LDAP-Linux-Como

Luiz Ernesto Pinheiro Malere, `malere@yahoo.com`. Traducción de J. Iván Juanes Prieto, `kerberos@insflug.org`. v1.01, 15 febrero 2000

En este documento se presenta la información acerca de la instalación, configuración, ejecución y mantenimiento de un servidor del Protocolo Ligero de Acceso a Directorios (LDAP) en una máquina Linux. También se dan detalles sobre cómo crear bases de datos LDAP, cómo actualizar y borrar información de la base de datos, cómo implementar acceso móvil y cómo utilizar la Libreta de Direcciones (Address Book) de Netscape. Este documento está fuertemente inspirado en las páginas informativas de LDAP de la Universidad de Michigan.

Contents

1 Introducción

La finalidad principal de este documento es permitirle configurar y utilizar un Servidor de directorio LDAP (Protocolo Ligero de Acceso a Directorios) en su máquina Linux. Aprenderá cómo instalar, configurar, ejecutar y mantener el servidor LDAP. Después, aprenderá también cómo almacenar, recuperar y actualizar información en su Directorio, utilizando las utilidades y clientes LDAP. El demonio o programa servidor para el directorio LDAP se llama *slapd* y puede ejecutarse sobre muchas plataformas UNIX diferentes.

Hay otro demonio o programa servidor que se encarga de la replicación entre servidores. Su nombre es `slurpd` y por el momento no necesitará preocuparse de él. En este documento, ejecutaremos un *slapd* que proporciona servicio de directorio para su dominio local únicamente, es decir, sin *slurpd*.

He aquí una configuración sencilla del servidor, válida para empezar, pero fácil también de actualizar a una configuración distinta más adelante, si lo desea. La información que se presenta en este documento representa una buena forma de iniciarse en el uso del protocolo LDAP. Es probable que tras la lectura del documento se sienta con fuerzas para ampliar las capacidades de su servidor, e incluso con ganas de escribir sus propios clientes, usando los entornos de desarrollo ya existentes para C, C++ y Java.

1.1 ¿Qué es LDAP?

LDAP ("Lightweight Directory Access Protocol", «Protocolo Ligero de Acceso a Directorios») es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio. Se usó inicialmente como un *front-end* o interfaz final para X.500, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

1.2 ¿Qué es un servicio de directorio?

Un directorio es como una base de datos, pero en general contiene información más descriptiva y más basada en atributos. La información contenida en un directorio normalmente es lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción (*rollback*) que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos. Por contra, las actualizaciones en un directorio son usualmente cambios sencillos de «todo o nada», si es que se permiten en algo.

Los directorios están afinados para proporcionar una repuesta rápida a operaciones de búsqueda o consulta. Pueden tener la capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y la fiabilidad, y a la vez reducir el tiempo de respuesta. Cuando se duplica (o se replica) la información del directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización.

Existen muchas maneras distintas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados, etc. Algunos servicios de directorio son locales, proporcionando servicios a un contexto restringido (por ejemplo, el servicio de `finger` en una única máquina). Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

1.3 ¿Cómo funciona LDAP?

El servicio de directorio LDAP se basa en un modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol del directorio LDAP o base de datos troncal. el cliente ldap se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de dónde puede el cliente hallar más información (normalmente otro servidor LDAP). No importa con qué servidor LDAP se conecte el cliente: siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que haría referencia en otro servidor LDAP. Es ésta una característica importante de un servicio de directorios universal como LDAP.

1.4 Backends, objetos y atributos en LDAP

slapd se suministra con tres diferentes bases de datos de backend (dorsal, o base de datos de segundo plano) entre las que elegir. Se trata de LDBM, una base de datos de gran rendimiento basada en disco: SHELL, una interfaz de base de datos para órdenes arbitrarias de UNIX o guiones (scripts) del intérprete de órdenes (shell); y PASSWD, una sencilla base de datos de contraseñas.

En el desarrollo de este documento, se da por supuesto que ha elegido la base de datos LDBM.

La base de datos LDBM funciona asignando un identificador compacto de cuatro bytes, único para cada entrada de la base de datos. La base de datos utiliza este identificador para hacer referencia a entradas en los índices. La base de datos está compuesta de un fichero índice principal, llamado `id2entry`, que mapea el identificador único de una entrada en la representación en texto de esa misma entrada. También se da mantenimiento a otros ficheros índice.

Para importar y exportar información de directorio entre servidores de directorios basados en LDAP, o para describir una serie de cambios que han de aplicarse al directorio, se usa en general del fichero de formato conocido como LDIF (siglas de *"LDAP interchange format"*, «formato de intercambio de LDAP»). Un fichero LDIF almacena información en jerarquías de entradas orientadas a objeto. El paquete de software LDAP que va a utilizar incluye una utilidad para convertir ficheros LDIF a formato LDBM.

Un fichero LDIF corriente tiene este aspecto:

```
dn: o=Insflug, c=ES
o: Insflug
objectclass: organization
dn: cn=Luiz Malere, o=Insflug, c=ES
cn: Luiz Malere
sn: Malere
mail: malere@yahoo.com
objectclass: person
```

Como puede comprobar, cada entrada está identificada unívocamente por un nombre distintivo (`DN`, *"distinguished name"*). El DN (nombre distintivo) está compuesto por el nombre de la entrada en cuestión, más la ruta de nombres que permiten rastrear la entrada hacia atrás hasta la parte superior de la jerarquía del directorio.

En LDAP, una clase de objetos define la colección de atributos que pueden usarse para definir una entrada. El estándar LDAP proporciona estos tipos básicos para las clases de objetos:

- Grupos en el directorio, entre ellos listas no ordenadas de objetos individuales o de grupos de objetos.
- Emplazamientos, como por ejemplo el nombre del país y su descripción.
- Organizaciones que están en el directorio.
- Personas que están en el directorio.

Una entrada determinada puede pertenecer a más de una clase de objetos. Por ejemplo, la entrada para personas se define mediante la clase de objetos `person`, pero también puede definirse mediante atributos en las clases de objetos `inetOrgPerson`, `groupOfNames` y `organization`. La estructura de clases de objetos del servidor (su esquema) determina la lista total de atributos requeridos y permitidos para una entrada concreta.

Los datos del directorio se representan mediante pares de atributo y su valor. Cualquier pieza de información específica se asocia con un atributo descriptivo.

Por ejemplo el atributo `commonName`, o `cn` («nombre de pila»), se usa para almacenar el nombre de una persona. Puede representarse en el directorio a una persona llamada Jonás Saqueiro mediante

```
cn: Jonás Saqueiro
```

Cada persona que se introduzca en el directorio se define mediante la colección de atributos que hay en la clase de objetos *person*. Otros atributos que se usan para definir esta entrada serán:

```
givenname: Jonás
surname: Saqueiro
mail: jonass@midominio.com
```

Los atributos requeridos son aquellos que deben estar presentes en las entradas que utilicen la clase de objetos. Todas las entradas precisan del atributo `objectClass`, que lista las clases de objeto a las que pertenece una entrada.

Los atributos permitidos son aquellos que pueden estar presentes en las entradas que utilicen la clase de objetos. Por ejemplo, en la clase de objetos `person`, se requieren los atributos `cn` y `sn`. Los atributos `description` («descripción»), `telephoneNumber` («número de teléfono»), `seeAlso` («véase también»), y `userpassword` («contraseña del usuario») se permiten pero no se requieren.

Cada atributo tiene la definición de sintaxis que le corresponde. La definición de sintaxis describe el tipo de información que proporciona ese atributo:

- `bin` binario
- `ces` cadena con mayúsculas y minúsculas exactas (las mayúsculas y minúsculas son significativas durante las comparaciones)
- `cis` cadena con mayúsculas y minúsculas ignoradas (las mayúsculas y minúsculas no son significativas durante las comparaciones)
- `tel` cadena de número de teléfono (como `cis`, pero durante las comparaciones se ignoran los espacios en blanco y los guiones `"-"`)
- `dn` "distinguished name" («nombre distintivo»)

Para conocer en qué lugar de su sistema se emplazan las definiciones de clases de objetos y de atributos, véase el primer párrafo de la 3 (sección 3).

1.5 Nuevas versiones de este documento.

Este documento puede experimentar actualizaciones y correcciones en razón de la respuesta que suscite entre sus lectores. Por favor busque nuevas versiones del original inglés en:

http://www.ddtc.dimes.tudelft.nl/˜malere/LDAP-Linux-HOWTO.html `<http://www.ddtc.dimes.tudelft.nl/~malere/LDAP-Linux-HOWTO.html>`

(y nuevas versiones de la traducción castellana de este *Cómo* en *http://www.insflug.org/* `<http://www.insflug.org/>`, **N. del T.**)

1.6 Opiniones y sugerencias

Si tiene alguna duda sobre cualquier información disponible en este documento, por favor contacte con nosotros en la siguiente dirección de correo electrónico:

malere@yahoo.com `<mailto:malere@yahoo.com>`

Si tiene algún comentario o sugerencia, no dude en comunicármelo.

1.7 Agradecimientos

Este *Cómo* es el resultado de unas prácticas que hemos realizado en la universidad de TUDelft, en Holanda. Queremos dar las gracias a las personas que nos animaron a escribir este documento: Rene van Leuken y Wim Tiwon. Muchísimas gracias. También ellos son entusiastas del Linux como nosotros.

1.8 Copyright y descargo de responsabilidad.

 Si tiene cualquier tipo de sugerencia, por favor envíeme un correo electrónico (actualizaré el documento si la sugerencia es adecuada).

Si desea una traducción, por ejemplo al Portugués, puede enviarme también un correo sobre el particular.

No liability for the contents of this document can be accepted. I have no responsability about the consequences of following the Steps provided in this document.

Si tiene preguntas, por favor contacte con el coordinador de Linux HOWTO en

linux-howto@metalab.unc.edu `<linux-howto@metalab.unc.edu>`

2 Instalación del servidor LDAP

Cuatro pasos son necesarios para instalar el servidor: obtener el paquete, descomprimir y desempaquetar el servidor, configurar los ficheros `Makefile` del programa y compilar el servidor.

2.1 Obtención del paquete

Existen dos servidores LDAP que se distribuyen libremente: el servidor LDAP de la Universidad de Michigan y el servidor *OpenLDAP*. También está el *Netscape Directory Server*, que es libre sólo bajo ciertas condiciones (por ejemplo, las instituciones educativas lo pueden obtener gratis). El servidor *OpenLDAP* está basado en la última versión del servidor de la Universidad de Michigan, y hay disponibles listas de correo y documentación adicional para él. Este documento da por supuesto que está Usted utilizando el servidor *OpenLDAP*.

La versión comprimida en formato `.gz` está disponible en la siguiente dirección:

http://www.openldap.org `<http://www.openldap.org>`

Si desea obtener la última versión del servidor de la Universidad de Michigan, diríjase a esta dirección:

ftp://terminator.rs.itd.umich.edu/ldap `<ftp://terminator.rs.itd.umich.edu/ldap>`

Para escribir este documento nos hemos basado en la última versión estable de *OpenLDAP*, utilizando OpenLDAP 1.2.8 sobre un servidor Slackware Linux con núcleo 2.2.6. En la sede Web de *OpenLDAP* encontrará las últimas versiones estables y de desarrollo del servidor OpenLDAP. En el momento de actualizar este documento, la última versión era `/openldap-stable-20000129.tgz`. La última versión de desarrollo era `openldap-1.2.9.tgz` (eran las últimas versiones en el momento de traducir, **N. del T.**)

2.2 Desempaquetado del servidor

Ahora que ya dispone del archivo `.tar.gz` en su máquina local, puede desempaquetarlo.

En primer lugar, copie el paquete en un directorio de su conveniencia, por ejemplo `/usr/local`.

Luego utilice la siguiente orden:

```
tar xvzf openldap-stable.tgz
```

También puede usar la siguiente orden:

```
gunzip openldap-stable.tgz | tar xvf -
```

2.3 Configuración del programa

Hay varias opciones que tal vez desee personalizar, de manera que el programa se construya de la forma más adaptada a sus sistema.

Para configurar el programa sólo necesita dos pasos:

- Edite el fichero `ldapconfig.h.edit`, situado en el subdirectorio `include/` que cuelga del directorio en el que ha desempaquetado el programa.

- Ejecute el guión `./configure`. Si le gustan las emociones fuertes, puede editar igualmente el fichero `Make-common` en lugar de ejecutar el guión de configuración :ˆ)

En el fichero `include/ldapconfig.h.edit` puede configurar opciones como el emplazamiento de los demonios *slapd* y *slurpd*. El fichero propiamente dicho contiene muchos comentarios y sus opciones por defecto también reflejan las opciones que los administradores eligen con más frecuencia, de manera que si tiene prisa puede saltarse este paso y ejecutar directamente:

```
vi include/ldapconfig.h.edit
```

El código fuente de *OpenLDAP* se distribuye con un guión de configuración para ajustar opciones como por ejemplo el directorio de instalación y las ««banderas»» del compilador y del enlazador. Escriba la orden siguiente en el directorio donde haya desempaquetado el programa:

```
./configure --help
```

Ello mostrará por pantalla todas las opciones que puede personalizar con el guión `configure` antes de compilar el programa. Algunas opciones útiles para establecer los directorios de instalación son `-prefix=pref`, `-exec-prefix=eprefix` y `-bindir=dir`. Normalmente, si ejecuta `./configure` sin opciones, él mismo autodetectará las opciones adecuadas y se preparará para construir el paquete en la localización común predeterminada. Así pues, teclee:

```
./configure
```

Y observe el resultado por pantalla para verificar que no se produce ningún error.

2.4 Compilación del servidor

Después de configurar el programa puede empezar a compilarlo. Primero construya las dependencias mediante la orden:

```
make depend
```

Después compile el servidor mediante la orden:

```
make
```

Si todo va bien, el servidor se compilará tal y como se haya configurado. En caso contrario, vuelva al paso anterior para revisar las opciones de configuración. Revise las sugerencias específicas para su plataforma, que se hallan en la ruta `doc/install/hints` que cuelga del directorio en el que desempaquetó el software.

Instale luego los ejecutables y las páginas de manual. Es posible que precise de permisos de superusuario para poder llevarlo a cabo (depende del lugar en donde instale los ficheros):

```
su
make install
```

Es todo. Ya dispone del ejecutable del servidor y de los ejecutables de otras varias utilidades. Para saber cómo configurar el funcionamiento de su servidor LDAP, véase la sección 3 (siguiente).

Si antes de aprender cómo se configura su servidor LDAP desea verificar los ejecutables recién compilados, las últimas versiones del servidor *OpenLDAP* vienen con un guión de verificación. Cuando se actualizó este documento el guión de verificación no era estable al 100% para todos los diagnósticos que llevaba a cabo. De todas maneras pruébelo y ejecútelo, si algún aspecto del guión no funciona bien, siempre puede pararlo pulsando `Ctrl+C`. En nuestro caso, antes de que el guión o script se detuviera, pudimos observar algunos mensajes que mostraban que los diagnósticos más comunes se habían llevado a cabo con éxito. Para ejecutar el guión de verificación, cámbiese al subdirectorio `test/` que cuelga de la ruta en la que desempaquetó el software, y luego teclee:

```
make
```

3 Configuración del servidor LDAP

Cuando el software se haya compilado e instalado, ya puede configurarlo para utilizarlo en su servidor. Toda la configuración en tiempo de ejecución de *slapd* se realiza mediante el fichero `slapd.conf`, que se instala en el directorio que haya especificado en `-prefix` en el guión de configuración, o bien, si no especificó ninguno, en `/usr/local/etc/openldap` de forma predeterminada.

En este directorio hallará asimismo los ficheros `slapd.oc.conf` y `slapd.at.conf` que se incluyen en el fichero `slad.conf` (véase la opción *include* en la 3.2 (sección 3.2)) y que incluyen, respectivamente, las definiciones de clases de objetos (*objectclasses*) y atributos para la base de datos de segundo plano de LDAP (*backend*). Lo que sigue es una descripción del formato general del fichero de configuración, y continuaremos con una descripción detallada de cada opción del fichero de configuración.

3.1 Formato del fichero de configuración

El fichero `slapd.conf` está compuesto por una serie de opciones globales de configuración que afectan a `slapd` en su conjunto (incluyendo todas las bases de datos de segundo plano o *backends*), seguido por cero o más definiciones de *backends*, las cuales contienen información específica de una instancia de *backend*.

Las opciones globales de configuración pueden anularse en un *backend* determinado (para opciones que aparecen más de una vez, se usa la última aparición en el fichero de configuración `slapd.conf`). Se ignoran las líneas en blanco y las líneas de comentario que comienzan por el carácter de «#». Si una línea comienza por un espacio en blanco, se considera una continuación de la línea anterior. El formato general del fichero `slapd.conf` es el siguiente:

```
# comentario - estas opciones se aplican a cualquier base de datos
<opciones de configuración globales>
# definición de la base de datos y opciones de configuración
database <backend tipo 1>
<opciones de configuración específicas del backend tipo 1>
#definición de la segunda base de datos y opciones de configuración
database <backend tipo 2>
<opciones de configuración específicas del backend tipo 2>
# definiciones subsiguientes de bases de datos y opciones de configuración
...
```

Los argumentos de la línea de configuración están separados por espacios en blanco. Si un argumento contiene espacios en blanco, el argumento debe encerrarse entre comillas dobles `"de esta manera"`. Si un argumento contiene unas dobles comillas o una barra invertida '\', el carácter ha de ir precedido de una barra invertida '\', (p. ej. '\\d').

La distribución de *OpenLDAP* contiene un fichero de configuración de ejemplo que se instalará en el directorio de configuración especificado en `-prefix`. También se proporcionan un `slapd.at.conf`, que contiene muchas definiciones de atributos utilizadas a menudo, y `slapd.oc.conf`, que contiene muchas definiciones de clases usadas con frecuencia.

3.2 Opciones globales

Las opciones que se describen en esta sección se aplican a todos los *backends*, a menos que se sobreescriban o anulen específicamente en la definición de un *backend* concreto. Los argumentos de opción que han de sustituirse por texto de verdad se muestran entre signos de «mayor que» y «menor que» <>.

access to <algo> [by <quién> <niveldeacceso>]+

Esta opción concede acceso (especificado en <niveldeacceso>) a una serie de entradas o atributos (especificados por <algo>) para uno o más peticionarios (especificados en <quién>). Véanse los ejemplos de control de acceso para más detalles.

attribute <nombre> [<nombre2>] { bin | ces | cis | tel | dn }

Esta opción asocia a una sintaxis con un nombre de atributo. Por defecto se supone que un atributo tiene sintaxis «cis». Se le puede proporcionar a un atributo un nombre alternativo opcional. Las posibles reglas de sintaxis y su significado son éstas:

- bin: binario
- ces: cadena con mayúsculas y minúsculas exactas (las mayúsculas y minúsculas son significativas durante las comparaciones)
- cis: cadena con mayúsculas y minúsculas ignoradas (las mayúsculas y minúsculas no son significativas durante las comparaciones)
- tel: cadena de número de teléfono (como «cis», pero durante las comparaciones se ignoran los espacios en blanco y los guiones "-")
- dn: "distinguished name" («nombre distintivo»)

defaultaccess { none | compare | search | read | write }

Esta opción especifica el acceso por defecto que se concederá a los solicitantes que no coincidan con ninguna otra línea de acceso (véanse los ejemplos de control de acceso más abajo). Nótese que un nivel de acceso implica en sí también los niveles de acceso inferiores a él. Por ejemplo, el acceso a escritura implica el acceso a lectura, el acceso a búsqueda y el acceso a comparación.

Valor predeterminado: `defaultaccess read`

include <nombrefichero>

Esta opción ordena a *slapd* que lea información adicional de configuración desde el fichero especificado, antes de continuar con la línea siguiente del fichero actual. El fichero que se especifica ha de seguir el formato normal de configuración de *slapd*. Utilice esta opción para incluir ficheros que contengan las clases de objetos (*objectclass*) y definiciones de atributo (*attribute definitions*) de su base de datos de segundo plano o *backend*. El paquete de software de LDAP viene con los ficheros `slapd.oc.conf` y `slapd.at.conf`.

Nota: Tenga cuidado al utilizar esta opción. No hay límite mínimo en el número de opciones `include` anidadas, ni tampoco se hace una detección de anidamiento para el caso de bucles sin fin.

loglevel <numeroentero>

Esta opción especifica el nivel de detalle con el que el sistema debe registrar en un archivo de registro (syslog) las informaciones de depuración y las estadísticas de funcionamiento (en este caso se registran mediante el servicio LOCAL4 de `syslogd(8)`. Para que esta característica esté habilitada, es necesario haber compilado *slapd* con la opción de compilación -DLDAP_DEBUG, excepto para los dos niveles de estadísticas, que están siempre habilitados. Los niveles de registro son acumulativos. Para visualizar qué números corresponden a cada tipo de depuración, ejecute `slapd` con la opción `-?` o consulte la tabla de más abajo. Los valores posibles para <numeroentero> son:

- 1 trazado de llamadas a función
- 2 manejo de paquetes de depurado
- 4 depurado de trazado intensivo *heavy trace*
- 8 gestión de conexiones
- 16 mostrar los paquetes enviados y recibidos
- 32 procesado del filtro de búsqueda
- 64 procesado de ficheros de configuración
- 128 procesado de listas de control de acceso
- 256 estadísticas de registro de conexiones/operaciones/resultados
- 512 enviar las entradas de registro de estadísticas
- 1024 imprimir los *backends* de comunicación con el intérprete de órdenes
- 2048 imprimir el análisis completo de depuración

Ejemplo: `loglevel 255` hará que grandes cantidades de información vayan a un archivo de registro a través de syslog.

Valor predeterminado: `loglevel 256`

objectclass <nombre>

```
objectclass <nombre>
[ requires <atributos> ]
[ allows <atributos> ]
```

Esta opción define las reglas de estructura o esquema para la clase de objetos (*objectclass*) especificada. Se usa junto con la opción **schemacheck**.

referral <url>

Esta opción especifica la autoridad en la que basarse cuando *slapd* no pueda hallar una base de datos local para gestionar una petición.

Ejemplo: `referral ldap://ldap.itd.umich.edu`

Esto remitirá las consultas no locales al servidor LDAP de la Universidad de Michigan. Algunos clientes LDAP con capacidades inteligentes podrán redirigir su consulta a dicho servidor, pero tenga en cuanta que la mayoría de esos clientes no gestionarán URLs sencillas de LDAP que contengan una parte de nombre de máquina y, como opción, una parte de nombre distintivo (`dn`).

schemacheck { on | off }

Esta opción activa (**on**) o desactiva (**off**) la verificación de estructura. Si la verificación de estructura está activada, se comprobarán las entradas que se añadan o modifiquen, con el fin de garantizar que obedecen a las reglas de estructura o esquema que implica la clase de objetos (*objectclass*) a la que pertenecen, tal y como las definen las correspondientes opciones de la clase de objetos correspondiente. Si la verificación de estructura está desactivada (**off**), esta verificación no se realiza.

Valor predeterminado: `schemacheck off`

sizelimit <numeroentero>

Esta opción especifica el número máximo de entradas que hay que devolver de una operación de búsqueda.

Valor predeterminado: `sizelimit 500`

srvtab <nombrefichero>

Esta opción especifica el fichero `srvtab` en el que *slapd* puede encontrar las claves *kerberos* necesarias para autentificar a los clientes que usen *kerberos*. Esto opción es significativa únicamente si Usted utiliza autentificación por *kerberos*, que ha de activarse en el momento de la compilación incluyendo las definiciones apropiadas en el fichero `Make-common`.

Valor predeterminado: `srvtab /etc/srvtab`

timelimit <numeroentero>

Esta opción especifica el número máximo de segundos (en tiempo real) que *slapd* pasará contestando una petición de búsqueda. Si pasado ese tiempo no se ha contestado una petición, se devolverá un resultado que indicará *exceeding time*, «tiempo sobrepasado».

Valor predeterminado: `timelimit 3600`

3.3 Opciones generales del backend

Las opciones de esta sección sólo se aplican al *backend* en el que estén definidas. Estas opciones están soportadas para todos los tipos de *backend*.

database <tipobasededatos>

Esta opción marca el comienzo de la definición de una nueva instancia de base de datos. **<tipobasededatos>** debe ser una de las siguientes: ldbm, shell, o passwd dependiendo del *backend* sobre el que servirá la base de datos.

Ejemplo: `database ldbm` marca el comienzo de la definición de una nueva instancia de una base de datos con *backend* LDBM.

lastmod { on | off }

Esta opción controla si *slapd* mantendrá automáticamente para cada entrada los atributos `modifiersName`, `modifyTimestamp`, `creatorsName` y `createTimestamp`.

Valor predeterminado: `lastmod off`

readonly { on | off }

Esta opción pone a la base de datos en modo «sólo lectura». Cualquier intento de modificar la base de datos devolverá un error de "unwilling to perform" («no se llevará a cabo la operación»).

Valor predeterminado: `readonly off`

replica host=<nombredemaquina>[:<puerto>]

```
replica host=<nombredemaquina>[:<puerto>]
"binddn=<DN>"
bindmethod={ simple | kerberos }
[credentials=<contraseña>]
[srvtab=<nombrefichero>]
```

Esta opción especifica una dirección para la duplicación o réplica esta base de datos. El parámetro `host=` especifica en qué máquina (y opcionalmente, en qué puerto) puede encontrarse la instancia del *slapd* esclavo. para `<nombremáquina>` puede usarse lo mismo un nombre que una dirección IP. Si no se proporciona el parámetro `<puerto>` se usará el puerto estándar de LDAP, el 389.

El parámetro `binddn` proporciona el `DN` al que se vinculará el *slapd* esclavo para sus actualizaciones. Ha de tratarse de un `DN` que tenga acceso de lectura y escritura a la base de datos del esclavo, que normalmente aparece como `rootdn` en el fichero de configuración del esclavo. También tiene que coincidir con la opción `updatedn` en el fichero de configuración del *slapd* esclavo. Puesto que los `DN` son proclives a contener espacios incrustados, la cadena completa `"binddn=<DN>"` ha de estar encerrada entre comillas.

`bindmethod` puede ser o bien `simple` o bien `kerberos`, dependiendo de si se usa autentificación sencilla basada en contraseñas o bien kerberos cuando se conecte con el *slapd* esclavo. La autentificación sencilla precisa que se proporcione una contraseña válida. La autentificación mediante kerberos precisa de un fichero `srvtab` válido.

El parámetro `credentials=`, que sólo se precisa si se usa autentificación sencilla, proporciona la contraseña para `binddn` en el *slapd* esclavo.

El parámetro `srvtab=`, que sólo se precisa si se usa autentificación mediante kerberos, especifica el nombre de fichero que aloja la llave kerberos para el *slapd* esclavo. Si se omite, se utiliza el fichero `/etc/srvtab`.

replogfile <nombrefichero>

Esta opción especifica el nombre del fichero de registro de duplicación (registro de réplica) en el cual *slapd* registrará los cambios. El registro de duplicación generalmente lo escribe *slapd* y lo lee *slurpd*. Esta opción normalmente sólo tiene efecto si se usa *slurpd* para duplicar la base de datos. Sin embargo, puede utilizarla también para generar un registro de transacciones, si *slurpd* no se está ejecutando. En este caso, necesitará truncar periódicamente el fichero, pues de otra manera crecería indefinidamente.

rootdn <dn>

Esta opción identifica al `DN` de una entrada no sujeta a control de acceso o a restricciones en los permisos de administración para las operaciones en esta base de datos.

Ejemplo: `rootdn "cn=Manager, o=U of M, c=US"`

rootkrbname <nombrekerberos>

Esta opción especifica un nombre kerberos que funcionará en todos los casos para el `DN` dado anteriormente, con independencia de que exista una entrada con el `DN` especificado o de que tenga el atributo `krbName`. Esta opción es útil al crear una base de datos y también cuando se utilice *slurpd* para proporcionar servicios de duplicación (servicios de réplica).

Ejemplo: `rootkrbname admin@umich.edu`

rootpw <password>

Esta opción especifica una contraseña, que funcionará en todos los casos, para el `DN` dado anteriormente, con independencia de que el `DN` en cuestión exista o ya tenga contraseña. Esta opción es útil al crear una base de datos y también cuando se utilice *slurpd* para proporcionar servicios de duplicación (servicios de réplica). Evite tener una contraseña de texto sencillo acompañando a esta opción. Proporcione una contraseña cifrada (puede usar una entrada del fichero de Unix `/etc/passwd/`). *slapd* soporta también otros métodos de cifrado.

Ejemplos: `rootpw secret` `rootpw {crypto}contraseña_cifrada_va_aquí`

suffix <dn sufijo>

Esta opción especifica el sufijo `DN` de consultas que se le pasará a la base de datos de *backend*. Pueden proporcionarse múltiples líneas de sufijo, y se requiere al menos una para cada definición de base de datos.

Ejemplo: `suffix "o=University of Michigan, c=US"`

Las consultas que tengan un `DN` terminado en `"o=University of Michigan, c=US"` se le pasarán a este *backend* de base de datos.

Nota: cuando se selecciona el *backend* al que hay que pasarle la consulta, *slapd* examina la línea o líneas de sufijo en cada definición de base de datos en el orden en que aparecen en el fichero. De esta manera, si el sufijo de una base de datos es el prefijo de otra, dicho sufijo debe aparecer después que el prefijo en el fichero de configuración.

updatedn <dn>

Esta opción sólo se aplica a un *slapd* esclavo. Especifica el `DN` al que se le permite hacer cambios en la duplicación. Generalmente se trata del `DN` al que *slurpd* se vincula cuando hace cambios a la duplicación o réplica.

3.4 Opciones específicas del *backend* LDBM

Las opciones de esta categoría sólo se aplican a la base de datos de `backend` LDBM. Es decir, tienen que ir después de una línea `"database ldbm"` y antes de otra línea de `"database"`.

cachesize <numeroentero>

Esta opción especifica a instancia de la base de datos de *backend* LDBM el número de entradas en la memoria caché interna que ha de mantener.

Valor predeterminado: `cachesize 1000`

dbcachesize <numeroentero>

Esta opción especifica el tamaño en bytes de la memoria caché interna asociada con cada fichero de índice abierto. En caso de no estar soportada por el método de base de datos subyacente, esta opción se ignora sin mayores avisos. El incremento de este número utilizará más memoria, pero también causará un aumento espectacular del rendimiento, especialmente durante las modificaciones o a la hora de construir los índices.

Valor predeterminado: `dbcachesize 100000`

directory <directorio>

Esta opción especifica el directorio donde residen los ficheros LDBM que contienen la base de datos y sus ficheros asociados.

Valor predeterminado: `directory` usr/tmp /

index {<listadeatributos> | default} [pres,eq,approx,sub,none]

Esta opción especifica qué índices hay que mantener para un atributo especificado. Si se proporciona únicamente una <listadeatributos> se mantendrán todos los índices posibles.

Ejemplos: `index cn` `index sn,uid eq,sub,approx` `index default none`

Este ejemplo hará que se dé mantenimiento a todos los índices para el atributo `cn`: que se mantengan índices de igualdad, subcadenas y cadenas aproximadas en el caso de los atributos `sn` y `uid`; y que no se mantengan índices para todos los demás atributos.

mode <numeroentero>

Esta opción especifica qué permisos de ficheros (modo de protección) debe tener el índice de la base de datos recién creada.

Valor predeterminado: `mode 0600`

3.5 Ejemplos de control de acceso

La característica de control de acceso presentada en la 3.2 (sección 3.2) es bastante potente. En esta sección se muestran varios ejemplos de su uso. Primeramente, algunos ejemplos sencillos:

```
access to * by * read
```

Esta directiva de acceso concede acceso de lectura a todo el mundo. Si aparece en solitario tiene el mismo efecto que la siguiente línea de `defaultaccess`:

```
defaultaccess read
```

El siguiente ejemplo muestra el uso de una expresión regular para seleccionar las entradas por `DN` en dos directivas de acceso en las que el orden es significativo.

```
access to dn=".*, o=U of M, c=US"
by * search
access to dn=".*, c=US"
by * read
```

El acceso en modo lectura se concede a las entradas que están bajo el sub-árbol `"o=University of Michigan, c=US"`, al que se permite el acceso en modo lectura. Si su hubiera invertido el orden de las directivas de acceso, la directiva específica de la Universidad de Michigan nunca hubiera coincidido, puesto que todas las entradas de la U. de M. son también entradas de `c=US`.

El próximo ejemplo vuelve a mostrar la importancia del orden, tanto en lo que se refiere a las directivas de acceso como a las cláusulas `"by"`. También muestra el uso de un selector de atributos para conceder acceso a un atributo específico y a varios selectores <quién> (<who>).

```
access to dn=".*, o=U of M, c=US" attr=homePhone
by self write
by dn=".*, o=U of M, c=US" search
by domain=.*\.umich\.edu read
by * compare
access to dn=".*, o=U of M, c=US"
by self write
by dn=".*, o=U of M, c=US" search
by * none
```

Este ejemplo se aplica a las entradas en el sub-árbol `"o=U of M, c=US"`. Para todos los atributos excepto `homePhone`, la propia entrada tiene puede escribirlos, otras entradas de "U of M" pueden buscar por ellas, y nadie más tiene acceso. La entrada tiene permisos de escritura sobre el atributo `homePhone`, permisos de búsqueda para otras entradas de la "U of M", permisos de lectura para otros clientes que conecten desde algún lugar del dominio umich.edu, y permisos de comparación para el resto del mundo.

A veces es útil permitir que un `DN` particular se añada o elimine a sí mismo de un atributo. Por ejemplo, si se desea crear un grupo y permitir que los usuarios lo añadan y eliminen de su atributo `member` en su propio `DN`, puede lograrse con una directiva de acceso como la siguiente:

```
access to attr=member,entry
by dnattr=member selfwrite
```

El selector `dnattr` <`quién`> nos dice que el acceso se aplica a entradas listadas en el atributo `member`. El selector `selfwrite access` especifica que tales miembros sólo pueden añadir o eliminar del atributo su propio `DN` y no otros valores. El añadido del atributo `entry` es necesario, ya que se requiere el `access` de la entrada para acceder a alguno de los atributos de esa entrada.

Observe que la construcción `attr=member` en la cláusula <`qué`> es un atajo para la cláusula `"dn=* attr=member"` (es decir, que coincide con el atributo `member` en todas las entradas).

4 Ejecución del servidor LDAP

Slapd puede ejecutarse de dos maneras diferentes, como demonio o servicio permanente, o bien desde `inetd(8)`. Se recomienda la ejecución como demonio permanente, sobre todo si usa el *backend* de LDBM. Ello permitirá al `backend` beneficiarse del uso de memoria de almacenamiento intermedio (*caché*) y evita problemas de acceso compartido a los ficheros de índices de LDBM. Si únicamente ejecuta un *backend* de tipo SHELL o PASSWD, entonces sí puede considerar la opción de ejecutar *slapd* desde `inetd`.

4.1 Opciones desde la línea de órdenes

Slapd soporta las siguientes opciones de línea de órdenes:

-d <nivel> | ?

Esta opción fija el nivel de depuración de *slapd* en <`nivel`>. Cuando el nivel es un carácter '`?`', se muestran los distintos niveles de depuración y *slapd* termina, con independencia de cualquier otra opción que se introduzca. Los niveles de depuración existentes son:

- 1 trazado de llamadas a función
- 2 manejo de paquetes de depurado
- 4 depurado de trazado intensivo *heavy trace*
- 8 gestión de conexiones
- 16 mostrar los paquetes enviados y recibidos
- 32 procesado del filtro de búsqueda
- 64 procesado de ficheros de configuración
- 128 procesado de listas de control de acceso
- 256 estadísticas de registro de conexiones/operaciones/resultados
- 512 enviar las entradas de registro de estadísticas
- 1024 imprimir los *backends* de comunicación con el intérprete de órdenes
- 2048 imprimir el análisis completo de depuración
- 65535 activar depuración completa

Los niveles de depuración son acumulativos. Si desea trazar llamadas a funciones y observar qué fichero de configuración se está procesando, fije el nivel de depuración al resultado de la suma de estos dos niveles (en este caso, 65). Consulte el fichero <`ldap.h`> para más detalles.

Observe que *slapd* se tendrá que haber compilado con la opción `-DLDAP_DEBUG` definida, si se desea un nivel de depuración superior a los dos niveles de estadísticas disponibles.

-f <nombrefichero>

Esta opción especifica un fichero de configuración alternativo para *slapd*

-i

Esta opción le especifica a *slapd* que se ejecute desde `inetd` en vez de hacerlo como un demonio o servicio independiente. En la próxima sección encontrará más detalles sobre la ejecución de *slapd* desde `inetd`.

-p <puerto>

Esta opción especifica un puerto TCP alternativo en el que *slapd* se mantendrá a la escucha para las conexiones. El puerto por defecto es el 389.

4.2 Ejecución de *slapd* como demonio o servicio independiente

Como norma general, *slapd* se ejecuta de la siguiente manera:

```
# $(ETCDIR)/slapd [<opción>]*
```

donde ETCDIR tiene el valor que le haya asignado en el fichero `Make-common` o en el guión `./configure` durante la configuración previa a la compilación, y <`opción`> es una de las opciones descritas más arriba. A menos que haya especificado un nivel de depuración, *slapd* se desvinculará automáticamente del terminal desde el que lo lanzó, y se ejecutará en segundo plano, en modo demonio o servicio. Cualquiera de las opciones de más arriba pueden darse en la línea de órdenes para hacer que *slapd* cargue un fichero de configuración diferente, o que escuche en otro puerto, etcétera.

Véase el siguiente ejemplo de comienzo de *slapd*:

```
$(ETCDIR)/slapd -f /home/malere/mi_slapd.conf -d 255
```

4.3 Ejecución de slapd desde inetd

En primer lugar, asegúrese de que sea una buena idea ejecutar *slapd* desde `inetd`. Si está usando el *backend* LDBM, entonces no es buena idea. Si está en un entorno de mucho servicio, entonces la sobrecarga que supone ejecutarlo desde `inetd` también lo convierte en una mala idea. Si no es su caso puede seguir adelante con los dos pasos necesarios.

El primer paso es añadir a `/etc/services/` una línea como la siguiente:

```
ldap 389 # ldap directory service
```

El segundo paso es añadir una línea como la siguiente a su fichero `/etc/inetd.conf`:

```
ldap stream tcp nowait nobody $(ETCDIR)/slapd slapd -i
```

donde ETCDIR tiene el valor que le haya asignado en el fichero `Make-common` o en el guión `./configure` durante la configuración previa a la compilación. Finalmente envíele a `inetd` una señal `-HUP` y ya tendrá su configuración. (**N. del T.:** pruebe con `killall -HUP inetd` o mejor todavía `kill -HUP $(pidof inetd)` o `kill -TERM ‘cat $(ETCDIR)/inetd.pid‘`)

5 Creación y mantenimiento de bases de datos

Esta sección le explica cómo crear una base de datos de *slapd* empezando desde cero. Hay dos maneras de crear una base de datos: la primera, puede crear la base de datos en línea, usando LDAP. Con este método, sólo tiene que ejecutar *slapd* y añadir entradas usando el cliente LDAP de su elección. Este método es adecuado para bases de datos relativamente pequeñas (algunos cientos o miles de entradas, dependiendo de los requerimientos).

El segundo método de creación de bases de datos es no hacerlo en línea, sin mediante herramientas de generación de índices. Este es el mejor método si tiene que crear muchos miles de entradas, que si se introdujeran con el método LDAP llevarían un tiempo intolerablemente largo. También es útil si desea asegurarse de que no se accederá a la base de datos durante su creación.

5.1 Creación de una base de datos en línea

El paquete de software *OpenLDAP* viene con una utilidad llamada `ldapadd`, que se utiliza para añadir entradas mientras el servidor LDAP se ejecuta. Si decide crear en línea la base de datos, puede utilizar la herramienta `ldapadd` para añadir las entradas. Tras de añadir las primeras entradas, puede seguir usando posteriormente `ldapadd` para añadir más entradas. Antes de iniciar *slapd*, asegúrese de que activa las siguientes opciones de configuración en su fichero `sladp.conf`:

```
suffix <dn>
```

Tal como se explicó en la 3 (sección 3), esta opción describe qué entradas se mantendrán en esta base de datos. Deberá dar a esta opción el valor del `DN` de la raíz del sub-árbol que va a crear. Por ejemplo:

```
suffix "o=TUDelft, c=NL"
```

Asegúrese de especificar en qué directorio se crearán los archivos de configuración:

```
directory <directorio>
```

Por ejemplo:

```
directory /usr/local/tudelft
```

Tendrá que realizar el siguiente paso para poder conectar con *slapd* como usuario con permisos para añadir entradas. Se lleva a cabo añadiendo las dos siguientes opciones en la definición de la base de datos:

```
rootdn <dn>
```

```
rootpw <contraseña> /* ¡Recuerde usar contraseña «cripto» aquí ! */
```

Estas opciones especifican un `DN` y una contraseña que pueden usarse para autentificarse como la entrada «superusuario» de una base de datos (es decir, la entrada que tiene permisos para realizar cualquier tarea). El `DN` y la contraseña especificados aquí funcionarán siempre, con independencia de que la entrada de `DN` exista realmente o tenga una contraseña válida igual a la especificada. Así se arregla del problema del qué va primero, si el huevo o la gallina, a la hora de autentificarse y añadir entradas antes de que las propias entradas existan siquiera.

Finalmente debe asegurarse de que la definición de base de datos contiene las definiciones de índices que usted desea:

```
index {<attrlist> | default} [pres,eq,approx,sub,none]
```

Para indexar los atributos de clase de objetos (`objectclass`) `cn`, `sn` y `uid` se pueden usar por ejemplo las siguientes líneas de configuración:

```
index cn,sn,uid
```

`index objectclass pres,eq`

`index default none`

Una vez que haya configurado las cuestiones a su gusto, arranque su cliente LDAP y comience a añadir entradas. Por ejemplo, para añadir la entrada `TUDelft` seguida de una entrada `Postmaster` utilizando la herramienta `ldapadd`, puede crear un fichero llamado `/tmp/entradanueva` con el contenido:

```
o=TUDelft, c=NL
objectClass=organization

o=TUDelft
description=Technical University of Delft Netherlands

cn=Postmaster, o=TUDelft, c=NL
objectClass=organizationalRole
cn=Postmaster
description= TUDelft postmaster - postmaster@tudelft.nl
```

y luego utilizar una orden como la siguiente para crear de verdad la entrada:

```
ldapadd -f /tmp/entradanueva -D "cn=Manager, o=TUDelft, c=NL" -w secret
```

Estar orden supone que Usted ha configurado `rootdn` como `"cn=Manager, o=TUDelft, c=NL"` y que la contraseña `rootpw` es «secret». Si no desea escribir la contraseña en la línea de órdenes, utilice la opción `-W` de la orden `ldapadd`, en lugar de `-w "contraseña"`. Se le pedirá que introduzca interactivamente la contraseña:

```
ldapadd -f /tmp/entradanueva -D "cn=Manager, o=TUDelft, c=NL" -W
Enter LDAP Password :
```

5.2 Creación de una base de datos sin estar en línea

El segundo método de creación de una base de datos es hacerlo sin estar en línea, usando las herramientas de generación de índices descritas más abajo. Este es el mejor método si tiene que crear muchos miles de entradas, y crearlas con el método interactivo de LDAP descrito arriba llevaría mucho tiempo. Estas herramientas leen el fichero de configuración de *slapd* y un fichero de entrada LDIF que contiene una representación de las entradas que hay que añadir en formato de texto. Estas herramientas generan los ficheros de índices LDBM directamente. Deberá asegurarse de la activación de varias opciones de configuración importantes, de manera que se encuentren primero en la definición de base de datos del fichero de configuración:

`suffix <dn>`

Tal y como se ha descrito en la sección anterior, esta opción especifica qué entradas se mantendrán mediante esta base de datos. Debe Usted ajustarla al `DN` de la raíz del sub-árbol que intenta crear, por ejemplo:

suffix "o=TUDelft, c=NL"

Asegúrese de especificar un directorio en el que crear los ficheros de índice:

`directory <directorio>`

Por ejemplo:

`directory /usr/local/tudelft`

Después querrá seguramente aumentar el tamaño de la memoria de almacenamiento intermedio (*caché*) interna de la aplicación, y que se utiliza para cada fichero de índice abierto. Para un mejor rendimiento durante la creación del fichero de índices, la situación de rendimiento ideal es aquella en la que el fichero completo se carga en memoria. Si el volumen de sus datos no permite esta operación, o bien si no dispone de mucha memoria, todavía podrá darle un valor alto a este parámetro y dejar que haga su trabajo la paginación a disco del sistema. El tamaño se configura con la opción siguiente:

dbcachesize <númeroentero>

Por ejemplo:

dbcachesize 50000000

Esto creará una memoria de almacenamiento intermedio (*caché*) de un tamaño de 50 MB, que ya es bastante grande (en la Universidad de Michigan la base de datos tiene cerca de 125.000 entradas, y el mayor fichero de índices ocupa aproximadamente 45 MB). Experimente Usted varias veces con este parámetro y con el grado de paralelismo (ver más abajo), con el fin de ver qué combinación funcione mejor en su sistema. Acuérdese de devolver a este número su valor original después de crear los ficheros de índices y antes de ejecutar *slapd*.

Finalmente tendrá que especificar concretamente qué índices desea construir. Esto se consigue con una o más opciones que se aplican a los índices.

`index {<listaatributos> | default} [pres,eq,approx,sub,none]`

Por ejemplo:

`index cn,sn,uid pres,eq,approx`

`index default none`

Esto creará índices de presencia (*presence*), igualdad (*equality*) y aproximación (*approximate*) de los atributos `cn`, `sn` y `uid`, y no creará ningún índice para ningún otro atributo. Para más información acerca de esta opción, véase el fichero de configuración en la 3 (sección 3).

Una vez que haya configurado estos parámetros según sus preferencias, cree los índices ejecutando el programa `ldif2ldbm`:

`ldif2ldbm -i <ficheroentrada> -f <ficheroconfigslapd> [-d <niveldepuración>] [-j <númeroentero>] [-n <numerodebasedatos>] [-e <directorioetc>]`

Los argumentos tienen estos significados:

`-i <ficheroentrada>`

Especifica el fichero de entrada LDIF que contiene en formato de texto las entradas por añadir.

-f <ficheroconfigslapd>

Especifica el fichero de configuración de *slapd* que indica dónde crear los índices, qué índices hay que crear, etc.

`-d <niveldepuración>`

Activa la depuración, según se especifique en <niveldepuración>. Los niveles de depuración son los mismos que para *slapd* (véase la 4.1 (sección 4.1)).

`-j <númeroentero>`

Es un argumento opcional que especifica que, como mínimo la cantidad <númeroentero> de procesos han de iniciarse en paralelo en el momento de construir los índices. El valor por defecto es 1. Si se especifica un valor superior a 1, `ldif2ldbm` creará como mínimo ese número de subprocesos a la hora de construir los índices. Para construir cada índice de atributos se crea un subproceso separado. La ejecución en paralelo de estos procesos puede acelerar grandemente el resultado, pero tenga cuidado de no crear demasiados procesos que compitan todos a la vez por los recursos de disco y memoria.

`-n <númerodebasedatos>`

Es un argumento opcional que especifica la base de datos del fichero de configuración para la cual hay que construir los índices. La primera base de datos aparece listada como «1», la segunda como «2», etc. Se usa por defecto la primera base de datos LDBM que aparezca en el fichero de configuración.

`-e <etcdir>`

Es un argumento opcional que especifica el directorio en donde `ldif2ldbm` podrá hallar las otras herramientas de conversión de bases de datos que precisa para ejecutarse (`ldif2index` y similares). El valor por defecto es el directorio de instalación que se especificó en el guión de instalación. Véase el siguiente ejemplo del uso de la orden `ldif2ldbm`:

```
/usr/local/sbin/ldif2ldbm -i nuevas_entradas -f myslapd.conf
```

5.3 Cuestiones adicionales sobre el formato LDIF

El formato de intercambio de datos de LDAP (*LDAP Data Interchange Format*, LDIF) se usa para representar entradas de LDAP en formato de texto sencillo. La forma básica de una entrada es:

```
[<id>]
dn: <distinguished name>
<tipodeatributo>: <valordel_atributo>
<tipodeatributo>: <valordel_atributo>
...
```

en donde <`id`> el ID opcional de la entrada (un número decimal positivo). No se suele pasar este parámetro, permitiendo que la base de datos lo haga por usted. El programa `ldbmcat`, no obstante, produce un formato LDIF que incluye <`id`> de manera que los nuevos índices que se creen sean consistentes.

Puede continuarse una línea añadiendo un espacio al principio de la siguiente, p. ej.:

```
dn: cn=Barbara J Jensen, o=University of Michi
 gan, c=US
```

Múltiples valores de un atributo se especifican en líneas separadas, por ejemplo:

```
cn: Barbara J Jensen
cn: Babs Jensen
```

Si un <valordel_atributo> contiene un carácter no imprimible, o comienza con un espacio o con dos puntos «:», entonces el <tipodeatributo> va seguido con el signo los dos puntos, dos veces, y el valor se codifica en notación de base 64; por ejemplo, el valor " begins with a space" se codificaría de la manera siguiente:

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

En el mismo fichero LDIF, las entradas múltiples se separan por líneas en blanco. He aquí un ejemplo de un fichero LDIF que contiene tres entradas:

```
dn: cn=Barbara J Jensen, o=University of Michigan, c=US
cn: Barbara J Jensen
cn: Babs Jensen
objectclass: person
sn: Jensen

dn: cn=Bjorn J Jensen, o=University of Michigan, c=US
cn: Bjorn J Jensen
```

```
cn: Bjorn Jensen
objectclass: person
sn: Jensen

dn: cn=Jennifer J Jensen, o=University of Michigan, c=US
cn: Jennifer J Jensen
cn: Jennifer Jensen
objectclass: person
sn: Jensen
jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
...
```

Nótese que el tipo de atributo `jpegPhoto` en la entrada de Jennifer Jensen se codifica usando base64. El programa *ldif* que viene con el paquete *OpenLDAP* puede usarse para producir el formato LDIF.

Nota: en un fichero LDIF, los espacios finales no se eliminan de los valores, ni tampoco se comprimen múltiples espacios internnnos. Si no los quiere en sus datos, no debe incluirlos.

5.4 Las utilidades ldapsearch, ldapdelete y ldapmodify

`ldapsearch` - *ldapsearch* es una interfaz, accesible desde la línea de órdenes, para la llamada a biblioteca *ldap_search(3)*. Use esta utilidad para buscar entradas en el dorsal (*backend*) de nuestra base de datos LDAP.

La sinopsis de las opciones de *ldapsearch* es la siguiente (véase la página de manual de `ldapsearch(1)` para conocer el significado de cada opción):

```
ldapsearch  [-n]  [-u]  [-v]
[-k]  [-K]  [-t]  [-A]
[-B] [-L] [-R]
[-d niveldepuración] [-F separador]
[-f fichero] [-D dn_deacceso]  [-W]
[-w contraseña_acceso]  [-h servidorldap]
[-p puertoldap]   [-b basebúsqueda]
[-s base|one|sub]
[-a never|always|search|find]
[-l límitetiempo] [-z límitetamaño] filtro
[atributos...]
```

`ldapsearch` abre una conexión a un servidor LDAP, se «engancha» a él y lleva a cabo una búsqueda utilizando el filtro `filtro`. Este filtro debe ajustarse a la representación de cadenas de texto para filtros LDAP, tal y como se definen en el Request for Comments 1558 (RFC 1558). Si *ldapsearch* encuentra una o más entradas, se obtienen los atributos especificados en `atributos` y se imprimen por salida estándar las entradas y sus valores. Si no se listan atributos, se devuelven todos los atributos.

He aquí algunos ejemplos del uso de *ldapsearch*:

```
ldapsearch -b 'o=TUDelft,c=NL' 'objectclass=*'

ldapsearch -b 'o=TUDelft,c=NL' 'cn=Rene van Leuken'

ldasearch -u -b 'o=TUDelft,c=NL' 'cn=Luiz Malere' sn mail
```

La opción `-b` representa la base de búsqueda (el punto inicial de la búsqueda) y la opción `-u` representa la opción «amigable para el usuario», refiriéndose a la información de salida.

`ldapdelete` - *ldapdelete* es una interfaz, accesible desde la línea de órdenes, para la llamada a biblioteca *ldap_delete(3)*. Use esta utilidad para buscar entradas en el dorsal (*backend*) de nuestra base de datos LDAP.

La sinopsis de las opciones de *ldapdelete* es la siguiente (véase la página de manual de `ldapdelete(1)` para conocer el significado de cada opción):

```
ldapdelete   [-n]   [-v]  [-k]
[-K]  [-c]  [-d nivel_depuración]
[-f fichero]  [-D dn_de_enganche]  [-W]
[-w contraseña]  [-h servidorldap]
[-p puertoldap] [dn]...
```

ldapdelete abre una conexión con un servidor LDAP, se «engancha» a él, y borra una o más entradas. Si se proporcionan uno o más argumentos de `dn`, se borrarán las entradas con estos `Distinguished Names`. Cada `dn` debe se la representación mediante una cadena de un `DN` de la forma especificada en el RFC 1779. Si no se proporcionan argumentos de `dn`, entonces se leerá la lista de `DNs` desde la entrada estándar (o bien desde un fichero si se utiliza la opción `-f`).

He aquí algunos ejemplos del uso de *ldapdelete*:

```
ldapdelete 'cn=Luiz Malere,o=TUDelft,c=NL'

ldapdelete -v 'cn=Rene van Leuken,o=TUDelft,c=NL' -D 'cn=Luiz Malere,o=TUDelft,c=NL' -W
```

La opción `-v` representa el modo verboso. La opción `-D` representa el DN de enganche (*Binddn*) y la opción `-W` sirve para que se nos pregunte interactivamente por la contraseña.

`ldapmodify` - *ldapmodify* es una interfaz, accesible desde la línea de órdenes, para la llamada a biblioteca *ldap_modify(3)* y *ldap_add(3)*. Use esta utilidad para modificar entradas en el dorsal (*backend*) de nuestra base de datos LDAP.

La sinopsis de las opciones de *ldapmodify* es la siguiente (véase la página de manual de `ldapmodify(1)` para conocer el significado de cada opción):

```
ldapmodify   [-a]  [-b]  [-c]
[-r]  [-n]  [-v]  [-k]
[-d nivelde_depuración]  [-D dn_de_enganche]
[-W]  [-w contraseña]  [-h servidorldap]
[-p puertoldap] [-f fichero]

ldapadd [-b] [-c] [-r] [-n]
[-v]  [-k]  [-K]
[-d nivelde_depuración]  [-D dn_de_enganche]
[-w contraseña]  [-h servidorldap]
[-p puertoldap] [-f fichero]
```

ldapadd está implementado en forma de enlace no simbólico (*hard link*) a la utilidad *ldapmodify*. Cuando se llama a la utilidad en la forma `ldapadd`, la opción `-a` (añadir nueva entrada) se activa automáticamente.

ldapmodify abre una conexión con un servidor LDAP, se «engancha» a él, y modifica o añade entradas. La información sobre la entrada que hay que modificar se lee desde la entrada estándar o desde un fichero a través de la opción `-f`.

He aquí algunos ejemplos del uso de ldapmodify:

Suponiendo que el fichero `/tmp/entrymods` exista y tenga un contenido:

```
dn: cn=Modify Me, o=University of Michigan, c=US
changetype: modify
replace: mail
mail: modme@terminator.rs.itd.umich.edu
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto: /tmp/modme.jpeg
-
delete: description
-
```

La orden:

```
ldapmodify -b -r -f /tmp/modif_entrada
```

sustituirá el contenido del atributo `mail` de la entrada `"Modify Me"` con el valor `"modme@terminator.rs.itd.umich.edu"`, le añadirá el título de `"Grand Poobah"`, el contenido del fichero */tmp/modme.jpeg* como `jpegPhoto`, y eliminará completamente el atributo `description`.

Pueden llevarse a cabo las mismas modificaciones usando el formato de introducción más antiguo de *ldapmodify*:

```
cn=Modify Me, o=University of Michigan, c=US
mail=modme@terminator.rs.itd.umich.edu
+title=Grand Poobah
+jpegPhoto=/tmp/modme.jpeg
-description
```

Esto más la orden siguiente:

```
ldapmodify -b -r -f /tmp/modif_entrada
```

Eso suponiendo que el fichero /tmp/newentry exista y tenga el siguiente contenido:

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US
objectClass: person
cn: Barbara Jensen
cn: Babs Jensen
sn: Jensen
title: the world's most famous manager
mail: bjensen@terminator.rs.itd.umich.edu
uid: bjensen
```

La orden:

```
ldapadd -f /tmp/modif_entrada
```

Suponiendo que el fichero /tmp/modif_entrada exista y tenga el contenido:

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US
changetype: delete
```

La orden:

```
ldapmodify -f /tmp/modif_entrada
```

eliminará la entrada de Babs Jensen.

La opción -f representa «fichero» (leer las modificaciones desde un fichero en vez de hacerlo desde la entrada estándar). La opción -b representa a «binario», es decir, cualquier tipo de valores que empiecen por '/' en el fichero de entrada se interpretan como binarios, y la -r representa «reemplazar» (sustituir los valores existentes de forma predeterminada).

6 Más información y características adicionales

En esta sección hallará información sobre el Libro de Direcciones de Netscape, un cliente LDAP que puede utilizar para consultar su Directorio; también presentamos los detalles sobre cómo implementar acceso móvil o itinerante (*roaming access*) utilizando el Netscape Navigator en sus versiones 4.5 y superiores más su servidor LDAP. Se ha vertido mucha tinta electrónica en las listas de correo de *OpenLDAP* sobre el acceso itinerante, pues se trata de una característica todavía no implementada totalmente. A muchas personas no les agrada la forma en que Netscape Navigator interactúa con el servidor LDAP a la hora de realizar grabaciones y recuperaciones de datos. Así pues, si tras la lectura de estas líneas tiene la impresión de que el acceso itinerante no funciona de la forma que usted desearía, no se preocupe; muchas personas tienen la misma impresión que usted. La finalidad de la introducción de esta característica ha sido principalmente dar a la gente una idea de las posibilidades del protocolo LDAP, más que otras consideraciones. Para terminar, verá algunas informaciones sobre cómo matar con seguridad el proceso *slapd* y sobre los ficheros de registro (logs) de *slapd*.

6.1 Acceso itinerante (perfiles móviles)

El objetivo del acceso itinerante (llamado en Netscape «perfiles móviles») es que, desde cualquier lugar de la Red donde se encuentre, pueda obtener localmente sus marcadores de URL's, preferencias que personalizan la aplicación, filtros de correo, etcétera, mediante la utilización de un Navegador Netscape y un servidor LDAP.

Se trata de una característica muy conveniente. Imagine que desde cualquier lugar al que pueda acceder a la Web, pueda tener sus propias preferencias en el navegador. Si va a viajar y precisa acceder a ese sitio de cambio de divisas que tiene almacenado en sus marcadores personales (*bookmarks*), no se inquiete; simplemente cargue sus marcadores y otros ficheros de configuración en un servidor LDAP y podrá recuperarlos todos después con independencia del lugar en el que se encuentre.

Para implementar acceso itinerante (en inglés *roaming access*) ha de seguir los pasos que se detallan a continuación:

- Cambiar su fichero de descripción de atributos
- Cambiar su fichero de descripción de clases de objetos (`objectclass`).
- Cambiar el fichero LDIF para que incluya perfiles
- Configurar el Netscape Navigator para que utilice el servidor LDAP como el servidor de acceso itinerante.

- Reiniciar el servidor LDAP con la nueva configuración.

- Cambiar el fichero de atributos Es preciso que añada nuevos atributos a la lista existente en el fichero `slapd.at.conf`; es este el fichero que se incluye en su `slapd.conf` y que normalmente se localiza en /usr/local/etc/openldap (**N. del T.:** si ha instalado su distribución OpenLDAP a partir de un fichero `.deb` o de un `.rpm`, el lugar más probable será `/etc/openldap/`) :

```
attribute       nsLIPtrURL            ces
attribute       nsLIPrefs             ces
attribute       nsLIProfileName       cis
attribute       nsLIData              bin
attribute       nsLIElementType       cis
attribute       nsLIServerType        cis
attribute       nsLIVersion           cis
```

- Cambiar el fichero `objectclass`: Debe añadir algunas clases nuevas a su fichero `lapd.oc.conf` (es otro fichero que se incluye en su `slapd.conf` y que se localiza normalmente en `/usr/local/etc/openldap`, para habilitar el acceso itinerante (**N. del T.:** si ha instalado su distribución OpenLDAP a partir de un fichero `.deb` o de un `.rpm`, el lugar más probable será `/etc/openldap/`):

```
objectclass nsLIPtr
requires
        objectclass
allows
        nsliptrurl,
        owner

objectclass nsLIProfile
requires
        objectclass,
        nsliprofilename
allows
        nsliprefs,
        uid,
        owner

objectclass nsLIProfileElement
requires
        objectclass,
        nslielementtype
allows
        owner,
        nslidata,
        nsliversion

objectclass nsLIServer
requires
        objectclass,
        serverhostname
allows
        description,
        cn,
        nsserverport,
        nsliservertype,
        serverroot
```

- Cambiar el fichero LDIF: Ahora ha de modificar el fichero LDIF, añadiéndole entradas de perfiles relativas a cada usuario que desee probar la característica de perfiles móviles del Netscape. Obsérvese un ejemplo de un fichero LDIF sencillo con entradas de perfiles:

```
dn: o=myOrg,c=NL
o: myOrg
objectclass: organization

dn: cn=seallers,ou=People,o=myOrg,c=NL
cn: seallers
userpassword: MiClaVE
objectclass: top
objectclass: person

dn: nsLIProfileName=seallers,ou=Roaming,o=myOrg,c=NL
changetype: add
objectclass: top
owner: cn=seallers,ou=People,o=myOrg,c=NL
objectclass: top
objectclass: nsLIProfile
```

El paso siguiente es configurar Netscape para que habilite los perfiles móviles basados en su servidor LDAP. Sólo tiene que seguir la secuencia:

- Vaya al menú Edit -> Preferences -> Roaming User

Ahora tiene que activar el perfil móvil (*Roaming Access*) para este perfil, haciendo click sobre la casilla de verificación correspondiente a esta opción.

- Rellene la caja del nombre de usuario (*username*) con el contenido apropiado, por ejemplo john

Despliegue la flecha de la opción de Roaming User en la parte izquierda de la ventana de preferencias, para poder ver las opciones detalladas del acceso itinerante (perfiles móviles).

- Haga click sobre Server Information, habilite la opción LDAP Server y rellene las cajas de diálogo con la siguiente información:

Address: ldap://myHost/nsLIProfileName=$USERID,ou=Roaming,o=myOrg,c=NL

User DN: cn=$USERID,ou=People,o=myOrg,c=NL

IMPORTANTE: Netscape sustituye automáticamente la variable $USERID por el nombre del perfil que haya seleccionado al arrancar el navegador. De manera que si ha elegido el perfil **sanchez**, sustituirá $USERID por sanchez, y si ha seleccionado el prefil **gonzalez**, sustituirá $USERID por gonzalez. Si no está familiarizado con los perfiles, ejecute la aplicación *Profile Manager* que se incluye en el paquete del Netscape Communicator (**N. del T.:** a partir de la versión 6.0, Netscape ha dejado otra vez de llamarse Communicator). El *Profile Manager* es una aplicación diseñada para satisfacer a múltiples usuarios de un navegador en una misma máquina, de manera que cada uno de ellos pueda tener sus propia configuración en el navegador.

El último paso consiste en reiniciar el servidor; examine la 6.3 (sección 6.3) para ver la manera de hacerlo con seguridad, y la 4 (section 4) para ver cómo reiniciarlo.

6.2 Libreta de direcciones de Netscape (Address Book)

Una vez que tenga su servidor LDAP configurado y en marcha, puede acceder a él a través de clientes muy diferentes (por ejemplo la utilidad de línea de órdenes *ldapsearch*). Un cliente muy interesante es la Libreta de direcciones de Netscape (Address Book). Está disponible a partir de la versión 4.x de Netscape pero, para interactuar de manera estable con su servidor LDAP, tendrá que usar la versión 4.5 o superiores (**N. del T.:** ya está disponible el Netscape 6.0).

Sólo tiene que seguir la secuencia:

Abra Netscape Navigator -> Vaya al ménu Communicator -> Address Book

La libreta de direcciones (Address Book) de Netscape arrancará con algunos directorios LDAP predeterminados. Ha de añadir también su propio directorio LDAP, evidentemente.

Vaya al menú File -> New Directory

Complete los cuadros de diálogo con la información de su servidor, por ejemplo:

- Description : TUDelft

- LDAP Server : dutedin.et.tudelft.nl

- Server Root : o=TUDelft, c=NL

El puerto por defecto para LDAP es 389; no debe cambiarlo, a menos que cambiara esta opción al compilar su servidor.

Realice ahora consultas sencillas a su servidor, unsando el cuadro de diálogo Show Names Containing, o consultas avanzadas, usando el botón Search for.

6.3 Matar al servidor LDAP

Para matar con seguridad al servidor *slapd*, debe utilizar una línea de órdenes como la siguiente:

```
kill -TERM ‘cat $(ETCDIR)/slapd.pid‘
```

(**N. del T.:** en RedHat y distribuciones basadas en rh, como Mandrake y Esware, valdrá simplemente con `/etc/rc.d/init.d/opeldap stop`, mientras que en Debian y distribuciones basadas en Debian (Corel, Storm, Citius) bastará con un `/etc/init.d/openldap stop`. En otras distribuciones el procedimiento es similar, buscando tal vez `slapd` en vez de `openldap`).

Matar *slapd* de una manera más drástica puede provocar corrupción de las bases de datos, pues puede ser preciso vaciar ciertos tampones de almacenamiento intermedio antes de salir del servidor. Nótese que *slapd* escribe su PID en un fichero llamado `slapd.pid` en el directorio que haya configurado en el fichero `slapd.conf`, por ejemplo en `/var/pid/slapd.pid` (**N. del T.:** es éste precisamente el caso de Debian).

Puede cambiar la localización de este fichero PID cambiando la variable SLAPD_PIDFILE en `include/ldapconfig.h.edit`.

slapd escribirá también sus argumentos en un fichero llamado `slapd.args` en el directorio que haya configurado en el fichero `slapd.conf` por ejemplo en `/usr/local/var/slapd.args`

Podrá cambiar la ubicación del fichero `slapd.args` si cambia la variable SLAPD_ARGSFILE en `include/ldapconfig.h.edit`.

6.4 Ficheros de registro (logs)

slapd utiliza el recurso `syslog(8)` para generar registros de sus actividad. El usuario predeterminado del recurso `the syslog(8)` es LOCAL4, pero se permiten valores que van de LOCAL0, LOCAL1, hasta LOCAL7.

Para habilitar la característica de generación de archivos de registro (logs), debe editar el fichero `syslog.conf`, situado generalmente en el directorio `/etc`.

Cree una línea como la siguiente:

local4.*   /usr/adm/ldalog

Esto hará que se utilice el usuario predeterminado LOCAL4 para el recurso *syslog*. Si no está familiarizado con la sintaxis de esta línea, examine las páginas de manual de `syslog`, `syslog.conf(5)` y `syslogd(8)` para el recurso de syslog. Si desea cambiar el usuario predeterminado o especificar el nivel de detalle de los registros generados (logs), tiene disponibles las siguientes opciones en el momento de arrancar *slapd*:

-s nivel-de-syslog Esta opción le dice a *slapd* en qué nivel de detalle deben registrarse las informaciones sobre depuración en el recurso `syslog(8)`. El nivel especifica la gravedad del mensaje, y representa una palabra clave tomada de la siguiente lista ordenada (de mayor a menor gravedad): emerg, alert, crit, err, warning, notice, info, y debug. Ejemplo: `slapd -f myslapd.conf -s debug`

-l usuario-local-de-syslog Selecciona el usuario local del recurso syslog(8). Los valores pueden ir desde LOCAL0, LOCAL1, y así hasta LOCAL7. El valor predeterminado es LOCAL4. No obstante, esta opción se permite únicamente en sistemas que soportan usuarios locales en el recurso syslog(8).

Eche un vistazo en este momento a los registros generados (logs); pueden ayudarle a resolver problemas con consultas, actualizaciones, enganches (bindings), etc.

7 Referencias

7.1 Vínculos (URLs)

Se ofrecen aquí URLs que contienen información muy útil acerca de LDAP. Se ha redactado este *Cómo* a partir de estas URLs, así que si necesita información mas específica tras la lectura de este documento, es probable que la encuentre aquí:

- Página del LDAP de la Universidad de Michigan: *http://www.umich.edu/~dirsvcs/ldap/index.html* `<http://www.umich.edu/dirsvcs/ldap/index.html>`
- Página de documentación del LDAP de la Universidad de Michigan: *http://www.umich.edu/~dirsvcs/ldap/doc/* `<http://www.umich.edu/dirsvcs/ldap/doc/>`
- Implementar manualmente el acceso itinerante (perfiles móviles) *http://help.netscape.com/products/client/communicator/manual_roaming2.html* `<http://help.netscape.com/products/client/communicator/manual_roaming2.html>`
- Personalizar las opciones de LDAP para Communicator 4.5: *http://developer.netscape.com/docs/manuals/communicator* `<http://developer.netscape.com/docs/manuals/communicator/ldap45.htm>`
- Linux Directory Service (Servicio de Directorio en Linux) *http://www.rage.net/ldap/* `<http://www.rage.net/ldap/>`

7.2 Libros

He aquí los libros más populares acerca de LDAP:

- *LDAP: Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*, por Howes and Smith
- *Understanding and Deploying LDAP Directory Servers*, por Howes, Smith, and Good

7.3 RFCs

He aquí los RFC que se refieren a la cuestión de LDAP. (**N. del T.:** si desea estar actualizado en los RFC de LDAP, teclee en Debian (v 2.2. y siguientes) : `apt-get install ldap-rfc`)

- RFC 1558: A String Representation of LDAP Search Filters («Representación en cadenas de los filtros de búsqueda de LDAP»)
- RFC 1777: Lightweight Directory Access Protocol («Protocolo ligero de acceso a directorios»)
- RFC 1778: The String Representation of Standard Attribute Syntaxes («Representación en cadenas de las sintaxis estándar de los atributos»)
- RFC 1779: A String Representation of Distinguished Names («Representación en cadenas de los nombres distintivos»)
- RFC 1781: Using the OSI Directory to Achieve User Friendly Naming («Utilización del directorio OSI para obtener denominaciones amigables para el usuario»)
- RFC 1798: Connectionless LDAP («LDAP sin conexión»)
- RFC 1823: The LDAP Application Programming Interface («La interfaz de programación de aplicaciones LDAP»)
- RFC 1959: An LDAP URL Format («Formato de URLs para LDAP»)
- RFC 1960: A String Representation of LDAP Search Filters («Representación en cadenas de los filtros de búsqueda de LDAP»)
- RFC 2251: Lightweight Directory Access Protocol (v3) («Protocolo ligero de acceso a directorios, versión 3»)
- RFC 2307: LDAP as a Network Information Service («LDAP como servicio de información en redes»)