are split on the separator's value, and only the last part
# (real username) is used.
#
# If winbind_separator is not set, which is the default, strict
# username equality checking will be done (modulo the setting
# of the 'utolower' directive), this means that users 'DOMAIN1/jerome',
# 'Domain2/jerome' and 'jerome' are different.
# winbind_separator: /

# What is the accounting backend to use
#
# supported values :
#
#    - hardware : asks the printer for its lifetime page counter
#                 via either SNMP, AppleTalk, or any external
#                 command. This method is the method used by
#                 default in PyKota since its beginning.
#
#                 In the lines below "%(printer)s" is automatically replaced
#                 at run time with your printer's Fully Qualified Domain Name
#                 for network printers.
#                 e.g. myprinter.example.com
#
#         Recommended values :
#
#             accounter: hardware(snmp)
#
#               Extracts the printer's internal page counter via SNMP.
#
#         Or :
#
#             accounter: hardware(pjl)
#
#               Extracts the printer's internal page counter via PJL queries
#               over port tcp/9100.
#
#         Other Examples :
#
#             accounter: hardware(/usr/bin/snmpget -v1 -c public -Ov \
#               %(printer)s mib-2.43.10.2.1.4.1.1 | cut -f 2,2 -d " ")
#
#         Another untested example, using npadmin :
#
#             accounter: hardware(/usr/bin/npadmin --pagecount %(printer)s)
#
#         Another example, for AppleTalk printers which works fine :
#         (You may need the pap CUPS backend installed, and copy the
#         pagecount.ps file from untested/netatalk into /etc or any
#         appropriate location)
#
```

```
#             accounter: hardware(/usr/share/pykota/papwaitprinter.sh \
#                        "MyPrinter:LaserWriter@*" && /usr/bin/pap -p \
#                        "MyPrinter:LaserWriter@*" /usr/share/pykota/pagecount.ps \
#                         2>/dev/null | /bin/grep -v status | /bin/grep \
#                         -v Connect | /usr/bin/tail -1)
#
#         An example for parallel printers like the HP Laserjet 5MP :
#
#             accounter: hardware(/bin/cat /usr/share/pykota/pagecount.pjl \
#                 >/dev/lp0 && /usr/bin/head -2 </dev/lp0 | /usr/bin/tail -1)
#
#         This value can be set either globally or per printer or both.
#         If both are defined, the printer option has priority.
#
#         Some examples and comments provided by Bob Martel from csuohio.edu
#
#         For several printers I could not get the page count using snmpget.  I
#         resorted to snmpwalk:
#
#             accounter: hardware(/opt/local/net-snmp/bin/snmpwalk -v 1 -Cc \
#                                 -c public %(printer)s | grep \
#                                 mib-2.43.10.2.1.4.1.1 | cut -d " " -f4)
#
#         The last example is still more ugly, some of the printers only provided
#         their counters without names, but at least always on the same line:
#
#             accounter: hardware(/opt/local/net-snmp/bin/snmpwalk \
#                                 -v 1 -Cc -c public -Ov %(printer)s | \
#                                 grep Counter32 | tail -2 | head -1 | cut -d " " -f2)
#
#         An example using netcat and a preformatted PJL job which you can find
#         in the untested/pjl directory, which is sent to a JetDirect print
#         server on port 9100 :
#
#             accounter: hardware(/bin/nc -w 2 %(printer)s 9100 \
#                        </usr/share/pykota/pagecount.pjl | /usr/bin/tail -2)
#
#         An example using the contributed pagecount.pl script which does
#         the same as above, but should work on more printers :
#
#             accounter: hardware(LC_ALL=C /usr/share/pykota/pagecount.pl \
#                                 %(printer)s 9100)
#
#         NB : the LC_ALL=C is used because sometimes Perl can correctly set
#              locale and is verbose about it, causing PyKota to miss the
#              correct answer.
#
#         WARNING : In any case, when using an hardware accounter, please test
#                   the command line outside of PyKota before. This will save
#                   you some headaches in case it doesn't work as expected.
#
#         The waitprinter.sh is there to wait until the printer is idle again.
#         This should prevent a job to be sent to the printer while another one is
```

```
#         not yet finished (not all pages are printed, but the complete job is in
#         the printer)
#
#   YOU ABSOLUTELY HAVE TO BE SURE YOU HAVE A SCRIPT WHICH WAITS FOR THE
#   PRINTER BEING READY BEFORE ASKING FOR ITS INTERNAL PAGE COUNTER.
#
#   PYKOTA INCLUDES SUCH SCRIPTS FOR SNMP AND APPLETALK PRINTERS, MORE TO COME
#
#   SOME OF THE ABOVE EXAMPLES DON'T USE SUCH A SCRIPT, YOU HAVE BEEN WARNED
#
#
#   WITH THE SPECIAL MAGIC hardware(snmp) AND hardware(pjl) VALUES, PYKOTA
#   TAKES CARE OF ALL THIS FOR YOU, SO PLEASE UNDERSTAND THAT IT IS PREFERABLE
#   TO USE THESE TWO METHODS : THEY WORK FINE, REQUIRE LITTLE TO NO CPU,
#   AND DO ALL THE HARD WORK AUTOMATICALLY. IF YOU REALLY NEED TO YOU CAN USE
#   YOUR OWN EXTERNAL COMMANDS AS DESCRIBED ABOVE, JUST BE CAREFUL WITH THIS.
#
#
#    - software : delegates the job's size computation to any
#                 external command of your choice.
#
#                 best choice for this is probably to set it
#                 this way :
#
#                   accounter: software(/usr/bin/pkpgcounter)
#
#                 pkpgcounter is a command line tool which is
#                 part of PyKota and which can handle both
#                 DSC compliant or binary PostScript, PCL5, PCL6 (aka PCLXL)
#                 and PDF documents. More file formats will be added
#                 in the future, as time permits.
#
#                 while pkpgcounter is the recommended value
#                 you can use whatever command you want provided
#                 that your command accepts the job's data on its
#                 standard input and prints the job's size in pages
#                 as a single integer on its standard output.
#
# This value can be set either globally or on a per printer basis
# If both are defined, the printer option has priority.
#
# accounter: hardware(/usr/share/pykota/waitprinter.sh %(printer)s && \
#                     /usr/bin/snmpget -v1 -c public -Ov %(printer)s \
#                     mib-2.43.10.2.1.4.1.1 | cut -f 2,2 -d " ")
# accounter: hardware(snmp)
# accounter: hardware(pjl)
accounter: software(/usr/bin/pkpgcounter)

# What should we do if the accounter's subprocess doesn't return
# a valid result (for example doesn't return an integer on its stdout)
#
# Valid values are : 'continue' and 'stop'. 'stop' is the default
# if unset.
```

```
#
# 'continue' means try to process as usual, this may introduce
# accounting errors and free jobs. This was the default behavior
# until v1.20alpha5.
#
# 'stop' means fail and stop the print queue. If an accounter
# error occurs, most of the time this is a misconfiguration, so
# stopping the print queue is usually the better thing to do
# until the admin has fixed the configuration.
#
# This value can be set either globally or on a per printer basis
# If both are defined, the printer option has priority.
#
# onaccountererror: continue
onaccountererror: stop

# Print Quota administrator
# These values can be set either globally or per printer or both.
# If both are defined, the printer option has priority.
# If these values are not set, the default admin root
# and the default adminmail root@localhost are used.
admin: Sergio González González
adminmail: root@localhost

#
# Who should we send an email to in case a quota is reached ?
# possible values are : DevNull, User, Admin, Both, External(some command)
# The Both value means that the User and the Admin will receive
# an email message.
# The DevNull value means no email message will be sent.
# This value can be set either globally or per printer or both.
# If both are defined, the printer option has priority.
# If the value is not set, then the default BOTH applies.
#
#   Format of the external syntax :
#
#       mailto: external(/usr/bin/mycommand >/dev/null)
#
#   You can use :
#
#       '%(action)s'            will contain either WARN or DENY
#       '%(username)s'          will contain the user's name
#       '%(printername)s'       will contain the printer's name
#       '%(email)s'             will contain the user's email address
#       '%(message)s'           will contain the message if you want
#                               to use it.
#
#   On your command line, to pass arguments to your command.
#   Example :
#
#       mailto: external(/usr/bin/callpager %(username)s \
#                        "Quota problem on %(printername)s" >/dev/null)
#
```

```
#   To automatically send a WinPopup message (this may only work with a PDC,
#   here the same machine does Samba as PDC + CUPS) :
#
#       mailto: external(echo "%(message)s"  | /usr/bin/iconv --to-code utf-8 \
#        --from-code iso-8859-15 | /usr/bin/smbclient -M "%(username)s" 2>&1 >/dev/null)
#
#   NB : I use ISO-8859-15, but Windows expects UTF-8, so we pipe the message
#        into iconv before sending it to the Windows user.
#
# or more simply :
#
#       mailto: external(/usr/share/pykota/mailandpopup.sh %(username)s \
#                        %(printername)s "%(email)s" "%(message)s" 2>&1 >/dev/null)
#
#   NB : The mailandpopup.sh shell script is now included in PyKota
#
#   NB : in ANY case, don't forget to redirect your command's standard output
#        somewhere (e.g. >/dev/null) so that there's no perturbation to the
#        underlying layer (filter or backend)
#
mailto: both

#
# Grace delay in days
# This value can be set either globally or per printer or both.
# If both are defined, the printer option has priority.
# If the value is not set then the default seven (7) days applies.
gracedelay: 7

#
# Poor man's threshold
# If account balance reaches below this amount,
# a warning message is sent by email
#
# If unset, default poor man's threshold is 1.0.
# This option can only appear in the global section
poorman: 2.0

# Poor man's warning message
# The warning message that is sent if the "poorman" value is reached
# Again this must appear in the global section
poorwarn: Su saldo en la cuota de impresión es bajo.
 Dentro de poco no podrá volver a imprimir.

# Soft limit reached warning message
# The warning message that is sent if the soft quota limit is reached
# May appear either globally or on a per-printer basis
softwarn: Ha alcanzado su límite blando en la cuota de impresión.
 Esto significa que podrá seguir imprimiendo algún tiempo,
 pero debería contactar con su administrador para comprar
 más cuota de impresión.

# Hard limit reached error message
```

```
# The error message that is sent if the hard quota limit is reached
# May appear either globally or on a per-printer basis
hardwarn: Ha alcanzado su límite duro en la cuota de impresión.
 Esto significa que no podrá volver a imprimir.
 Contacte con su administrador en <root@gsr.pt> tan
 pronto como le sea posible para solucionar el
 problema.

# one section per printer, or no other section at all if all options
# are defined globally.
# Each section's name must be the same as the printer's queue name as defined
# in your printing system, be it CUPS or LPRng, between square brackets, for
# example a print queue named 'hpmarketing' would appear in this file as
# [hpmarketing]


# Default policy to apply when either :
#
#       - Printer doesn't exist in PyKota's database
#       - User doesn't exist in PyKota's database
#       - User has no quota entry for this Printer in PyKota's database
#
# Value can be either allow or deny or external(some command here)
#
# This value can be set either globally or per printer or both.
# If both are defined, the printer option has priority.
# If the value is not set then the default policy DENY applies.
# There's no policy wrt inexistant groups, they are ignored.
#
# external policy can be used to launch any external command of your choice,
# for example to automatically add the user to the quota storage
# if he is unknown. Example :
#
#   policy: external(/usr/bin/edpykota --add --printer %(printername)s \
#                    --softlimit 50 --hardlimit 60 %(username)s >/dev/null)
#
# NB : If you want to limit users by their account balance value, it is preferable to
# use the following policy to automate user account creation on first print :
#
#   policy: external(/usr/bin/autopykota --initbalance 25.0 >/dev/null)
#
#   This will automatically add the user if he doesn't already exist, and
#   set his initial balance value to 25.0 (for example). If the user already
#   exists then his balance value will not be modified.
#   Please don't use autopykota if you want to limit your users by page
#   quota, and in any case, carefully read autopykota's help or manpage
#   and understand its goal before using it in your own configuration.
#
# Of course you can launch any command of your choice with this, e.g. :
#
#   policy: external(/usr/local/bin/myadminscript.sh %(username)s >/dev/null)

# You can use :
```

```
#
#       '%(username)s'          will contain the user's name
#       '%(printername)s'       will contain the printer's name
#
#   On your command line, to pass arguments to your command.
#
#   NB : Don't forget to redirect your command's standard output somewhere
#        (e.g. >/dev/null) so that there's no perturbation to the underlying
#        layer (filter or backend)
#
# If the printer, user, or user quota entry still doesn't exist after
# external policy command was launched (the external command didn't add it),
# or if an error occured during the execution of the external policy
# command, then the job is rejected.
#
policy: deny

# Pre and Post Hooks
# These directives allow the easy plug-in of any command of your choice
# at different phases of PyKota's execution.
# Pre and Post Hooks can access some of PyKota's internal information
# by reading environment variables as described below.
# The actual phase of PyKota's execution is available in the
# PYKOTAPHASE environment variable.
# Pre and Post Hooks can be defined either globally, per printer,
# or both. If both are defined, the printer specific hook has
# priority.
#
# List of available environment variables :
# NB : Most of these variables are also available during the execution
# of external commands defined in the accounter and mailto
# directives.
#
# PYKOTAMD5SUM : Contains an hexadecimal digest of the md5 sum of the job's datas
# PYKOTAPHASE : BEFORE or AFTER the job is sent to the printer
# PYKOTAACTION : ALLOW or DENY or WARN for current print job
# PYKOTAUSERNAME : user's name
# PYKOTAPRINTERNAME : printer's name
# PYKOTAPGROUPS : list of printers groups the current printer is a member of
# PYKOTAJOBID : job's id
# PYKOTATITLE : job's title
# PYKOTAFILENAME : job's filename
# PYKOTACOPIES : number of copies
# PYKOTAOPTIONS : job's options
# PYKOTABALANCE : user's account balance
# PYKOTALIFETIMEPAID : user's grand total paid
# PYKOTALIMITBY : user print limiting factor, for example 'quota' or 'balance'
# PYKOTAPAGECOUNTER : user's page counter on this printer
# PYKOTALIFEPAGECOUNTER : user's life time page counter on this printer
# PYKOTASOFTLIMIT : user's soft page limit on this printer
# PYKOTAHARDLIMIT : user's hard page limit on this printer
# PYKOTADATELIMIT : user's soft to hard limit date limit on this printer
# PYKOTASTATUS : contains "CANCELLED" when SIGTERM was received by PyKota
```

```
#               else is not set.
# PYKOTAJOBSIZEBYTES : contains the job's size in bytes. Always available.
# PYKOTAPRECOMPUTEDJOBSIZE : contains the precomputed job's size (with enforcement: strict
# PYKOTAPRECOMPUTEDJOBPRICE : contains the precomputed job's price (with enforcement: str
# PYKOTAJOBORIGINATINGHOSTNAME : contains the client's hostname if
#                                it is possible to retrieve it.
# PYKOTAPRINTERHOSTNAME : the printer's hostname or IP address for network
#                         printers, or "localhost" if not defined or not
#                         meaningful.

# PreHook : gets executed after being sure the user, printer and user quota
# entry on the printer both exist in the PyKota database, and after
# checking if the user is allowed to print or not, but just before
# the job is sent to the printer (if allowed)
# prehook has access to many environment variables :
#
# PYKOTAACTION contains either "ALLOW", "WARN" or "DENY" and
# represents the action which is to be done wrt the print job.
# PYKOTAPHASE contains 'BEFORE' during execution of prehook
#
# uncomment the line below to see what environment variables are available
# prehook: /usr/bin/printenv >/tmp/before

# PostHook : gets executed after the job has been added to the history.
# posthook has access to all the environment variables defined above,
# as well as two additionnal environment variables : PYKOTAJOBPRICE
# and PYKOTAJOBSIZE.
# PYKOTAPHASE contains 'AFTER' during execution of posthook.
#
# uncomment the line below to see what environment variables are available
# posthook: /usr/bin/printenv >/tmp/after

# How should enforcement be done for this printer ?
#
# "laxist" is the default if value is not set, and allows users
# to be over quota on their last job.
#
# "strict" tries to prevent users from ever being over quota.
#
# Enforcement can be defined either globally, per printer,
# or both. If both are defined, the printer specific enforcement
# setting has priority.
#
# valid values : "strict" or "laxist"
#
# default value
# enforcement : laxist
enforcement : strict
```

Apéndice AH. Archivo de configuración /etc/pykota/pykotadmin.conf

```
# PyKota sample administrator's configuration file
#
# Copy it into the /etc/pykota/ directory under
# the /etc/pykota/pykotadmin.conf name, and
# ensure that only the root user and the user
# the printing system is run as can read it.
#
# Under NO circumstances regular users should
# be allowed to read this file.
#
# PyKota - Print Quotas for CUPS and LPRng
#
# (c) 2003-2004 Jerome Alet <alet@librelogiciel.com>
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.
#
# $Id: pykotadmin.conf.sample,v 1.2 2004/01/08 14:10:32 jalet Exp $
#

#
# THIS FILE CONTAINS SENSITIVE DATAS LIKE A USERNAME AND PASSWORD
# WHICH ALLOW READ/WRITE ACCESS TO YOUR PRINT QUOTA DATABASE.
#
# ONLY THE root USER AND THE USER THE PRINTING SYSTEM IS RUN AS
# (e.g. lp) SHOULD BE ALLOWED TO READ THIS FILE !
#

#
# THIS FILE CAN ONLY CONTAIN A [global] SECTION AND TWO FIELDS
# NAMED storageadmin AND storageadminpw
#

[global]

# Quota Storage administrator's name and password
storageadmin: cn=pykotaadmin,dc=gsr,dc=pt
storageadminpw: **********
```

Apéndice AI. Archivo de configuración /var/www/phpldapadmin/config.php

```
<?php

/*
 *                  The phpLDAPadmin config file
 *
 *   This is where you customize phpLDAPadmin. The most important
 *   part is immediately below: The "LDAP Servers" section.
 *   You must specify at least one LDAP server there. You may add
 *   as many as you like. You can also specify your language, and
 *   many other options.
 *
 */

// Your LDAP servers
$i=0;
$servers = array();

/*  A convenient name that will appear in the tree viewer and throughout
    phpLDAPadmin to identify this LDAP server to users. */
$servers[$i]['name'] = 'TodoSCSI';

/*  Examples:

       'ldap.example.com',
       'ldaps://ldap.example.com/',
       'ldapi://%2fusr%local%2fvar%2frun%2fldapi'
        (Unix socket at /usr/local/var/run/ldap)

    Note: Leave 'host' blank to make phpLDAPadmin ignore this server. */
$servers[$i]['host'] = 'ldap://gsr.pt';

/*  The base DN of your LDAP server. Leave this blank to have phpLDAPadmin
    auto-detect it for you. */
$servers[$i]['base'] = 'dc=gsr,dc=pt';

/*  The port your LDAP server listens on (no quotes). 389 is standard. */
$servers[$i]['port'] = 389;

/*  Three options for auth_type:

       1. 'cookie': you will login via a web form, and a client-side cookie will
          store your login dn and password.
       2. 'session': same as cookie but your login dn and password are stored on
          the web server in a session variable.
       3. 'config': specify your login dn and password here in this config file.
          No login will be required to use phpLDAPadmin for this server.

    Choose wisely to protect your authentication information appropriately
```

```
    for your situation. */
$servers[$i]['auth_type'] = 'session';

/* The DN of the user for phpLDAPadmin to bind with. For anonymous binds or
   'cookie' or 'session' auth_types, leave the login_dn and login_pass blank.
   If you specify a login_attr in conjunction with a cookie or session auth_type,
   then you can also specify the login_dn/login_pass here for searching the
   directory for users (ie, if your LDAP server does not allow anonymous binds. */
$servers[$i]['login_dn'] = 'cn=admin,dc=gsr,dc=pt';

/* Your LDAP password. If you specified an empty login_dn above, this MUST
   also be blank. */
$servers[$i]['login_pass'] = '';

/* Use TLS (Transport Layer Security) to connect to the LDAP server. */
$servers[$i]['tls'] = true;

/* If the link between your web server and this LDAP server is slow, it is
   recommended that you set 'low_bandwidth' to true. This will cause
   phpLDAPadmin to forego some "fancy" features to conserve bandwidth. */
$servers[$i]['low_bandwidth'] = false;

/*  Default password hashing algorithm. One of md5, ssha, sha, md5crpyt,
    smd5, blowfish, crypt or leave blank for now default algorithm. */
$servers[$i]['default_hash'] = 'crypt';

/* If you specified 'cookie' or 'session' as the auth_type above, you can optionally
   specify here an attribute to use when logging in. If you enter 'uid' and login as
   'dsmith', phpLDAPadmin will search for (uid=dsmith) and log in as that user. Leave
   blank or specify 'dn' to use full DN for logging in. Note also that if your LDAP
   server requires you to login to perform searches, you can enter the DN to use when
   searching in 'login_dn' and 'login_pass' above. */
$servers[$i]['login_attr'] = 'dn';

/* If 'login_attr' is used above such that phpLDAPadmin will search for your DN
   at login, you may restrict the search to a specific objectClass.
   E.g., set this to 'posixAccount' or 'inetOrgPerson', depending upon your setup. */
$servers[$i]['login_class'] = '';

/* Specify true If you want phpLDAPadmin to not display or permit any
   modification to the LDAP server. */
$servers[$i]['read_only'] = false;

/* Specify false if you do not want phpLDAPadmin to draw the 'Create new'
   links in the tree viewer. */
$servers[$i]['show_create'] = true;

/* This feature allows phpLDAPadmin to automatically determine the next
   available uidNumber for a new entry. */
$servers[$i]['enable_auto_uid_numbers'] = true;

/* The mechanism to use when finding the next available uidNumber. Two possible
   values: 'uidpool' or 'search'. The 'uidpool' mechanism uses an existing
```

```
   uidPool entry in your LDAP server to blindly lookup the next available
   uidNumber. The 'search' mechanism searches for entries with a uidNumber value
   and finds the first available uidNumber (slower). */
$servers[$i]['auto_uid_number_mechanism'] = 'search';

/* The DN of the search base when the 'search' mechanism is used above. */
$servers[$i]['auto_uid_number_search_base'] = 'ou=people,dc=gsr,dc=pt';

/* The minimum number to use when searching for the next available UID number
   (only when 'search' is used for auto_uid_number_mechanism' */
$servers[$i]['auto_uid_number_min'] = 1000;

/* The DN of the uidPool entry when 'uidpool' mechanism is used above. */
$servers[$i]['auto_uid_number_uid_pool_dn'] = 'cn=uidPool,dc=example,dc=com';

/* If you set this, then phpldapadmin will bind to LDAP with this user
   ID when searching for the uidnumber. The idea is, this user id would
   have full (readonly) access to uidnumber in your ldap directory (the
   logged in user may not), so that you can be guaranteed to get a unique
   uidnumber for your directory. */
$servers[$i]['auto_uid_number_search_dn'] = '';

/* The password for the dn above */
$servers[$i]['auto_uid_number_search_dn_pass'] = '';



// If you want to configure additional LDAP servers, do so below.
#$i++;
#servers[$i]['name'] = 'Another server';
#servers[$i]['host'] = '';
#servers[$i]['base'] = 'dc=gsr,dc=pt';
#servers[$i]['port'] = 636;
#servers[$i]['auth_type'] = 'session';
#servers[$i]['login_dn'] = '';
#servers[$i]['login_pass'] = '';
#servers[$i]['tls'] = true;
#servers[$i]['low_bandwidth'] = false;
#servers[$i]['default_hash'] = 'crypt';
#servers[$i]['login_attr'] = 'dn';
#servers[$i]['login_class'] = '';
#servers[$i]['read_only'] = false;
#servers[$i]['show_create'] = true;
#servers[$i]['enable_auto_uid_numbers'] = false;
#servers[$i]['auto_uid_number_mechanism'] = 'search';
#servers[$i]['auto_uid_number_search_base'] = 'ou=People,dc=example,dc=com';
#servers[$i]['auto_uid_number_min'] = 1000;
#servers[$i]['auto_uid_number_uid_pool_dn'] = 'cn=uidPool,dc=example,dc=com';

// If you want to configure more LDAP servers, copy and paste the above
// (including the "$i++;")

// The temporary storage directory where we will put jpegPhoto data
```

```
// This directory must be readable and writable by your web server
$jpeg_temp_dir = "/tmp";       // Example for Unix systems
//$jpeg_temp_dir = "c:\\temp"; // Example for Windows systems

/**                            **/
/**   Appearance and Behavior  **/
/**                            **/

// Aliases and Referrrals
//
// Similar to ldapsearh's -a option, the following options allow you to configure
// how phpLDAPadmin will treat aliases and referrals in the LDAP tree.
// For the following four settings, avaialable options include:
//
//    LDAP_DEREF_NEVER     - aliases are never dereferenced (eg, the contents of
//                           the alias itself are shown and not the referenced entry).
//    LDAP_DEREF_SEARCHING - aliases should be dereferenced during the search but
//                           not when locating the base object of the search.
//    LDAP_DEREF_FINDING   - aliases should be dereferenced when locating the base
//                           object but not during the search.
//    LDAP_DEREF_ALWAYS    - aliases should be dereferenced always (eg, the contents
//                           of the referenced entry is shown and not the aliasing entry)

// How to handle references and aliases in the search form. See above for options.
$search_deref = LDAP_DEREF_ALWAYS;

// How to handle references and aliases in the tree viewer. See above for options.
$tree_deref = LDAP_DEREF_NEVER;

// How to handle references and aliases for exports. See above for options.
$export_deref = LDAP_DEREF_NEVER;

// How to handle references and aliases when viewing entries. See above for options.
$view_deref = LDAP_DEREF_NEVER;


// The language setting. If you set this to 'auto', phpLDAPadmin will
// attempt to determine your language automatically. Otherwise, available
// lanaguages are: 'ct', 'de', 'en', 'es', 'fr', 'it', 'nl', and 'ru'
// Localization is not complete yet, but most strings have been translated.
// Please help by writing language files. See lang/en.php for an example.
$language = 'auto';

// Set to true if you want to draw a checkbox next to each entry in the tree viewer
// to be able to delete multiple entries at once
$enable_mass_delete = false;

// Set to true if you want LDAP data to be displayed read-only (without input fields)
// when a user logs in to a server anonymously
$anonymous_bind_implies_read_only = true;

// Set to true if you want phpLDAPadmin to redirect anonymous
// users to a search form with no tree viewer on the left after
```

```
// logging in.
$anonymous_bind_redirect_no_tree = false;

// If you used auth_type 'form' in the servers list, you can adjust how long the
// cookie will last (default is 0 seconds, which expires when you close the browser)
$cookie_time = 0; // seconds

// How many pixels wide do you want your left frame view (for the tree browser)
$tree_width = 320; // pixels

// How long to keep jpegPhoto temporary files in the jpeg_temp_dir directory
// (in seconds)
$jpeg_tmp_keep_time = 120; // seconds

// Would you like to see helpful hint text occacsionally?
$show_hints = true; // set to false to disable hints

// When using the search page, limit result size to this many entries
$search_result_size_limit = 50;

// If true, display password values as ******. Otherwise display them in clear-text
// If you use clear-text passwords, it is recommended to set this to true. If you use
// hashed passwords (sha, md5, crypt, etc), hashed passwords are already obfuscated by
// the hashing algorithm and this should probably be left false.
$obfuscate_password_display = false;

/**                              **/
/** Simple Search Form Config **/
/**                              **/

// Which attributes to include in the drop-down menu of the simple search form
// (comma-separated) Change this to suit your needs for convenient searching.
// Be sure to change the corresponding list below ($search_attributes_display)
$search_attributes = "uid, cn, gidNumber, objectClass, telephoneNumber, mail, street";

// This list corresponds to the list directly above. If you want to present
// more readable names for your search attributes, do so here. Both lists
// must have the same number of entries.
$search_attributes_display = "User Name, Common Name, Group ID, Object Class, Phone \
                              Number, Email, Address";

// The list of attributes to display in each search result entry.
// Note that you can add * to the list to display all attributes
$search_result_attributes = "cn, sn, uid, postalAddress, telephoneNumber";

// You can re-arrange the order of the search criteria on the simple search
// form by modifying this array. You cannot however change the names of the
// criteria. Criteria names will be translated at run-time.
$search_criteria_options = array( "equals", "starts with", "contains", \
                                  "ends with", "sounds like" );

// If you want certain attributes to be editable as multi-line, include them
// in this list. A multi-line textarea will be drawn instead of a single-line text field
```

```
$multi_line_attributes = array( "postalAddress", "homePostalAddress", "personalSignature"

// A list of syntax OIDs which support multi-line attribute values:
$multi_line_syntax_oids = array(
                          // octet string syntax OID:
                          "1.3.6.1.4.1.1466.115.121.1.40",
                          // postal address syntax OID:
                          "1.3.6.1.4.1.1466.115.121.1.41"  );

/**                                       **/
/** User-friendly attribute translation   **/
/**                                       **/

$friendly_attrs = array();

// Use this array to map attribute names to user friendly names. For example, if you
// don't want to see "facsimileTelephoneNumber" but rather "Fax".

$friendly_attrs[ 'facsimileTelephoneNumber' ] =        'Fax';
$friendly_attrs[ 'telephoneNumber' ]  =                'Phone';

/**                                       **/
/** Hidden attributes                     **/
/**                                       **/

// You may want to hide certain attributes from being displayed in the editor screen
// Do this by adding the desired attributes to this list (and uncomment it). This
// only affects the editor screen. Attributes will still be visible in the schema
// browser and elsewhere. An example is provided below:

//$hidden_attrs = array( 'jpegPhoto', 'objectClass' );

/**                                       **/
/** Read-only attributes                  **/
/**                                       **/

// You may want to phpLDAPadmin to display certain attributes as read only, meaning
// that users will not be presented a form for modifying those attributes, and they
// will not be allowed to be modified on the "back-end" either. You may configure
// this list here:

//$read_only_attrs = array( 'objectClass' );

// An example of how to specify multiple read-only attributes:
// $read_only_attrs = array( 'jpegPhoto', 'objectClass', 'someAttribute' );

/**                                       **/
/** Predefined Queries (canned views)     **/
/**                                       **/

// To make searching easier, you may setup predefined queries below
// (activate the lines by removing "//")
//$q=0;
```

```
//$queries = array();
// /* The name that will appear in the simple search form */
//$queries[$q]['name'] = 'Samba Users';
// /* The ldap server to query, must be defined in the $servers list above */
//$queries[$q]['server'] = '0';
// /* The base to search on */
//$queries[$q]['base'] = 'dc=gsr,dc=pt';
// /* The search scope (sub, base, one) */
//$queries[$q]['scope'] = 'sub';
// /* The LDAP filter to use */
//$queries[$q]['filter'] = '(&(objectclass=sambaAccount)(objectClass=posixAcount))';
// /* The attributes to return */
//$queries[$q]['attributes'] = 'uid, smbHome, uidNumber';


// Add more pre-defined queries by copying the text below
//$q++;
//$queries[$q]['name'] = 'Organizations';
//$queries[$q]['server'] = '0';
//$queries[$q]['base'] = 'dc=gsr,dc=pt';
//$queries[$q]['scope'] = 'sub';
//$queries[$q]['filter'] = '(|(objeCtclass=organization)(objectClass=organizationalUnit)
//$queries[$q]['attributes'] = 'ou, o';

//$q++;
//$queries[$q]['name'] = 'Last name starts with S';
//$queries[$q]['server'] = '0';
//$queries[$q]['base'] = 'dc=gsr,dc=pt';
//$queries[$q]['scope'] = 'sub';
//$queries[$q]['filter'] = '(sn=s*)';
//$queries[$q]['attributes'] = '*';

?>
```

Apéndice AJ. Archivo de configuración /var/www/phpldapadmin/templates/template_config

```
<?php
// $Header: /cvsroot/phpldapadmin/phpldapadmin/templates/template_config.php,v \
                                          1.17 2004/05/08 11:14:55 xrenard Exp $

/**
 * template_config.php
 * -------------------
 * General configuration file for templates.
 * File Map:
 * 1 - Generic templates configuration
 * 2 - Samba template configuration
 * 3 - method used in template and other files
 */


/*##############################################################################################
## Templates for entry creation                                                               ##
## ----------------------------                                                               ##
##                                                                                            ##
## Fill in this array with templates that you can create to suit your needs.                  ##
## Each entry defines a description (to be displayed in the template list) and                ##
## a handler, which is a file that will be executed with certain POST vars set.               ##
## See the templates provided here for examples of how to make your own template.             ##
##                                                                                            ##
##############################################################################################*/


$templates = array();

$templates[] =
        array(  'desc'    => 'User Account',
                'icon'    => 'images/user.png',
                'handler' => 'new_user_template.php' );
  // You can use the 'regexp' directive to restrict where
  // entries can be created for this template
                //'regexp' => '^ou=People,o=.*,c=.*$'
  //'regexp' => '^ou=People,dc=.*,dc=.*$'

$templates[] =
        array(  'desc'    => 'Address Book Entry (inetOrgPerson)',
                'icon'    => 'images/user.png',
                'handler' => 'new_address_template.php' );

$templates[] =
        array(  'desc'    => 'Kolab User Entry',
                'icon'    => 'images/user.png',
                'handler' => 'new_kolab_template.php' );
```

```
$templates[] =
        array(  'desc'    => 'Organizational Unit',
                'icon'    => 'images/ou.png',
                'handler' => 'new_ou_template.php' );

$templates[] =
        array(  'desc'    => 'Posix Group',
                'icon'    => 'images/ou.png',
                'handler' => 'new_posix_group_template.php' );

$templates[] =
        array(  'desc'    => 'Samba NT Machine',
                'icon'    => 'images/nt_machine.png',
                'handler' => 'new_nt_machine.php' );
$templates[] =
        array(  'desc'    => 'Samba 3 NT Machine',
                'icon'    => 'images/nt_machine.png',
                'handler' => 'new_smb3_nt_machine.php' );
/*$templates[] =
        array(  'desc'    => 'Samba  User',
                'icon'    => 'images/nt_user.png',
                'handler' => 'new_smbuser_template.php' );
*/
$templates[] =
        array(  'desc'    => 'Samba 3 User',
                'icon'    => 'images/nt_user.png',
                'handler' => 'new_smb3_user_template.php' );
$templates[] =
        array(  'desc'    => 'Samba 3 Group Mapping',
                'icon'    => 'images/ou.png',
                'handler' => 'new_smbgroup_template.php' );

$templates[] =
        array(  'desc'    => 'DNS Entry',
                'icon'    => 'images/dc.png',
                'handler' => 'new_dns_entry.php' );

$templates[] =
 array(  'desc'    => 'Simple Security Object',
  'icon'    => 'images/user.png',
  'handler' => 'new_security_object_template.php' );

$templates[] =
 array(  'desc'    => 'Custom',
  'icon'    => 'images/object.png',
  'handler' => 'custom.php' );


/*##############################################################################################
## POSIX GROUP TEMPLATE CONFIGURATION                                                         ##
## ---------------------------------                                                          ##
##                                                                                            ##
##############################################################################################*/
```

```
// uncomment to set the base dn of posix groups
// default is set to the base dn of the server
$base_posix_groups="ou=groups,dc=gsr,dc=pt";



/*##############################################################################################
##  SAMBA TEMPLATE CONFIGURATION                                                              ##
##  ----------------------------                                                              ##
##                                                                                            ##
##  In order to use the samba templates, you might edit the following properties:             ##
##  1 - $mkntpwdCommand : the path to the mkntpwd utility provided with/by Samba.             ##
##  2 - $default_samba3_domains : the domain name and the domain sid.                         ##
##                                                                                            ##
##############################################################################################*/

// path 2 the mkntpwd utility (Customize)
$mkntpwdCommand = "/usr/sbin/smbldap-passwd";

// Default domains definition (Customize)
//   (use 'net getlocalsid' on samba server)
$default_samba3_domains = array();
$default_samba3_domains[] =
        array(  'name'   => 'GSRDOMAIN',
                'sid' => 'S-1-5-21-2817058862-34499604-3382793611' );

// The base dn of samba group. (CUSTOMIZE)
$samba_base_groups = "ou=groups,dc=gsr,dc=pt";


//Definition of built-in local groups
$built_in_local_groups = array(
                "S-1-5-21-2817058862-34499604-3382793611-512" => "Administrators",
                "S-1-5-21-2817058862-34499604-3382793611-513" => "Users",
                "S-1-5-21-2817058862-34499604-3382793611-514" => "Guests",
                "S-1-5-21-2817058862-34499604-3382793611-21007" => "Power Users",
                "S-1-5-21-2817058862-34499604-3382793611-21009" => "Account Operators",
                "S-1-5-21-2817058862-34499604-3382793611-21011" => "Server Operators",
                "S-1-5-21-2817058862-34499604-3382793611-2101" => "Print Operators",
                "S-1-5-21-2817058862-34499604-3382793611-21015" => "backup Operators",
                "S-1-5-21-2817058862-34499604-3382793611-21017" => "Replicator" );


/*##############################################################################################
##  Methods used in/by templates                                                              ##
##  ----------------------------                                                              ##
##############################################################################################*/

/*
 * Returns the name of the template to use based on the DN and
 * objectClasses of an entry. If no specific modification
```

```
 * template is available, simply return 'default'. The caller
 * should append '.php' and prepend 'templates/modification/'
 * to the returned string to get the file name.
 */

function get_template( $server_id, $dn )
{
        // fetch and lowercase all the objectClasses in an array
        $object_classes = get_object_attr( $server_id, $dn, 'objectClass', true );

        if( $object_classes === null || $object_classes === false)
                return 'default';

        foreach( $object_classes as $i => $class )
                $object_classes[$i] = strtolower( $class );

        $rdn = get_rdn( $dn );
 if( in_array( 'groupofnames', $object_classes ) ||
     in_array( 'groupofuniquenames', $object_classes ) )
      return 'group_of_names';
 /*
        if( in_array( 'person', $object_classes ) &&
            in_array( 'posixaccount', $object_classes ) )
                return 'user';
 */
 // TODO: Write other templates and criteria therefor
 // else if ...
 //    return 'some other template';
 // else if ...
 //    return 'some other template';
 // etc.

 return 'default';
}

/**
 * Return the domains info
 *
 */

function get_samba3_domains(){
  global $default_samba3_domains;

  // do the search for the sambadomainname object here
  // In the meantime, just return the default domains
  return $default_samba3_domains;
}


/**
 * Utily class to get the samba passwords.
 */
```

```
class MkntPasswdUtil{


  var $clearPassword = NULL;
  var $sambaPassword ;
  function MkntPasswdUtil(){
    $sambaPassword = array("sambaLMPassword" => NULL,
      "sambaNTPassword" => NULL);
  }

  function createSambaPasswords($password){
    global $mkntpwdCommand;
    $this->clearPassword = $password;
    file_exists ( $mkntpwdCommand ) && is_executable ( $mkntpwdCommand ) or \
                  pla_error(' Unable to create the Samba passwords. Please, \
                  check the configuration in template_config.php');
    $sambaPassCommand = $mkntpwdCommand . " " . $password;
    if($sambaPassCommandOutput = shell_exec($sambaPassCommand)){
      $this->sambaPassword['sambaLMPassword'] = trim( substr( \
             $sambaPassCommandOutput , 0 , strPos( $sambaPassCommandOutput,':' ) ) );
      $this->sambaPassword['sambaNTPassword'] = trim( substr( \
             $sambaPassCommandOutput, strPos( $sambaPassCommandOutput ,':' ) +1 ) );
      return true;
    }
    else{
      return false;
    }
  }

  function getSambaLMPassword(){
    return $this->sambaPassword['sambaLMPassword'];
  }

  function getSambaNTPassword(){
    return $this->sambaPassword['sambaNTPassword'];
  }

  function getSambaClearPassword(){
    return $this->clearPassword;
  }

  function valueOf($key){
    return  $this->sambaPassword[$key];
  }

}


/**
 * Return posix group entries
 *
 */
```

```
function get_posix_groups( $server_id , $base_dn = NULL ){
  global $servers;
  if( is_null( $base_dn ) )
    $base_dn = $servers[$server_id]['base'];

  $results = pla_ldap_search( $server_id, "objectclass=posixGroup", $base_dn, array() );
  if( !$results )
    return false;
  else
    return $results;
}
?>
```

Apéndice AK. Archivo de configuración /etc/smbldap-tools/smbldap.conf

```
# $Source: /opt/cvs/samba/smbldap-tools/smbldap.conf,v $
# $Id: smbldap.conf,v 1.14 2004/06/25 20:57:51 jtournier Exp $
#
# smbldap-tools.conf : Q & D configuration file for smbldap-tools

#  This code was developped by IDEALX (http://IDEALX.org/) and
#  contributors (their names can be found in the CONTRIBUTORS file).
#
#                 Copyright (C) 2001-2002 IDEALX
#
#  This program is free software; you can redistribute it and/or
#  modify it under the terms of the GNU General Public License
#  as published by the Free Software Foundation; either version 2
#  of the License, or (at your option) any later version.
#
#  This program is distributed in the hope that it will be useful,
#  but WITHOUT ANY WARRANTY; without even the implied warranty of
#  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#  GNU General Public License for more details.
#
#  You should have received a copy of the GNU General Public License
#  along with this program; if not, write to the Free Software
#  Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
#  USA.

#  Purpose :
#       . be the configuration file for all smbldap-tools scripts

##############################################################################
#
# General Configuration
#
##############################################################################

# Put your own SID
# to obtain this number do: net getlocalsid
SID="S-1-5-21-2817058862-34499604-3382793611"

##############################################################################
#
# LDAP Configuration
#
##############################################################################

# Notes: to use to dual ldap servers backend for Samba, you must patch
# Samba with the dual-head patch from IDEALX. If not using this patch
# just use the same server for slaveLDAP and masterLDAP.
# Those two servers declarations can also be used when you have
```

```
# . one master LDAP server where all writing operations must be done
# . one slave LDAP server where all reading operations must be done
#   (typically a replication directory)

# Ex: slaveLDAP=127.0.0.1
slaveLDAP="gsr.pt"
slavePort="389"

# Master LDAP : needed for write operations
# Ex: masterLDAP=127.0.0.1
masterLDAP="gsr.pt"
masterPort="389"

# Use TLS for LDAP
# If set to 1, this option will use start_tls for connection
# (you should also used the port 389)
ldapTLS="1"

# How to verify the server's certificate (none, optional or require)
# see "man Net::LDAP" in start_tls section for more details
verify="require"

# CA certificate
# see "man Net::LDAP" in start_tls section for more details
cafile="/etc/ldap/ssl/cacert.pem"

# certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientcert="/home/certs/ldap.cliente.cert.pem"

# key certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientkey="/home/certs/ldap.cliente.key.pem"

# LDAP Suffix
# Ex: suffix=dc=IDEALX,dc=ORG
suffix="dc=gsr,dc=pt"

# Where are stored Users
# Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
usersdn="ou=people,${suffix}"

# Where are stored Computers
# Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
computersdn="ou=machines,${suffix}"

# Where are stored Groups
# Ex groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
groupsdn="ou=groups,${suffix}"

# Where are stored Idmap entries (used if samba is a domain member server)
# Ex groupsdn="ou=Idmap,dc=IDEALX,dc=ORG"
#idmapdn="ou=Idmap,${suffix}"
```

```
# Where to store next uidNumber and gidNumber available
#sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"

# Default scope Used
scope="sub"

# Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA)
hash_encrypt="MD5"

# if hash_encrypt is set to CRYPT, you may set a salt format.
# default is "%s", but many systems will generate MD5 hashed
# passwords if you use "$1$%.8s". This parameter is optional!
crypt_salt_format="%s"

##############################################################################
#
# Unix Accounts Configuration
#
##############################################################################

# Login defs
# Default Login Shell
# Ex: userLoginShell="/bin/bash"
userLoginShell="/bin/bash"

# Home directory
# Ex: userHome="/home/%U"
userHome="/home/samba/users/%U"

# Gecos
userGecos="System User"

# Default User (POSIX and Samba) GID
defaultUserGid="1001"

# Default Computer (Samba) GID
defaultComputerGid="1000"

# Skel dir
skeletonDir="/etc/skel"

# Default password validation time (time in days) Comment the next line if
# you don’t want password to be enable for defaultMaxPasswordAge days (be
# careful to the sambaPwdMustChange attribute’s value)
# defaultMaxPasswordAge="99"

##############################################################################
#
# SAMBA Configuration
#
##############################################################################
```

```
# The UNC path to home drives location (%U username substitution)
# Ex: \\My-PDC-netbios-name\homes\%U
# Just set it to a null string if you want to use the smb.conf 'logon home'
# directive and/or disable roaming profiles
userSmbHome="\\TODOSCSI\%U"

# The UNC path to profiles locations (%U username substitution)
# Ex: \\My-PDC-netbios-name\profiles\%U
# Just set it to a null string if you want to use the smb.conf 'logon path'
# directive and/or disable roaming profiles
userProfile="\\TODOSCSI\profiles\%U"

# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
# Ex: H: for H:
userHomeDrive="H:"

# The default user netlogon script name (%U username substitution)
# if not used, will be automatically username.cmd
# make sure script file is edited under dos
# Ex: %U.cmd
# userScript="startup.cmd" # make sure script file is edited under dos
userScript=""

# Domain appended to the users "mail"-attribute
# when smbldap-useradd -M is used
mailDomain="gsr.pt"

##############################################################################
#
# SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
#
##############################################################################

# Allows not to use smbpasswd (if with_smbpasswd == 0 in smbldap_conf.pm) but
# prefer Crypt::SmbHash library
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
```

Apéndice AL. Archivo de configuración `/etc/smbldap-tools/smbldap_bind.conf`

```
##############################
# Credential Configuration #
##############################
# Notes: you can specify two differents configuration if you use a
# master ldap for writing access and a slave ldap server for reading access
# By default, we will use the same DN (so it will work for standard Samba
# release)
slaveDN="cn=admin,dc=gsr,dc=pt"
slavePw="********"
masterDN="cn=admin,dc=gsr,dc=pt"
masterPw="********"
```

Apéndice AM. Archivo de configuración /etc/apache/conf.d/mod_ssl-00-global.conf

```
# The whole SSL configuration in this context applies both to
# the main server and all SSL-enabled virtual hosts.

# We surround the directives with <IfModule> .. </Ifmodule>, so that Apache
# will keep a valid configuration even if mod_ssl is unavailable.
<IfModule mod_ssl.c>
 # These will make apache listen to port 443 in addition to the
 # standard port 80. HTTPS requests use port 443.
 #Listen 80
 Listen 443

 # Some MIME-types for downloading Certificates and CRLs
 AddType application/x-x509-ca-cert .crt
 AddType application/x-pkcs7-crl    .crl

 # Semaphore:
 #   Configure the path to the mutual exclusion semaphore the
 #   SSL engine uses internally for inter-process synchronization.
 SSLMutex file:/var/run/mod_ssl_mutex

 # Inter-Process Session Cache:
 #   Configure the SSL Session Cache: First either ‘none’
 #   or ‘dbm:/path/to/file’ for the mechanism to use and
 #   second the expiring timeout (in seconds).
 SSLSessionCache         dbm:/var/run/mod_ssl_scache
 SSLSessionCacheTimeout  300
 #SSLSessionCache         none

 # Pseudo Random Number Generator (PRNG):
 #   Configure one or more sources to seed the PRNG of the
 #   SSL library. The seed data should be of good random quality.
 SSLRandomSeed startup file:/dev/urandom 512
 SSLRandomSeed connect file:/dev/urandom 512

 # Logging:
 #   The home of the dedicated SSL protocol logfile. Errors are
 #   additionally duplicated in the general error log file.  Put
 #   this somewhere where it cannot be used for symlink attacks on
 #   a real server (i.e. somewhere where only root can write).
 #   Log levels are (ascending order: higher ones include lower ones):
 #   none, error, warn, info, trace, debug.
 SSLLog /var/log/apache/ssl_engine.log
 SSLLogLevel info
</IfModule>
```

Apéndice AN. Archivo de configuración `/etc/apache/conf.d/vhost.conf`

```
### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them.
# Please see the documentation at <URL:http://www.apache.org/docs/vhosts/>
# for further details before you try to setup virtual hosts.
# You may use the command line option '-S' to verify your virtual host
# configuration.

#
# If you want to use name-based virtual hosts you need to define at
# least one IP address (and port number) for them.

NameVirtualHost gsr.pt
NameVirtualHost gsr.pt:443

#
# gsr.pt
#

<VirtualHost gsr.pt>
        ServerName gsr.pt
        ServerAdmin sergio@gsr.pt
        DocumentRoot /var/www/
        # Logs Globales
        ErrorLog /var/log/apache/error.log
        CustomLog /var/log/apache/access.log combined
</VirtualHost>

#
# gsr.pt:443
#

<VirtualHost gsr.pt:443>
        ServerName gsr.pt
        ServerAdmin sergio@gsr.pt
        DocumentRoot /var/www/
        # Logs
        ErrorLog /var/log/apache/ssl-error.log
        CustomLog /var/log/apache/ssl-access.log combined

        <IfModule mod_ssl.c>
                SSLEngine on
                SSLCertificateFile    /etc/apache/ssl.crt/server.crt
                SSLCertificateKeyFile /etc/apache/ssl.key/server.key
                SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
        </IfModule>
</VirtualHost>
```

Apéndice AO. Archivo de configuración `/etc/hosts.allow`

```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5), hosts_options(5)
#                   and /usr/doc/netbase/portmapper.txt.gz
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper. See portmap(8)
# and /usr/doc/portmap/portmapper.txt.gz for further information.
#
slapd: 192.168.2.1
```

Apéndice AP. Archivo de configuración `/etc/hosts.deny`

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5), hosts_options(5)
#                  and /usr/doc/netbase/portmapper.txt.gz
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper. See portmap(8)
# and /usr/doc/portmap/portmapper.txt.gz for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address. You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

# Desautorizar a todos los hosts con nombre sospechoso
ALL: PARANOID

# Desautorizar a todos los hosts
ALL:ALL
```

VII. Licencias

Apéndice AQ. Creative Commons, legal code: Reconocimiento-CompartirIgual 2.0

0. Licencia

LA OBRA (SEGÚN SE DEFINE MÁS ADELANTE) SE PROPORCIONA BAJO TÉRMINOS DE ESTA LICENCIA PÚBLICA DE CREATIVE COMMONS ("CCPL" O "LICENCIA"). LA OBRA SE ENCUENTRA PROTEGIDA POR LA LEY ESPAÑOLA DE PROPIEDAD INTELECTUAL Y/O CUALESQUIERA OTRAS NORMAS RESULTEN DE APLICACIÓN. QUEDA PROHIBIDO CUALQUIER USO DE LA OBRA DIFERENTE A LO AUTORIZADO BAJO ESTA LICENCIA O LO DISPUESTO EN LAS LEYES DE PROPIEDAD INTELECTUAL.

MEDIANTE EL EJERCICIO DE CUALQUIER DERECHO SOBRE LA OBRA, USTED ACEPTA Y CONSIENTE LAS LIMITACIONES Y OBLIGACIONES DE ESTA LICENCIA. EL LICENCIADOR LE CEDE LOS DERECHOS CONTENIDOS EN ESTA LICENCIA, SIEMPRE QUE USTED ACEPTE LOS PRESENTES TÉRMINOS Y CONDICIONES.

1. *Definiciones*

   a. La “obra” es la creación literaria, artística o científica ofrecida bajo términos de esta licencia.

   b. El “autor” es la persona o la entidad que creó la obra.

   c. Se considerará “obra conjunta” aquella susceptible de ser incluida en alguna de las siguientes categorías:

      i. “Obra en colaboración”, entendiendo por tal aquella que sea resultado unitario de la colaboración de varios autores.

      ii. “Obra colectiva”, entendiendo por tal la creada por la iniciativa y bajo la coordinación de una persona natural o jurídica que la edite y divulgue bajo su nombre y que esté constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada.

      iii. “Obra compuesta e independiente”, entendiendo por tal, la obra nueva que incorpore una obra preexistente sin la colaboración del autor de esta última.

   d. Se considerará “obra derivada” aquella que se encuentre basada en una obra o en una obra y otras preexistentes, tales como: las traducciones y adaptaciones; las revisiones, actualizaciones y anotaciones; los compendios, resúmenes y extractos; los arreglos musicales y; en general, cualesquiera transformaciones de una obra literaria, artística o científica, salvo que la obra resultante tenga el carácter de obra conjunta en cuyo caso no será considerada como una obra derivada a los efectos de esta licencia. Para evitar la duda, si la obra consiste en una composición musical o grabación de sonidos, la sincronización temporal de la obra con una imagen en movimiento ("synching") será considerada como una obra derivada a los efectos de esta licencia.

e. Tendrán la consideración de “obras audiovisuales” las creaciones expresadas mediante una serie de imágenes asociadas, con o sin sonorización incorporada, así como las composiciones musicales, que estén destinadas esencialmente a ser mostradas a través de aparatos de proyección o por cualquier otro medio de comunicación pública de la imagen y del sonido, con independencia de la naturaleza de los soportes materiales de dichas obras.

f. El “licenciador” es la persona o la entidad que ofrece la obra bajo términos de esta licencia y le cede los derechos de explotación de la misma conforme a lo dispuesto en ella.

g. “Usted” es la persona o la entidad que ejercita los derechos cedidos mediante esta licencia y que no ha violado previamente los términos de la misma con respecto a la obra, o que ha recibido el permiso expreso del licenciador de ejercitar los derechos cedidos mediante esta licencia a pesar de una violación anterior.

h. La “transformación” de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente. Cuando se trate de una base de datos según se define más adelante, se considerará también transformación la reordenación de la misma. La creación resultante de la transformación de una obra tendrá la consideración de obra derivada.

i. Se entiende por “reproducción” la fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella.

j. Se entiende por “distribución” la puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma.

k. Se entenderá por “comunicación pública” todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas. No se considerará pública la comunicación cuando se celebre dentro de un ámbito estrictamente doméstico que no esté integrado o conectado a una red de difusión de cualquier tipo. A efectos de esta licencia se considerará comunicación pública la puesta a disposición del público de la obra por procedimientos alámbricos o inalámbricos, incluida la puesta a disposición del público de la obra de tal forma que cualquier persona pueda acceder a ella desde el lugar y en el momento que elija.

l. La “explotación” de la obra comprende su reproducción, distribución, comunicación pública y transformación.

m. Tendrán la consideración de “bases de datos” las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos propiamente dichas que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos.

n. Los “elementos de la licencia” son las características principales de la licencia según la selección efectuada por el licenciador e indicadas en el título de esta licencia: Reconocimiento de autoría (Reconocimiento), Compartir de manera igual (CompartirIgual).

2. *Límites y uso legítimo de los derechos.* Nada en esta licencia pretende reducir o restringir cualesquiera límites legales de los derechos exclusivos del titular de los derechos de propiedad intelectual de acuerdo con la Ley de Propiedad Intelectual o cualesquiera otras leyes aplicables, ya sean derivados de usos legítimos, tales como el derecho de copia privada o el derecho a cita, u otras limitaciones como la derivada de la primera venta de ejemplares.

3. *Concesión de licencia*. Conforme a los términos y a las condiciones de esta licencia, el licenciador concede (durante toda la vigencia de los derechos de propiedad intelectual) una licencia de ámbito mundial, sin derecho de remuneración, no exclusiva e indefinida que incluye la cesión de los siguientes derechos:

   a. Derecho de reproducción, distribución y comunicación pública sobre la obra;

   b. Derecho a incorporarla en una o más obras conjuntas o bases de datos y para su reproducción en tanto que incorporada a dichas obras conjuntas o bases de datos;

   c. Derecho para efectuar cualquier transformación la obra y crear y reproducir obras derivadas;

   d. Derecho de distribución y comunicación pública de copias o grabaciones de la obra, como incorporada a obras conjuntas o bases de datos;

   e. Derecho de distribución y comunicación pública de copias o grabaciones de la obra, por medio de una obra derivada.

   f. Para evitar la duda, sin perjuicio de la preceptiva autorización del licenciador, y especialmente cuando la obra se trate de una obra audiovisual, el licenciador se reserva el derecho exclusivo a percibir, tanto individualmente como mediante una entidad de gestión de derechos, o varias, (por ejemplo: SGAE, Dama, VEGAP), los derechos de explotación de la obra, así como los derivados de obras derivadas, conjuntas o bases de datos, si dicha explotación pretende principalmente o se encuentra dirigida hacia la obtención de un beneficio mercantil o la remuneración monetaria privada.

   Los anteriores derechos se pueden ejercitar en todos los medios y formatos, tangibles o intangibles, conocidos o por conocer. Los derechos mencionados incluyen el derecho a efectuar las modificaciones que sean precisas técnicamente para el ejercicio de los derechos en otros medios y formatos. Todos los derechos no cedidos expresamente por el licenciador quedan reservados.

4. *Restricciones.* La cesión de derechos que supone esta licencia se encuentra sujeta y limitada a las restricciones siguientes:

   a. Usted puede reproducir, distribuir o comunicar públicamente la obra solamente bajo términos de esta licencia y debe incluir una copia de la misma, o su Identificador Uniforme de Recurso (URI), con cada copia o grabación de la obra que usted reproduzca, distribuya o comunique públicamente. Usted no puede ofrecer o imponer ningún término sobre la obra que altere o restrinja los términos de esta licencia o el ejercicio de sus derechos por parte de los cesionarios de la misma. Usted no puede sublicenciar la obra. Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías. Usted no puede reproducir, distribuir o comunicar públicamente la obra con medidas tecnológicas que controlen el acceso o uso de la obra de una manera contraria a los términos de esta licencia. Lo anterior se aplica a una obra en tanto que incorporada a una obra conjunta o base de datos, pero no implica que éstas, al margen de la obra objeto de esta licencia, tengan que estar sujetas a los términos de la misma. Si usted crea una obra conjunta o base de datos, previa comunicación del licenciador, usted deberá quitar de la obra conjunta o base de datos cualquier referencia a dicho licenciador o al autor original, según lo que se le requiera y en la medida de lo posible. Si usted crea una obra derivada, previa comunicación del licenciador, usted deberá quitar de la obra derivada cualquier referencia a dicho licenciador o al autor original, lo que se le requiera y en la medida de lo posible.

   b. Usted puede reproducir, distribuir o comunicar públicamente una obra derivada solamente bajo los términos de esta licencia, o de una versión posterior de esta licencia con sus mismos elementos principales, o de una licencia iCommons de Creative Commons que contenga los

mismos elementos principales que esta licencia (ejemplo: Reconocimiento-Compartir 2.0 Japón). Usted debe incluir una copia de la esta licencia o de la mencionada anteriormente, o bien su Identificador Uniforme de Recurso (URI), con cada copia o grabación de la obra que usted reproduzca, distribuya o comunique públicamente. Usted no puede ofrecer o imponer ningún término respecto de las obras derivadas o sus transformaciones que alteren o restrinjan los términos de esta licencia o el ejercicio de sus derechos por parte de los cesionarios de la misma, Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías. Usted no puede reproducir, distribuir o comunicar públicamente la obra derivada con medidas tecnológicas que controlen el acceso o uso de la obra de una manera contraria a los términos de esta licencia. Lo anterior se aplica a una obra derivada en tanto que incorporada a una obra conjunta o base de datos, pero no implica que éstas, al margen de la obra objeto de esta licencia, tengan que estar sujetas a los términos de esta licencia.

c. Si usted reproduce, distribuye o comunica públicamente la obra o cualquier obra derivada, conjunta o base datos que la incorpore, usted debe mantener intactos todos los avisos sobre la propiedad intelectual de la obra y reconocer al autor original, de manera razonable conforme al medio o a los medios que usted esté utilizando, indicando el nombre (o el seudónimo, en su caso) del autor original si es facilitado; el título de la obra si es facilitado; de manera razonable, el Identificador Uniforme de Recurso (URI), si existe, que el licenciador especifica para ser vinculado a la obra, a menos que tal URI no se refiera al aviso sobre propiedad intelectual o a la información sobre la licencia de la obra; y en el caso de una obra derivada, un aviso que identifique el uso de la obra en la obra derivada (e.g., "traducción francesa de la obra de Autor Original," o "guión basado en obra original de Autor Original"). Tal aviso se puede desarrollar de cualquier manera razonable; con tal de que, sin embargo, en el caso de una obra derivada, conjunta o base datos, aparezca como mínimo este aviso allá donde aparezcan los avisos correspondientes a otros autores y de forma comparable a los mismos.

d. En el caso de la inclusión de la obra en alguna base de datos o recopilación, el propietario o el gestor de la base de datos tiene que renunciar a cualquier derecho relacionado con esta inclusión y concerniente a los usos de la obra una vez extraída de les bases de datos, ya sea de manera individual o conjuntamente con otros materiales.

5. *Ausencia de responsabilidad*

A MENOS QUE SE ACUERDE MUTUAMENTE ENTRE LAS PARTES, EL LICENCIADOR OFRECE LA OBRA TAL CUAL (ON AN "AS-IS" BASIS) Y NO CONFIERE NINGUNA GARANTÍA DE CUALQUIER TIPO RESPECTO DE LA OBRA O DE LA PRESENCIA O AUSENCIA DE ERRORES QUE PUEDAN NO SER DESCUBIERTOS. ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE TALES GARANTÍAS, POR LO QUE TAL EXCLUSIÓN PUEDE NO SER DE APLICACIÓN A USTED.

6. *Limitación de responsabilidad.*

SALVO QUE LO DISPONGA EXPRESA E IMPERATIVAMENTE LA LEY APLICABLE, EN NINGÚN CASO EL LICENCIADOR SERÁ RESPONSABLE ANTE USTED POR CUALQUIER TEORÍA LEGAL DE CUALESQUIERA DAÑOS RESULTANTES, GENERALES O ESPECIALES (INCLUIDO EL DAÑO EMERGENTE Y EL LUCRO CESANTE), FORTUITOS O CAUSALES, DIRECTOS O INDIRECTOS, PRODUCIDOS EN CONEXIÓN CON ESTA LICENCIA O EL USO DE LA OBRA, INCLUSO SI EL LICENCIADOR HUBIERA SIDO INFORMADO DE LA POSIBILIDAD DE TALES DAÑOS.

7. *Finalización de la licencia*

a. Esta licencia y la cesión de los derechos que contiene terminarán automáticamente en caso de cualquier incumplimiento de los términos de la misma. Las personas o entidades que hayan recibido obras derivadas, conjuntas o bases de datos de usted bajo esta licencia, sin embargo, no verán sus licencias finalizadas, siempre que tales personas o entidades se mantengan en el cumplimiento íntegro de esta licencia. Las secciones 1, 2, 5, 6, 7 y 8 permanecerán vigentes pese a cualquier finalización de esta licencia.

b. Conforme a las condiciones y términos anteriores, la cesión de derechos de esta licencia es perpetua (durante toda la vigencia de los derechos de propiedad intelectual aplicables a la obra). A pesar de lo anterior, el licenciador se reserva el derecho a divulgar o publicar la obra en condiciones distintas a las presentes, o de retirar la obra en cualquier momento. No obstante, ello no supondrá dar por concluida esta licencia (o cualquier otra licencia que haya sido concedida, o sea necesario ser concedida, bajo los términos de esta licencia), que continuará vigente y con efectos completos a no ser que haya finalizado conforme a lo establecido anteriormente.

8. *Cuestiones diversas*

a. Cada vez que usted explote de alguna forma la obra, o una obra conjunta o una base datos que la incorpore, deberá ceder los derechos de explotación mediante una licencia sobre la obra original en las mismas condiciones y términos que la licencia concedida a usted.

b. Cada vez que usted explote de alguna forma una obra derivada, deberá ceder los derechos de explotación mediante una licencia sobre la obra por usted creada en las mismas condiciones y términos que la licencia concedida a usted.

c. Si alguna disposición de esta licencia resulta inválida o inaplicable según la Ley vigente, ello no afectará la validez o aplicabilidad del resto de los términos de esta licencia y, sin ninguna acción adicional por cualquiera las partes de este acuerdo, tal disposición se entenderá reformada en lo estrictamente necesario para hacer que tal disposición sea válida y ejecutiva.

d. No se entenderá que existe renuncia respecto de algún término o disposición de esta licencia, ni que se consiente violación alguna de la misma, a menos que tal renuncia o consentimiento figure por escrito y lleve la firma por la parte que renuncie o consienta.

e. Esta licencia constituye el acuerdo pleno entre las partes con respecto a la obra objeto de la licencia. No caben interpretaciones, acuerdos o términos con respecto a la obra que no se encuentren expresamente especificados en la presente licencia. El licenciador no estará obligado por ninguna disposición complementaria que pueda aparecer en cualquier comunicación de usted. Esta licencia no se puede modificar sin el mutuo acuerdo por escrito entre el licenciador y usted.

Creative Commons no es parte de esta licencia, y no ofrece ninguna garantía en relación con la obra. Creative Commons no será responsable frente a usted o a cualquier parte, por cualquier teoría legal de cualesquiera daños resultantes, incluyendo, pero no limitado, daños generales o especiales (incluido el daño emergente y el lucro cesante), fortuitos o causales, en conexión con esta licencia. A pesar de las dos (2) oraciones anteriores, si Creative Commons se ha identificado expresamente como el licenciador, tendrá todos los derechos y obligaciones del licenciador.

Salvo para el propósito limitado de indicar al público que la obra está licenciada bajo la CCPL, ninguna parte utilizará la marca registrada "Creative Commons" o cualquier marca registrada o insignia relacionada con "Creative Commons" sin su consentimiento por escrito. Cualquier uso permitido se hará de conformidad con las pautas vigentes en cada momento sobre el uso de la marca registrada por "Creative Commons", en tanto que sean publicadas su página web (website) o sean proporcionadas a petición previa.

Puede contactar con Creative Commons en: http://creativecommons.org/.

Apéndice AR. GNU General Public License

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software - to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps:

1. copyright the software, and
2. offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING,

DISTRIBUTION AND MODIFICATION

Section 0

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

Section 1

You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Section 2

You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.

Exception:: If the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

Section 3

You may copy and distribute the Program (or a work based on it, under Section 2 in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

Section 4

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

Section 5

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

Section 6

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

Section 7

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have

made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

Section 8

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

Section 9

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

Section 10

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE

PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Section 12

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Apéndice AS. GNU LESSER GENERAL PUBLIC LICENSE

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author’s reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

Section 0

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications

and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

Section 1

You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Section 2

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of la sección de nombre *Section 1* above, provided that you also meet all of these conditions:

1. The modified work must itself be a software library.
2. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
3. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
4. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   > **Example:** (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

Section 3

You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

Section 4

You may copy and distribute the Library (or a portion or derivative of it, under la sección de nombre *Section 2*) in object code or executable form under the terms of la sección de nombre *Section 1* and la sección de nombre *Section 2* above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of la sección de nombre *Section 1* and la sección de nombre *Section 2* above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

Section 5

A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in

isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. la sección de nombre *Section 6* states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under la sección de nombre *Section 6*.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of la sección de nombre *Section 6*. Any executables containing that work also fall under la sección de nombre *Section 6*, whether or not they are linked directly with the Library itself.

Section 6

As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer’s own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

1. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under la sección de nombre *Section 1* and la sección de nombre *Section 2* above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
2. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user’s computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
3. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this

distribution.

4. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
5. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

Section 7

You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

1. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
2. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

Section 8

You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

Section 9

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

Section 10

Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

Section 11

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

Section 12

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

Section 13

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and

conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

Section 14

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Section 16

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Apéndice AT. The OpenLDAP Public License

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders

VIII. Derechos de copia

Apéndice AU. Derechos de copia de OpenLDAP

Derechos de copia de: Kurt D. Zeilenga, Net Boolean Incorporated e IBM Corporation

Derechos de copia de: Howard Y.H. Chu, Symas Corporation y Hallvard B. Furuseth

Derechos de copia de: Regents of the University of Michigan

Apéndice AV. Common UNIX Printing System License Agreement

Easy Software Products
44141 AIRPORT VIEW DR STE 204,
Hollywood,
Maryland 20636-3111
USA

Voice: +1.301.373.9600

Email:<cups-info@cups.org>

WWW: http://www.cups.org

INTRODUCTION

The Common UNIX Printing System™, ("CUPS™"), is provided under the GNU General Public License ("GPL ") and GNU Library General Public License ("LGPL "), Version 2, with exceptions for Apple operating systems and the OpenSSL toolkit. A copy of the exceptions and licenses follow this introduction.

The GNU LGPL applies to the CUPS API library, located in the "cups" subdirectory of the CUPS source distribution and in the "cups" include directory and library files in the binary distributions. The GNU GPL applies to the remainder of the CUPS distribution, including the "pdftops" filter which is based upon Xpdf and the CUPS imaging library.

For those not familiar with the GNU GPL, the license basically allows you to:

- Use the CUPS software at no charge.
- Distribute verbatim copies of the software in source or binary form.
- Sell verbatim copies of the software for a media fee, or sell support for the software.
- Distribute or sell printer drivers and filters that use CUPS so long as source code is made available under the GPL.

What this license *does not* allow you to do is make changes or add features to CUPS and then sell a binary distribution without source code. You must provide source for any new drivers, changes, or additions to the software, and all code must be provided under the GPL or LGPL as appropriate. The only exceptions to this are the portions of the CUPS software covered by the Apple operating system license exceptions outlined later in this license agreement.

The GNU LGPL relaxes the "link-to" restriction, allowing you to develop applications that use the CUPS API library under other licenses and/or conditions as appropriate for your application.

LICENSE EXCEPTIONS

In addition, as the copyright holder of CUPS, Easy Software Products grants the following special exceptions:

1. Apple Operating System Development License Exception;

    a. Software that is developed by any person or entity for an Apple Operating System ("Apple OS-Developed Software"), including but not limited to Apple and third party printer drivers, filters, and backends for an Apple Operating System, that is linked to the CUPS imaging library or based on any sample filters or backends provided with CUPS shall not be considered to be a derivative work or collective work based on the CUPS program and is exempt from the mandatory source code release clauses of the GNU GPL. You may therefore distribute linked combinations of the CUPS imaging library with Apple OS-Developed Software without releasing the source code of the Apple OS-Developed Software. You may also use sample filters and backends provided with CUPS to develop Apple OS-Developed Software without releasing the source code of the Apple OS-Developed Software.

    b. An Apple Operating System means any operating system software developed and/or marketed by Apple Computer, Inc., including but not limited to all existing releases and versions of Apple's Darwin, Mac OS X, and Mac OS X Server products and all follow-on releases and future versions thereof.

    c. This exception is only available for Apple OS-Developed Software and does not apply to software that is distributed for use on other operating systems.

    d. All CUPS software that falls under this license exception have the following text at the top of each source file:

        This file is subject to the Apple OS-Developed Software exception.

2. OpenSSL Toolkit License Exception;

    a. Easy Software Products explicitly allows the compilation and distribution of the CUPS software with the OpenSSL Toolkit.

No developer is required to provide these exceptions in a derived work.

TRADEMARKS

Easy Software Products has trademarked the Common UNIX Printing System, CUPS, and CUPS logo. These names and logos may be used freely in any direct port or binary distribution of CUPS. Please contract Easy Software Products for written permission to use them in derivative products. Our intention is to protect the value of these trademarks and ensure that any derivative product meets the same high-quality standards as the original.

BINARY DISTRIBUTION RIGHTS

Easy Software Products also sells rights to the CUPS source code under a binary distribution license for vendors that are unable to release source code for their drivers, additions, and modifications to CUPS under the GNU GPL and LGPL. For information please contact us at the address shown above.

The Common UNIX Printing System provides a "pdftops" filter that is based on the Xpdf software. For binary distribution licensing of this software, please contact:

Derek B. Noonburg

Email: <derekn@foolabs.com>

WWW: http://www.foolabs.com/xpdf/

SUPPORT

Easy Software Products sells software support for CUPS as well as a commercial printing product based on CUPS called ESP Print Pro. You can find out more at our web site:

http://www.easysw.com/

Apéndice AW. Derechos de copia de Pykota (Print Quota for CUPS and LPRng)

Bibliografía

Documentación sobre LDAP

[Danen01] *Using OpenLDAP For Authentication (http://www.mandrakesecure.net/en/docs/ldap-auth.php)*, Vincent Danen, 18/06/2002.

[Danen02] *Using OpenLDAP For Authentication; Revision 2 (http://www.mandrakesecure.net/en/docs/ldap-auth2.php)*, Vincent Danen, 06/05/2003.

[Findlay01] *Security with LDAP (http://www.skills-1st.co.uk/papers/security-with-ldap-jan-2002/security-with-ldap.html)*, Andrew Findlay.

[Fredriksson01] *LDAPv3 (http://www.bayour.com/LDAPv3-HOWTO.html)*, Turbo Fredriksson, 04/11/2003, 2001.

[HowesSmithGoodSloanRothwell01] *The SLAPD and SLURPD Administrators Guide (http://www.umich.edu/~dirsvcs/ldap/doc/guides/slapd/)*, Tim Howes, Mark Smith, Gordon Good, Lance Sloan, Steve Rothwell, 30/04/1996, 1992-1996.

[Marshall01] *System Authentication using LDAP (http://quark.humbug.org.au//publications/system_auth/sage-au/system_auth.html)*, Brad Marshall.

[metaconsultancy01] *LDAP Authentication for Linux (http://www.metaconsultancy.com/whitepapers/ldap-linux.htm)*, metaconsultancy, 2002.

[OpenLDAPProject01] *OpenLDAP 2.2 Administrator's Guide (http://www.openldap.org/doc/admin22/)*, The OpenLDAP Project, 31/12/2003, 2004.

[OpenLDAPProject02] *OpenLDAP Faq-O-Matic (http://www.openldap.org/faq/index.cgi?file=1)*, 2004.

[Roncero01] *Instalación y configuración de OpenLDAP (http://bulmalug.net/body.phtml?nIdNoticia=1343)*, Jesús Roncero, 30/05/2002 a las 18:48.

[Roncero02] *Autentificación de un cliente linux a través de LDAP (http://bulmalug.net/body.phtml?nIdNoticia=1371)*, Jesús Roncero, 13/06/2002 a las 02:17.

[Soper01] *OpenLDAP SSL/TLS How-To (http://www.openldap.org/pub/ksoper/OpenLDAP_TLS_howto.html)*, D. Kent Soper, 05/06/2003.

[vanMeerLoBiondo01] *LDAP Implementation HOWTO (http://www.tldp.org/HOWTO/LDAP-Implementation-HOWTO/)*, Roel van Meer, Giuseppe Lo Biondo, 30/03/2001, 2001.

Presentaciones sobre LDAP

[Clark01] *Practical LDAP on Linux (http://www.lugs.org.sg/lugsfiles/presentations/2002-08-Practical-LDAP-and-Linux.pdf)*, Michael Clark.

[HyukZeilenga01] *LDAP Content Synchronization*, Jong Hyuk Choi y Kurt D. Zeilenga, 18/04/2003, 2003.

[Williams01] *LDAP and OpenLDAP (on the Linux Platform) (ftp://ftp.kalamazoolinux.org/pub/pdf/ldapv3.pdf)*, Adam Tauno Williams, 21/03/2003, 2001.

Documentación sobre Samba

[Barrios01] *Cómo configurar SAMBA (http://www.linuxparatodos.com/linux/13-como-samba.php)*, Joel Barrios Dueñas, 1999, 2000, 2001, 2002, 2003.

[Berger01] *SAMBA Setup I (Client) (http://www.mandrakeuser.org/docs/connect/csamba.html)*, Tom Berger, 05/06/2002, 1999-2002.

[Berger02] *SAMBA Setup II (Server) (http://www.mandrakeuser.org/docs/connect/csamba2.html)*, Tom Berger, 28/06/2002, 1999-2002.

[Berger03] *SAMBA Setup III (http://www.mandrakeuser.org/docs/connect/csamba3.html)*, Tom Berger, 05/06/2002, 1999-2002.

[Milne01] *SAMBA V: Domain Membership (http://www.mandrakeuser.org/docs/connect/csamba5.html)*, Buchan Milne, 15/10/2001, 1999-2002.

[Milne02] *SAMBA VI: As a Domain Controller (http://www.mandrakeuser.org/docs/connect/csamba6.html)*, Buchan Milne, 18/12/2001, 1999-2002.

[CarstensenGomilsekGrimmerHaskinsKaplenk01] *Implementing Linux in your Network using Samba (http://www.redbooks.ibm.com/redpapers/pdfs/redp0023.pdf)*, Jakob Carstensen, Ivo Gomilsek, Lenz Grimmer, Jay Haskins, y Joe Kaplenk, Noviembre de 1999, 1999.

[Coldiron01] *Replacing Windows NT Server with Linux (http://citnews.unl.edu/linux/LinuxPresentation.html)*, Quinn P. Coldiron, 1997.

[Cortes01] *Recopilación de información sobre Samba. (http://bulma.net/body.phtml?nIdNoticia=967)*, Carlos Cortes Cortes, 05/11/2001 a las 00:31.

[EcksteinCollier-BrownKelly01] *Usando Samba, primera edición*, Robert Eckstein, David Collier-Brown, y Peter Kelly, 1-56592-449-5, Noviembre de 1999.

[Gabriel01] *HowTo, los primeros pasos para Instalar Samba (http://bulma.net/body.phtml?nIdNoticia=1123)*, Gabriel, 08/01/2002 a las 00:12.

[Hertel01] *Understanding the Network Neighborhood - How Linux Works With Microsoft Networking Protocols (http://www.linux-mag.com/2001-05/smb_01.html)*, Christopher R. Hertel, Mayo de 2001, 2001.

[Hertel02] *Samba: An Introduction (http://www.samba.org/samba/docs/SambaIntro.html)*, Christopher R. Hertel, 27/11/2001 a las 21:50:29 GMT.

[SambaTeam01] *Samba FAQ (http://www.samba.org/faq/samba-faq.html)*, Samba Team, Octubre de 2002.

[Sharpe01] *Just what is SMB? (http://samba.anu.edu.au/cifs/docs/what-is-smb.html)*, Richard Sharpe, 08/10/2002, 1996, 1997, 1998, 1999, 2001, 2002.

[Syroid02] *Using Samba as a PDC (http://www-106.ibm.com/developerworks/eserver/tutorials/samba.html)*, Tom Syroid.

[TsEcksteinCollier-Brown01] *Using Samba, 2nd Edition (http://www.oreilly.com/catalog/samba2/)*, Jay Ts, Robert Eckstein, y David Collier-Brown, 0-596-00256-4, Febrero 2003, 2003.

[VernooijTerpstraCarter01] *Samba HOWTO Collection (http://www.samba.org/samba/devel/docs/html/Samba-HOWTO-Collection.html)*, Jelmer R. Vernooij, John H. Terpstra, Gerald (Jerry) Carter.

[Wood01] *SMB HOWTO (http://www.tldp.org/HOWTO/SMB-HOWTO.html)*, David Wood, 20/04/2000, 2000.

Documentación sobre CUPS

[CUPS01] *F.A.Q. (http://www.cups.org/faq.php)*, 1993-2003.

[CUPS02] *CUPS Software Administrators Manual (http://www.cups.org/sam.html)*, 1997-2003.

[Kamppeter01] *Printing With CUPS - Setup And Configuration II (http://www.mandrakeuser.org/docs/hardware/hcups3.html)*, Till Kamppeter, 15/11/2000, 1999-2002.

[Pfeifle01] *Troubleshooting-CUPS-and-Asking-for-Help HOWTO (http://www.cups.org/cups-help.html)*, Kurt Pfeifle, Febrero de 2002.

[Sweet01] *An Overview of the Common UNIX Printing System, Version 1.1 (http://www.cups.org/overview.html)*, Michael Sweet, 10/07/2000, 1998-2003.

Documentación sobre PyKota

[Romero01] *Configuración de un PrintServer CUPS para restricción de número de impresiones por usuario*, Dennis Romero L..

[Alet01] *PyKota Documentation - A full featured Print Quota Solution for CUPS and LPRng*, Jérôme Alet, 12/01/2004 a las 23:16:42, 2003,2004.

Otros documentos consultados

[BraatenJuellNordnes01] *ICT administration manual for Skolelinux (http://developer.skolelinux.no/dokumentasjon/IKT-bok.en.html)*, Vibeke Braaten, Christian Juell, Tor Harald Nordnes, Truls Teigen, , 2002, 2003.

[Carter01] *Storing Samba's User/Machine Account information in an LDAP Directory (http://www.samba.org/samba/ftp/docs/htmldocs/Samba-LDAP-HOWTO.html)*, Gerald (Jerry) Carter.

[Collings01] *Implementing a Samba LDAP Primary Domain Controller Setup on Mandrake 9.x (http://www.mandrakesecure.net/en/docs/samba-pdc.php)*, Jim Collings, 22/05/2003.

[Comer01] *Glosario de términos de "Internetworking with TCP/IP principles, protocols, and architectures" (volume 1)*, Douglas E. Comer, 676,684,691,694,695,696,700,701,702,708,713,716,717,718.

[Coupeau01] *Samba PDC LDAP howto (http://www.unav.es/cti/ldap-smb-howto.html)*, Ignacio Coupeau, 05/01/2004.

[FrohaugSporildDahl01] *SkoleLinux - User Administration (http://developer.skolelinux.no/info/studentgrupper/2003-HiG-useradmin/SkolelinuxUserAdminFinal.pdf)*, Trond Christian Frøhaug, Morten Sporild, Ole Martin Dahl, 19/05/2003.

[KDE01] *Glosario de términos de KDE (http://www.kde.org/)*.

[Lemaire01] *The SAMBA-2.2.4/LDAP PDC HOWTO (http://www.idealx.org/prj/samba/samba-ldap-howto.pdf)*, Olivier Lemaire, 07/06/2002.

[Milne03] *Implementing Disconnected Authentication and PDC/BDC Relationships Using Samba and OpenLDAP (http://www.mandrakesecure.net/en/docs/samba-ldap-advanced.php)*, Buchan Milne, 05/06/2003.

[Morgan01] *The Linux-PAM System Administrators' Guide (http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html)*, Andrew G. Morgan, 26/02/2002, 1996-2002.

[RedHatLinuxRefGuide] *Red Hat Linux 9 - Red Hat Linux Reference Guide (http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/)*, Red Hat, Inc., 2003.

[Sigle01] *Glosario de términos del documento Building a Secure RedHat Apache Server HOWTO*, Richard Sigle, 06/02/2001.

[Syroid01] *Using an LDAP Directory for Samba Authentication (http://www-106.ibm.com/developerworks/eserver/tutorials/smb_ldap.html)*, Tom Syroid.

[Tanenbaum01] *Redes de computadoras, tercera edición*, Andrew S. Tanenbaum, 46.

[Tournier01] *Smbldap-tools User Manual (Release : 0.8.4)*, Jérôme Tournier, 9/02/2004.

Páginas del manual

[Man] *A lo largo del desarrollo del trabajo se consultaron numerosas páginas del manual, sobre todo aquellas relativas a los programas utilizados. Debido a que la lista de páginas consultadas ha sido muy grande, se deja como referencia únicamente el hecho de que se han consultado .*

Servidor de diccionarios y sus diccionarios asociados

[Dictd] *Durante la realización del presente trabajo, se hizo uso del servidor de diccionarios, así como sus diccionarios asociados para consultar términos y aclarar ideas .*

Software relacionado y utilizado

[OpenLDAP] *OpenLDAP (http://www.openldap.org/), implementación open source del protocolo LDAP .*

[Samba] *Samba (http://www.samba.org/), servidor SMB/CIFS para Unix .*

[CUPS] *CUPS (http://www.cups.org/), sistema de impresión portable y extensible para Unix .*

[PyKota] *PyKota (http://www.librelogiciel.com/software/PyKota/action_Presentation.html) software de control de cuotas de impresión centralizado para CUPS y LPRng .*

[Dia] *Dia (http://www.lysator.liu.se/~alla/dia/), programa editor de diagramas .*

[TheGimp] *The Gimp! (http://www.gimp.org/), programa de tratamiento digital de la imagen .*

[Wine] *Wine (http://www.winehq.org/), programa que permite la interoperabilidad de programas DOS y MS Windows (ejecutables Windows 3.x y Win32) en sistemas Unix, como Linux. .*

Sistemas Operativos empleados

[DebianGNULinux] *Debian GNU/Linux (http://www.debian.org/)* .

Núcleos implicados

[Linux] *Linux (http://www.kernel.org/)* .

Otros

[MS Windows] *MS Windows (http://www.microsoft.com/windows/)* .

Glosario de términos

A

ACE

(*Access Control Entries*). Una entrada de control de acceso posee un SID y los derechos de acceso asociados a este. Las ACLs están formadas por una o más ACEs.

Ver también: ACL, SID.

ACL

(*Access Control Lists*).Las ACLs son utilizadas para comprobar que tipo de acceso tiene un usuario dado (autentificado).

API

(*Application Program Interface*). Una API comprende las especificaciones de las operaciones que un programa ha de invocar para comunicarse a través de la red.

ASCII

(*American Standard Code of Information Interchange*). Código Estándar Americano para Intercambio de Información. Código consistente en un conjunto de combinaciones de 128 elementos de 7 bits usado internamente por los ordenadores digitales, con el fin de mostrar información e intercambiar datos entre ordenadores. Su uso está muy extendido, pero debido a la limitación del número de caracteres codificados, otros códigos lo complementan o lo reemplazan para codificar símbolos especiales o palabras en otros idiomas distintos al inglés.

B

BDC

(*Backup Domain Controller*). Un BDC es un servidor Windows que actúa como respaldo de un PDC dentro de un dominio Windows. Este posee una copia de la base de datos SAM que sincroniza frecuentemente desde un PDC. Cuando un PDC deja de estar disponible, el BDC se encarga de continuar con las tareas que este desempeñaba hasta que vuelva a estar disponible.

Ver también: SAM, PDC.

BIOS

(*Basic Input/Output System*). BIOS, el sistema básico de entrada/salida, no es más que un programa empotrado generalmente en la memoria ROM, que se ejecuta en el momento del arranque inicial del ordenador.

BMP

(*BipMaP*). Formato de mapa de bits de Microsoft Windows. Es el único formato de gráficos donde la compresión aumenta el tamaño del archivo. No obstante, el formato es muy usado.

C

CA

(*Certificate Authority*). Entidad certificadora.

CAL

(*Client Access License*). Sistema de licencias que empresas como Microsoft imponen a sus productos, de forma que ha de pagar una cantidad de dinero por cada equipo en el que quiera ejecutar e instalar el software de estas compañías.

CEO

(*Chief Executive Officer*). Un CEO es el responsable ejecutivo para las operaciones de firma, genera informes para el grupo de directores y muchos designan otros administradores (incluyendo al presidente).

CIFS

(*Common Internet File System*). Alrededor de 1996, Microsoft (http://www.microsoft.com/) aparentemente decidió que SMB necesitaba incluir la palabra Internet, por este motivo cambió el nombre hacia CIFS.

Ver también: Samba, SMB.

Copyleft

(Un juego sobre el término “copyright”). El concepto de copyright y la Licencia Pública General, GPL, aplicados al trabajo de la FSF, garantizando la reutilización y la reproducción de estos derechos para cualquier persona.

Normalmente el derecho de copia (copyright) restringe la libertad; el copyleft ("izquierdo de copia") la preserva. Es un instrumento legal que exige a aquellas personas que distribuyen un programa a incluir los derechos de uso, modificación y redistribución del código; el código y la libertad son de esta manera legalmente dependientes.

El copyleft utilizado por el proyecto GNU combina un aviso sobre el derecho de copia (copyright) y la "GNU General Public License" (GPL). La GPL es una licencia de derechos de copia que dice, básicamente, lo que se ha mencionado anteriormente sobre la libertad. Esta licencia está incluida en cada distribución del código fuente del proyecto GNU así como en sus manuales.

Ver también: GNU, GPL, FSF.

CSR

(*Certificate Signing Request*). Petición para la firma de un certificado.

CUPS

(*Common UNIX Printing System*). CUPS es el más moderno sistema de impresión para UNIX y GNU/Linux, provee también servicios de impresión a clientes Apple (http://www.apple.com/) MacOS y Microsoft (http://www.microsoft.com/) Windows. Basado en el protocolo IPP, deja atrás las dificultades del viejo sistema de impresión BSD, proveiendo autentificación, cifrado y ACLs, a parte de otras muchas características.

Al mismo tiempo, es lo suficientemente compatible hacia atrás como para servir a todos aquellos clientes que no soportan todavía IPP, gracias a LPR/LPD (estilo BSD). CUPS puede controlar cualquier impresora PostScript haciendo uso de los archivos PPD suministrados por los vendedores.

Ver también: ACL, IPP, PS, PPD.

CVS

(*Concurrent Versions System*).

D

DAP

(*Directory Access Protocol*). DAP es un protocolo de acceso a directorio de la pila OSI.

Ver también: LDAP, OSI, X.500, Directory Access Protocol.

DEN

Directory Enabled Networking, relativo a Microsoft.

DESQview

Un sistema de *Quarterdeck Office Systems* que implementa la multitarea bajo MS-DOS.

Ver también: MS-DOS.

Dfs

(*Distributed File System*). Sistema de archivos distribuido.

DHCP

(*Dynamic Host Configuration Protocol*). Protocolo que utiliza un determinado equipo para obtener toda la información de configuración necesaria, incluyendo la dirección IP.

DIT

(*Directory Information Tree*). DIT es el acrónimo de *Directory Information Tree*, relativo a un directorio LDAP

Ver también: LDAP.

DN

(*Distinguished Name*). DN es utilizado para referirse a una entrada de un directorio LDAP sin ambigüedades. Esta está formada por el nombre de la propia entrada, o RDN, y la concatenación de los nombres de las entradas que le anteceden.

Ver también: RDN.

DNS

(*Domain Name System*). DNS es un estándar para traducir nombres de dominios en direcciones IP, o viceversa, solicitando la información a una base de datos centralizada.

DOS

(*Disk Operating System*).

Ver también: MS-DOS.

DSC

(*Document Structuring Conventions*).

E

EMACS

(*Editing MACroS o Extensible MACro System*). Un editor muy popular para Unix y otros muchos sistemas operativos.

Ver también: GNU.

EMS

(*Expanded Memory Specification*). Añadido para MS-DOS que permite a los programas utilizar más de 1 megabyte de memoria.

Ver también: MS-DOS.

F

FQDN

(*Fully Qualified DOMAIN Name*).

FSF

(*Free Software Foundation*). Abreviatura común (tanto hablada como escrita) para el nombre de la *Free Software Foundation*, una asociación educacional sin ánimo de lucro formada para dar soporte al proyecto GNU.

Ver también: GNU.

G

GID

(*Group IDentification*). Número único que identifica a un grupo dentro de un sistema Unix o en un dominio NIS.

Ver también: RID, UID.

GNU

(*GNU's Not Unix!*). Este acrónimo recursivo hace referencia al esfuerzo colectivo de desarrollo Unix llevado a cabo por la *Free Software Foundation*, encabezada por Richard Stallman. GNU EMACS y el compilador GNU C, dos de las herramientas diseñadas por este proyecto, se han vuelto muy populares en el dominio hacker y en cualquier otro lugar. El proyecto GNU fue diseñado en parte por la posición proselitista de RMS, que defendía que la información es propiedad de la comunidad y que todo el código fuente de las aplicaciones software debe ser

compartido. Uno de sus lemas es “¡Ayuda a terminar con la acumulación de software!”. Aunque esto pueda parecer controvertido (porque implícitamente niega cualquier derecho a los diseñadores de poseer, asignar y vender el resultado de su trabajo), a pesar de todo, muchos hackers que no estaban de acuerdo con RMS, cooperaron para producir grandes cantidades de software de gran calidad para redistribuirlo bajo el imprimátur de la Free Software Foundation. El proyecto GNU tiene una página web en http://www.gnu.org/.

Ver también: FSF, RMS.

GNU/Linux

Algunas personas sugieren que el nombre “Linux” se utilice para referirse únicamente al núcleo, no al sistema operativo completo. Este reclamo deja paso a una disputa territorial subyacente; la gente que insiste en utilizar el término GNU/Linux quiere que la FSF obtenga los mayores créditos sobre Linux, ya que RMS y compañía han escrito muchas de sus herramientas de nivel de usuario. Ni esta teoría ni el término GNU/Linux no han ganado más que una aceptación minoritaria.

Por otro lado, hay personas que están en desacuerdo con el término GNU/Linux debido a que no todo el software que se distribuye junto a una distribución Linux es perteneciente al proyecto GNU.

Una interpretación más general del término GNU/Linux lo define como un conjunto de aplicaciones de libre distribución más el núcleo Linux, independientemente del proyecto original de dichas aplicaciones. Lo importante aquí es la idea de libertad que promulga el proyecto GNU (de ahí su uso en el término) y la importancia de no referirse a Linux como un sistema operativo completo, ya que por si sólo no sería de mucha utilidad.

Ver también: GNU, FSF, Linux, RMS.

GPL

(*General Public Licence*). Para más detalles diríjase al término *Copyleft*. Si quiere leer la licencia GPL, acceda a la sección: GNU General Public License.

Ver también: GNU.

H

HTTP

(*HyperText Transfer Protocol*). Protocolo empleado para transferir documentos web desde un servidor a un navegador.

I

IANA

(*Internet Assigned Number Authority*). Formada esencialmente por una persona, Jon Postel, IANA

fue la responsable originalmente de la asignación de direcciones IP y las constantes utilizadas en los protocolos TCP/IP. En 1999 fue reemplazada por ICANN.

Ver también: ICANN.

ICANN

(*Internet Corporation For Assigned Names and Numbers*). La organización que asumió las tareas de IANA después de la muerte de Jon Postel.

Ver también: IANA.

ID

(*IDentification*). Acrónimo de IDentificación.

IEEE

(*Institute of Electrical and Electronics Engineers*). Instituto de Ingenieros Eléctricos y Electrónicos.

IETF

(*Internet Engineering Task Force*). IETF es una organización de Internet compuesta por expertos en software y hardware que discuten nuevas tecnologías para la red y muy frecuentemente llegan a conclusiones que se plasman en estándares.

TCP/IP es el ejemplo más notorio de este grupo. IETF no sólo estandariza, sino también crea borradores, discusiones, ideas o útiles tutoriales que son escritos en los famosos RFCs, disponibles al público e incluidos en muchos de los CDs de GNU/Linux o BSD.

Ver también: IPP, PWG, SSL, SSL.

IP

(*Internet Protocol*). El protocolo estándar TCP/IP define los datagramas IP como la unidad de información pasada a través de una interred que provee el servicio básico para la entrega de paquetes en conexiones no orientadas a conexión y de mejor esfuerzo. La suite protocolar completa suele referirse como TCP/IP porque TCP e IP son los dos protocolos fundamentales.

Ver también: TCP, TCP/IP.

IPC

(*InterProcess Communication*). IPC hace referencia a los mecanismos de comunicación entre procesos del System V: colas de mensajes, conjuntos de semáforos y segmentos de memoria compartida.

IPng

(*Internet Protocol - the Next Generation*). IPng se aplica a todas las actividades alrededor de la especificación y estandarización de la siguiente versión de IP.

Ver también: IPv6.

IPP

(*Internet Printing Protocol*). IPP está definido en una serie de RFCs aceptados por IETF, con el estado de “proposed standard”; este fue diseñado por PWG.

IPP es un diseño completamente nuevo para la impresión en red, pero utiliza un método bien conocido y probado para la transmisión de datos actual: HTTP 1.1. Para no *reinventar la rueda*, y basado en un estándar de Internet existente y robusto, IPP es capaz de manejar fácilmente otros estándares HTTP como: * autentificación básica, en modo *digest* o utilizando certificados; * SSL o TLS, para la transmisión de datos cifrados; * LDAP para servicios de directorio (publicar datos en una impresora, opciones del dispositivo, controladores, coste de la red; o comprobar una clave mientras se está tratando una autentificación).

Ver también: CUPS, IETF, LDAP, PWG, RFC, SSL, TLS.

IPv4

(*Internet Protocol versión 4*). IPv4 es el nombre oficial de la versión actual de IP.

Ver también: IP.

IPv6

(*Internet Protocol versión 6*). IPv6 es el nombre de la siguiente versión de IP.

Ver también: IPng.

IPX

(*Internetwork Packet eXchange*). IPX es un protocolo de la capa de red no confiable. Este protocolo transfiere paquetes del origen al destino en forma transparente, aun si la fuente y el destino se encuentran en redes diferentes. En lo funcional, IPX es similar a IP, excepto que usa direcciones de 10 bytes en lugar de direcciones de 4 bytes.

Ver también: IP.

ISO

(*International Organization for Standardization*). ISO es un equipo internacional que crea borradores, discute, propone y especifica estándares para los protocolos de red. ISO es muy conocido por su modelo de referencia de 7 capas que describe la organización conceptual de los protocolos. Aunque propuso una suite de protocolos para *Open System Interconnection*, los protocolos OSI no fueron muy aceptados por el mercado comercial.

Ver también: OSI.

K

Kerberos

Sistema de autentificación del Proyecto Athena del Instituto Tecnológico de Massachusetts (MIT).

Basado en el método criptográfico de llave simétrica.

L

LAN

(*Local Area Network*). LAN hace referencia a cualquier red física diseñada para abarcar cortas distancias (algunos miles de metros). Normalmente, las redes LAN operan entre 10 megabits por segundo y varios gigabits por segundo. Un ejemplo de este tipo de redes puede ser Ethernet.

LDAP

(*Lightweight Directory Access Protocol*). LDAP es un protocolo estándar y abierto para acceder a los servicios de directorio X.500. El protocolo se ejecuta sobre los protocolos de transporte de Internet, conocidos como TCP.

LDAP es una alternativa *ligera* al protocolo X.500: *Directory Access Protocol* (DAP), pensado para usarse en Internet (utiliza la pila TCP/IP).

Ver también: X.500, Directory Access Protocol, DAP.

LGPL

(*Lesser General Public License*). Licencia Pública General de “Pequeña” del proyecto GNU.

Ver también: GNU.

Linux

Implementación del núcleo Unix originalmente escrito desde cero, sin código propietario.

El desarrollo del núcleo está coordinado por Linus Torvalds, quien ostenta el copyright de gran parte del mismo. El resto del copyright pertenece a un gran número de contribuidores (o sus empleados). Independientemente de quien posea el copyright, el núcleo en su conjunto está disponible bajo los términos de la licencia pública general, GPL. El proyecto GNU soporta el núcleo Linux como su núcleo hasta que la investigación del núcleo Hurd esté completada.

Este núcleo no es útil sin aplicaciones externas. El Proyecto GNU ha provisto a la comunidad de un gran número de aplicaciones de calidad, que junto con otro software de dominio público se ha convertido en un potente entorno de trabajo Unix. Estas herramientas junto con el núcleo Linux es lo que se conoce como una distribución Linux. Módulos de compatibilidad y/o emuladores existen por docenas en otros ambientes computacionales.

Ver también: GNU, GNU/Linux, GPL.

LPD

(*Line Printer Daemon*). LPD se refiere al demonio de impresión en línea de Berkeley, que históricamente se ha utilizado como sistema de impresión en los sistemas Unix.

LPRng

(*LPR Next Generation*). LPRng es una versión mejorada, extendida y portable de LPR de Berkeley (la cola de impresión estándar de los sistemas UNIX).

Ver también: PyKota.

M

MIME

(*Multipurpose Internet Mail Extensions*). Los tipos MIME se utilizaron por primera vez para permitir la transmisión de datos binarios (como las imágenes adjuntas a un correo electrónico) con el correo electrónico, ya que este se utilizaba normalmente para transmitir únicamente caracteres ASCII. Más tarde este concepto fue extendido para describir un formato de datos independiente de la plataforma, pero al mismo tiempo, de una forma no ambigua.

Bajo el protocolo IPP, los campos de impresión se describen haciendo uso de esquema tipo MIME. Los tipos MIME están registrados en IANA, para que permanezcan sin ambigüedades. CUPS posee algunos tipos MIME, como el tipo *application/vnd.cups-raster*.

Ver también: CUPS, IANA, IPP.

MIT

(*Massachusetts Institute of Technology*). Universidad de ingenierías en Cambridge.

MS-DOS

(*MicroSoft Disk Operating System*). Sistema operativo monousuario que ejecuta un programa cada vez y sólo puede trabajar con un megabyte de memoria, 640 kilobytes de los cuales se usan por el programa de aplicación. Un añadido especial de memoria, EMS, permite al software compatible con EMS exceder el límite de 1 MB. Añadidos de DOS, como Microsoft Windows y DESQview, hacen uso de las ventajas de EMS y permiten al usuario ejecutar más de una aplicación a la vez y cambiar entre ellas.

Ver también: DESQview, EMS.

MS-RPC

(*MicroSoft Remote Procedure*).

Ver también: RPC.

N

NBNS

(*NetBIOS Name Service*). Como su propio nombre indica, NBNS hace referencia a un servidor de nombres basado en NetBIOS.

Ver también: NetBIOS.

NBT

(*NetBios over TCP/IP*). Como su propio nombre indica, NBT no es más que el protocolo NetBios sobre el conjunto de protocolos definido por TCP/IP

Ver también: NetBIOS, TCP/IP.

NFS

(*Network File Sharing*). Protocolo desarrollado por SUN Microsystems. Hace uso del protocolo IP para permitir a un conjunto de ordenadores el acceso a los sistemas de archivos de cada uno de ellos como si fuesen locales.

NetBEUI

(*NetBIOS Extended User Interface*). NetBEUI es un protocolo de bajo coste diseñado para pequeñas redes, que permite a cada ordenador de la red utilizar un nombre que todavía no esté en uso.

Ver también: NetBIOS.

NetBIOS

(*Network Basic Input Output System*). NetBIOS es la interfaz estándar para redes en PCs IBM y ordenadores personales compatibles. TCP/IP incluye una serie de guías que describen como mapear las operaciones NetBIOS en las operaciones TCP/IP equivalentes.

NIS

(*Network Information Services*). NIS es muy utilizado para permitir a varias máquinas de una red compartir la misma información de las cuentas de usuario (por ejemplo el archivo de claves). NIS se denominaba originalmente Yellow Pages (YP).

Ver también: YP.

NSCD

(*Name Service Cache Daemon*). nscd es un demonio que administra las búsquedas de claves, grupos y hosts de los programas que están en ejecución, cacheando los resultados obtenidos para la siguiente petición. Esta caché está indicada para servicios lentos, como pueden ser: LDAP, NIS o NIS+.

O

OSI

(*Open Systems Interconnection*). OSI es la referencia para los protocolos desarrollados por ISO como competidor de TCP/IP. Actualmente ya no se desarrolla ni tiene soporte.

Ver también: ISO, TCP/IP.

P

Palladin

Sistema de impresión desarrollado por el MIT.

Ver también: MIT.

PAM

(*Pluggable Authentication Modules*). Suite de librerías compartidas que permiten al administrador local del sistema la elección del método que van a utilizar las aplicaciones para autentificar a los usuarios.

PCL

(*Printer Control Language*). Un lenguaje descriptivo utilizado por las impresoras Laserjet de Hewlett-Packard.

PDC

(*Primary Domain Controller*). Un PDC es un servidor Windows encargado de autentificar a los usuarios dentro de un dominio Windows así como establecer los permisos asociados. Otras de sus funciones es la de almacenar y mantener la base de datos del dominio, denominada SAM.

Ver también: SAM, PDC.

PDF

(*Portable Document Format*). Acrónimo de Formato de Documentación Portable, cuyo nombre es autoexplicativo.

PJL

(*Print Job Language*). PJL fue desarrollado por Hewlett-Packard para controlar las características por defecto y por trabajo de una impresora.

Ver también: PPD.

PLP

(*Portable Line Printer*). Sistema de control de colas de impresión en línea portátil. Más detalles aquí (http://www-usa.iona.com//hyplan/jmason/plp.html).

POSIX

(*Portable Operating System for unIX*). La interfaz de sistema operativo portátil para UNIX es una compilación de estándares para los sistemas operativos basados en UNIX.

PPD

(*PostScript Printer Description*). PPD no es más que un archivo ASCII que almacena toda la información sobre las capacidades especiales de una impresora. Además almacena también la definición de las órdenes PostScript o PJL para hacer uso de capacidades específicas de una impresora.

Ver también: CUPS, PJL, PS.

Printer-MIB

(*Printer-Management Information Base*). Printer-MIB define un conjunto de parámetros que han de ser almacenados dentro de la impresora para que puedan ser accedidos a través de la red.

Ver también: PWG.

PS

(*PostScript*). PostScript (normalmente abreviado como PS) es el estándar de facto en el sistema de impresión del mundo UNIX. Fue desarrollado por Adobe y licenciado a los ensambladores y compañías de software. Como las especificaciones de PostScript fueron publicadas por Adobe, existen implementaciones de terceros para generar e interpretar PostScript disponibles (como el conocidísimo programa de Software Libre Ghostscript, un potente intérprete de PS).

Ver también: CUPS, PPD.

PWG

(*Printer Working Group*). PWG es un grupo cerrado de representantes de la industria de la impresión, que en los pasados años han desarrollado diferentes estándares en relación con la impresión en red.

Las últimas propuestas aceptada por IETF como RFC han sido “Printer-MIB” e IPP.

Ver también: IETF, IPP, Printer-MIB, RFC.

PyKota

PyKota es una solución software GPL para cuotas y cuentas de impresión. Puede ser utilizado tanto con CUPS como con LPRng y en sistemas GNU/Linux y sistemas operativos similares a UNIX.

PyKota ofrece gran flexibilidad gracias a los distintos métodos de contado de página que soporta.

Ver también: CUPS, LPRng.

R

RDN

(*Relative Distinguished Name*). RDN corresponde al nombre de una entrada en el servicio de directorio LDAP.

RFC

(*Request For Comment*). *Petición de comentarios*, un modo habitual de publicar ideas de nuevos protocolos o procedimientos para ser evaluados por la comunidad de Internet. Aunque los RFCs no son obligatorios, muchas aplicaciones intentan adherirse a ellos, una vez aprobados por la comunidad.

Ver también: IPP, PWG.

RID

(*Relative IDentifier*). RID es un número único dentro de un dominio Windows que identifica a un usuario, un grupo, un ordenador o cualquier otro objeto. El número RID es análogo al *user ID* (UID) o al *group ID* (GID) en un sistema Unix o dentro de un dominio NIS.

Ver también: GID, UID.

RIP

(*Raster Image Processor*).

RMS

(*Richard Matthew Stallman*).

Ver también: FSF, GNU.

RPC

(*Remote Procedure Call*). Tecnología por la cual un programa invoca servicios a través de la red haciendo distintas llamadas a procedimientos.

S

SAM

(*Security Account Manager*). SAM es el servicio encargado de mantener la base de datos, con la información asociada a un dominio, en los controladores de dominio de los sistemas Windows.

Samba

Samba es una suite de aplicaciones Unix que "habla" el protocolo SMB (*Server Message Block*). Muchos sistemas operativos, incluidos MS Windows y OS/2, usan SMB para operaciones de red cliente-servidor. Mediante el soporte de este protocolo, Samba permite a los servidores Unix entrar en acción, comunicando con el mismo protocolo de red que los productos de Microsoft Windows. De este modo, una máquina Unix con Samba puede enmascararse como servidor en su red Microsoft.

Ver también: CIFS, SMB.

SASL

(*Simple Authentication and Security Layer*). SASL es un método para añadir soporte de autentificación a los protocolos basados en conexión.

SAT

(*Security Access Token*). Señal de acceso que es creada en un cliente Windows una vez que el controlador de dominio ha verificado y validado el usuario y la clave de acceso enviada por el cliente durante el proceso de ingreso en el dominio Windows. Esta señal contiene la información sobre el usuario codificada en su interior, la cual incluye el nombre de usuario, el grupo y los permisos que el usuario posee en el dominio.

SID

(*Security IDentifier*). Los SIDs se utilizan para identificar objetos en un dominio de sistemas Windows. Estos objetos pueden ser, aunque no se limitan sólo a esta pequeña muestra, los usuarios, los grupos, los ordenadores y los procesos.

SMB

(*Server Message Block*). SMB es un protocolo de compartición de archivos, impresoras, puertos serie y abstracción de comunicaciones (como *pipas* y *slots* de correo) entre ordenadores.

Ver también: CIFS, Samba.

SNMP

(*Simple Network Management Protocol*).

SSL

(*Secure Socket Layer*). SSL es un método de cifrado propietario para la transmisión de datos a través del protocolo HTTP, que fue desarrollado por Netscape y hoy en día está siendo reemplazado por un estándar de IETF denominado TLS.

Ver también: IETF, IPP, TLS.

SWAT

(*Samba Web Administration Tool*). SWAT es una interfaz web que se puede utilizar para la configuración de Samba. Esta herramienta se suministra con Samba.

Ver también: Samba.

T

TCP

(*Transmission Control Protocol*). Protocolo de la capa de transporte del estándar TCP/IP que provee el servicio confiable y *full duplex* del cual dependen muchos protocolos de aplicación. TCP permite a un proceso de una máquina el envío de datos a un proceso de otra máquina. TCP está orientado a conexión en el sentido de que antes de transmitir información, los participantes han de establecer una conexión. Todos los datos viajan en segmentos TCP, cada uno de los cuales viaja a través de Internet en un datagrama IP. La suite protocolar completa suele referirse como TCP/IP porque TCP e IP son los dos protocolos fundamentales.

Ver también: IP, TCP/IP.

TCP/IP

(*Suite protocolar de Internet TCP/IP*). Nombre oficial de los protocolos TCP/IP.

Ver también: IP, TCP.

TLS

(*Transport Layer Security*). TLS es el sucesor del protocolo SSL, creado por IETF para la comunicación general (tanto de autentificación como de cifrado) de las redes TCP/IP. La versión 1 de TLS es prácticamente idéntica a la versión 3 de SSL.

Ver también: IETF, IPP, SSL.

U

UDP

(*User Datagram Protocol*). UDP es un protocolo que permite a un programa en una determinada máquina enviar un datagrama a otra aplicación ejecutándose en otra máquina. UDP hace uso del protocolo de Internet (IP) para enviar los datagramas. Conceptualmente, la diferencia más importante entre los datagramas UDP y los datagramas IP es que UDP incluye el número del puerto, permitiendo al emisor distinguir entre múltiples programas en una determinada máquina destino.

Ver también: IP.

UID

(*User IDentification*). Número único que identifica a un usuario dentro de un sistema Unix o en un dominio NIS.

Ver también: GID, RID.

UNC

(*Universal Naming Convention*). UNC hace referencia a la notación empleada en el mundo Windows para referirse a los recursos compartidos en una red (*maquina-de-red**directorio*).

Unicode

Conjunto de caracteres de 16 bits estándar, diseñado y mantenido por el consorcio sin ánimo de lucro Unicode Inc.

Unicode se ha diseñado para ser universal, único y uniforme. Esto quiere decir: el código debe cubrir los mayores lenguajes modernos escritos (universal), cada carácter tienen que poseer exactamente una codificación (único) y cada carácter se debe representar por un conjunto de bits fijo (uniforme).

URI

Universal Resource Identifier.

URL

(*Uniform Resource Locators*). URL hace referencia a una cadena que hace referencia a una pieza de información. La cadena comienza con el tipo de protocolo (por ejemplo: FTP) seguida de la identificación de una información específica (por ejemplo el nombre del dominio de un servidor y la ruta a un determinado archivo en dicho servidor).

V

VFS

Virtual File System.

W

WAN

(*Wide Area Network*). Cualquier red física que se extienda a lo largo de una zona geográfica muy amplia. Las redes WAN tienen retrasos y costes más altos que las redes que operan sobre distancias más cortas.

Ver también: LAN.

WINS

(*Windows Internet Name Service*). WINS es el nombre de la implementación NBNS de Microsoft.

Ver también: NBNS.

X

X.500, Directory Access Protocol

Ver también: DAP, LDAP.

Y

YP

(*Yellow Pages*). YP fue el nombre original de la implementación de Sun (http://www.sun.org) de *Network Information Service*

Ver también: NIS.