UNIVERSIDAD DEL AZUAY

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

"*Servidor de directorios LDAP (Lightweight Directory Access Protocol)*"

Trabajo de graduación previo a la obtención del título de "Ingeniero de Sistemas"

Autor: José Alfredo Llerena

Director: Ing. Pablo Esquivel

Cuenca, Ecuador

2007

Dedicatoria

Dedico este estudio a mis padres y a toda mi familia que durante toda mi vida me han apoyado incondicionalmente en mis estudios.

JOSE

FIRMAS DE RESPONSABILIDAD

Los criterios vertidos en esta monografía son de responsabilidad de su autor.

Jose Llerena

AGRADECIMIENTO

A Dios, por que es el quien da la fuerza, sabiduría, seguridad y firmeza para realizar con éxito el presente trabajo de graduación.

Un sincero agradecimiento a la “Universidad del Azuay” y a sus profesores que, con su enseñanza, han podido contribuir en la formación académica y personal en todos los días de vida estudiantil.

Un gran agradecimiento a todas las personas que siempre me han dado ánimos para salir adelante y que siempre han confiado en mi.

INDICE DE CONTENIDOS

INDICE DE ILUSTRACIONES Y CUADROS

INDICE DE ANEXOS

RESUMEN

El presente proyecto pretende dar a conocer en que consiste y como funciona un servidor de directorios (LDAP).

Dentro de este marco se verá como crear una estructura de directorio, base de datos y su configuración. La parte práctica consistirá en la aplicación de la parte teórica en un ejemplo de funcionamiento utilizando para el efecto dos computadoras para de esta forma poder ver el proceso de autentificación.

Al final del proyecto se obtendrá una visión de en que se puede aplicar LDAP así como las recomendaciones necesarias para su implementación.

ABSTRACT

The current project pretends to let it know what a directory server is and how the directory server (LDAP) works.

Inside of this frame it will be shown how to create a directory structure, a database and its configuration. The practice will consist in the application of the theory part in a working example using for the purpose two computers to expose the authentication process.

At the end of the project a vision of how LDAP can be applied will be gotten, so the necessary recommendations for its implementation.

INTRODUCCION

Este trabajo es una aplicación de los conocimientos adquiridos durante nuestros estudios en el área del sistema operativo Linux, el mismo que tiene muchas importancia dentro del desarrollo profesional. Mediante este podemos aportar soluciones para el manejo de directorios.

Linux es la denominación de un sistema operativo tipo Unix y el nombre de un núcleo. Es uno de los paradigmas más prominentes del software libre y del desarrollo del código abierto, cuyo código fuente está disponible públicamente, para que cualquier persona pueda libremente usarlo, estudiarlo, redistribuirlo y, con los conocimientos informáticos adecuados, modificarlo.

Linux es usado como sistema operativo en una amplia variedad de plataformas de hardware y computadores.

La marca *Linux* pertenece a Linus Torvalds y se define como "un sistema operativo para computadoras que facilita su uso y operación".

Un servicio de directorio se basa en contener la información de una manera descriptiva y basada en atributos; esta información es trabajada mucho mas en tareas de lectura mas no bien en lo referente a escritura de datos, por eso un servicio de directorios no tiene alguna relación directa con una base de datos o con ciertas operaciones que estas tienen como los manejos de esquemas y las operaciones de rollback.

Es muy importante dentro de un ambiente de red el mantener la información importante estructurada y rápidamente disponible. El caos en los datos afecta tanto en tiempo como en dinero, por eso se ha creado los servicios de directorios para que esto no ocurra y se lo evite.

Ante la necesidad de manejar datos de una manera rápida y eficiente se prevé utilizar el servidor de directorios con el que se cuenta el cual es LDAP con el que se hará las operaciones diversas que se pueden hacer en la misma.

CAPITULO 1: TEORIAS DE LDAP

Introducción

Antes de realizar la instalación, configuración y pruebas del servidor de directorios, se considera necesario dar conocer algunos conceptos referentes al mismo y conocer aspectos importantes como su concepto, manera de funcionar, sus atributos, objetos, directivas y librerías. Con esto se tendrá la base necesaria para poder realizar la instalación, configuración y pruebas del servidor LDAP.

Debido a la importancia de tener la información importante estructurada y rápidamente disponible en un ambiente de red es necesario saber lo relacionado al servidor LDAP.

1.1 Introducción conceptual de LDAP.

LDAP es un servicio de directorios. Un servidor de directorios es una base de datos no relacional especializada que esta optimizada para leer, consultar y buscar datos. Los directorios tienen por lo general información descriptiva y basada en atributos, se lee mucho más de lo que se escribe; también tienen la capacidad de soporte de filtrado el cual es sofisticado.

Los directorios generalmente no tienen soporte para las transacciones complejas, por ejemplo los esquemas de *roll-back* que se los encuentran en los sistemas de administración de bases de datos. Los directorios son especializados para dar una rápida respuesta ante búsquedas o consultas; deben tener la habilidad para replicar información ampliamente en orden de incrementar disponibilidad y fiabilidad mientras se trata de reducir el tiempo de respuesta. Cuando la información del directorio es duplicada, las inconsistencias temporales entre las replicas puede tolerarse, siempre y cuando a la final exista sincronismo.

Las actualizaciones en un directorio son usualmente cambios sencillos ya sea de todo o parte del directorio.

Existen diferentes modos de proveer un servicio de directorio. Con métodos diferentes se puede permitir diversos tipos de información a ser almacenada en el directorio, establecer diferentes requerimientos de cómo esa información puede ser referenciada, consultada y actualizada; como debe ser protegida de accesos no autorizados. Algunos servicios de directorios son locales, dando servicios dentro de un contexto restringido (una simple PC). Otros servicios son globales dando servicio a un contexto mucho más amplio (la Internet). Los servicios globales son usualmente distribuidos; es decir, que los datos son regados entre varias maquinas, de las cuales todas cooperan para proveer el servicio de directorio.

Por lo tanto LDAP (Lightweight Directory Access Protocol), en español Protocolo Ligero de Acceso a Directorios es como su nombre lo dice es un protocolo ligero que permite acceder a servicios de directorios, sobre todo a los servicios de directorios basados en X. 500. LDAP funciona sobre TCP/IP u otra conexión orientada a servicios de transferencia.

LDAP no esta restringida a solamente redes tipo UNIX, sino también tiene soporte con Windows servers (desde el 2000 en adelante). Igualmente *Novell* ofrece el servicio LDAP.

LDAP en principio puede ser aplicado a cualquier estructura de datos que debe ser centralmente administrada. Algunos ejemplos de aplicaciones son:
- Empleado como un reemplazo para el servicio NIS (*Network information service*), en español servicio de información de red.
- Mail routing (postfix, sendmail).
- Libreta de direcciones para clientes de correo como *Mozilla*, *Evolutio*n y *Outlook.*
- Administración de descripciones de zonas para un nombre de servidor BIND (Berkeley Internet name domain) en español nombre de dominio de Internet Berkeley.

Ventajas de LDAP

Un directorio LDAP tiene ciertas ventajas sobre los demás tipos de bases de datos por los motivos siguientes:

- Es bastante rápido en la lectura de los registros.

- Permite replicar al servidor de una manera bastante sencilla y económica

- Muchas aplicaciones de diverso tipo tienen interfaces de conexión con LDAP y pueden ser integradas fácilmente

- Dispone de un modelo de nombres globales que permite que todas las entradas sean únicas

- Usa un sistema jerárquico de almacenamiento de información.

- Permite múltiples directorios independientes

- Funciona sobre TCP/IP y SSL

- La mayoría de aplicaciones disponen de soporte para LDAP

- La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

Características del servidor LDAP.

- Operaciones de lectura muy rápidas._ Debido a los tipos de datos que se guardan en los directorios las lecturas son mucho más comunes que las escrituras.

- Datos relativamente estáticos._ Los datos que se almacenan en los directorios no saben ser actualizados con mucha frecuencia.

- Entorno distribuido._ fácil replicación

- Estructura jerárquica._ Al igual que dentro de sus ventajas los directorios almacenan la información jerárquicamente, de forma nativa.

- Orientado a objetos._ El directorio representa a elementos, atributos y a objetos. Los objetos son creados como entradas, que representan a una colección de atributos.

- Esquema Standard._ Los directorios utilizan un sistema estándar que pueden usar fácilmente diferentes tipos de aplicaciones.

- Atributos multi-valor._ Los atributos pueden almacenar valores únicos o varios.

- Replicación multi-master._ Muchos de los servidores LDAP permiten realizar escrituras o actualizaciones en múltiples servidores.

Luego de revisar las características de LDAP se puede decir que sus usos más comunes son:

- **Directorios de información._** Por decir bases de datos de trabajadores y que se organice por departamentos o en base a las páginas amarillas.

- **Sistemas de correo electrónico**. Grandes sistemas de correo compuestos por más de un servidor que accedan a un depósito de datos en común. Por ejemplo un usuario hace un login con su email, para este usuario sus atributos serian la contraseña, el almacenamiento permitido, la ruta donde se guardan los correos, y cualquier otro tipo de atributo, así este directorio hará operaciones de lectura y las operaciones de escritura serán muy bajo.

- **Sistemas de alojamiento de páginas web y FTP**, con el depósito de datos de usuario compartido.

- **Sistemas de autenticación o autorización centralizada._** Grandes sistemas en donde se guarda una cantidad grande de registros y que requiera un uso constante de los mismos. Por ejemplo sistemas de autenticación para las páginas Web, o el control de acceso a usuarios a una red. En este caso el usuario tiene su username, los atributos serian la contraseña, permisos y al grupo que pertenece; así el directorio recibirá una consulta cuando el usuario se conecte y otra cuando el usuario acceda a los recursos de la red, el relación a esta gran cantidad de consultas, pocas veces se hará una operación de escritura como por ejemplo cambio de contraseña.

- Servidores de certificados públicos y llaves de seguridad.

- Autenticación única para la personalización de aplicaciones.

- Perfiles de usuarios centralizados.

1.2 Como funciona LDAP

LDAP se basa en un modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol del directorio que se vera un poco mas adelante. El cliente LDAP se conecta con el servidor LDAP y realiza una consulta. El servidor contesta con la respuesta respectiva, o bien puede ser 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 aparece a un servidor LDAP hace referencia a la misma entrada a la que se hace referencia en otro servidor LDAP. Es esto un punto importante de un servicio de directorios universal como lo es LDAP.

1.3 Atributos y objetos de LDAP

LDAP permite controlar que atributos son requeridos y permitidos en una entrada a través del uso de un atributo especial llamado *objectclass*. Los objetos de este atributo determinan las reglas del esquema sobre la cual la entrada debe obedecer.

La información es referenciada por su nombre distinguido, el cual es construido tomando el nombre de la entrada propia (RDN) y concatenando los nombres de sus entradas ancestros. Basándonos en la figura 2 la entrada para Juana Mills tiene un nombre distinguido relativo de cn = Juana Mills, ou = contabilidad, o = Guapan, pr (en realidad st) = Azuay, c = Ecuador.

LDAP define las operaciones interrogando y actualizando el directorio. Las operaciones son provistas por añadir y eliminar una entrada del directorio, cambiando una entrada existente, y cambiando el nombre de una entrada. LDAP es usado mayoritariamente para buscar información en el directorio, la operación de búsqueda permite que se pueda buscar en una porción del directorio para las entradas que coincidan con los criterios de búsqueda especificados por el filtrador de búsqueda. Entonces puede ser requerida por cada entrada que coincida con el criterio.

Por ejemplo, si se desea buscar el subárbol de directorio entero en y debajo de o = Guapan las personas con el nombre de Juana Mills, se obtiene la dirección de correo para cada entrada encontrada, LDAP da facilidad para hacer esto.

La determinación global de que tipos de objetos deberían ser grabados en la información de un directorio se lo hace siguiendo un esquema. El tipo de un objeto es determinado por la clase del objeto, la cual determina a que atributos el objeto en cuestión tiene o puede ser asignado. Un esquema, por lo tanto, debe contener las definiciones de todas las clases objetos y atributos usados en la aplicación deseada.

Hay algunos esquemas comunes, pero es posible personalizar esquemas o usar múltiples esquemas complementando unos con otros, siempre que sea requerido por el ambiente en el cual el servidor LDAP opera.

En el siguiente grafico se ve una pequeña revisión de las clases objetos de los esquemas *core.shema* e *inetorgperson.schema* usados en la figura 1, incluyendo atributos requeridos y valores de atributos validos.

Clases objeto	Significado	Ejemplo de entrada	Atributos
dcObject	domainComponent Componente nombre del dominio	UDA	dc
organizational unit	organizationalUnit unidad organizacional	doc	ou
inetOrgPerson	inetOrgPerson (datos de relación persona para intranet o internet)	Jorge Smith	sn y cn

Tabla 1.1: Objetos y atributos usados comúnmente

Algunos servicios de directorio no proveen un mecanismo de protección, lo cual permite que cualquier persona vea la información. LDAP ofrece un mecanismo para un cliente para autenticarse, probar su identidad a un servidor de directorios, abriendo el camino para un rico control de acceso para proteger la información que el servidor contiene. Igualmente tiene el soporte de seguridad de datos, o sea servicios de integridad y confidencialidad.

El archivo principal para configurar el servidor LDAP es *slapd.conf* que se encuentra en la ruta */etc/openldap/slapd.conf* para tener este archivo es necesario instalar el paquete necesario dentro de la instalación de LINUX.

Para importar y exportar información de los directorios entre los distintos servidores de directorios basados en LDAP, o para describir una serie de cambios que se aplican

al directorio, se toma en cuenta el archivo de formato conocido como LDIF (son las siglas de *"LDAP interchange format")* en español formato de intercambio de LDAP. Un archivo LDIF almacena información en jerarquías de entradas orientadas a objeto.

Un archivo LDIF común tiene en su contenido lo siguiente:

dn: o=UDA, c=ES
o: UDA
objectclass: persona
dn: cn=José Llerena, o=UDA, dc=ES
cn: José Llerena
sn: Llerena
mail: jose_llerena@yahoo.com
objectclass: persona

Como se ha visto, cada entrada está identificada por un nombre distintivo (*distinguished name*). El nombre distintivo está compuesto por el nombre de la entrada, la ruta de los nombres que permiten seguir la entrada hacia atrás hasta la parte superior de la jerarquía del directorio.

En LDAP, una clase objeto define la colección de atributos que pueden usarse para definir una entrada. El estándar LDAP proporciona estos tipos básicos para las clases 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 objeto, la entrada para personas se define por medio de una clase objeto “persona”, pero también puede definirse mediante atributos en las clases objetos inetOrgPerson, groupOfNames y

organization. La estructura de las clases objetos del servidor determina la lista total de atributos requeridos y que se permiten para una entrada dada.

Los datos del directorio se representan mediante pares de atributo y su valor. Cualquier parte de la 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 con el nombre José Llerena mediante cn: José Llerena.

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

nombre: José
apellido: Llerena
correo: jose_llerena@josellerena.com

Los atributos requeridos son los que deben estar en las entradas que utilicen la clase objeto. Todas las entradas necesitan el atributo objectClass, que muestra las clases objeto a las que pertenece una entrada.

Los atributos permitidos son aquellos que pueden estar presentes en las entradas que utilicen la clase objeto. Por ejemplo, en la clase objeto person, se requieren de los atributos cn y sn. Los atributos description (descripción), telephoneNumber (número de teléfono), seeAlso (vea 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

- cis cadena con mayúsculas y minúsculas ignoradas

- tel cadena de número de teléfono (como cis, pero en las comparaciones se ignoran los espacios en blanco y los guiones).

- dn "distinguished name" (nombre distintivo)

Dentro de la línea de comandos los atributos se utilizan de la siguiente manera; attribute <nombre> [<nombre2>] { bin | ces | cis | tel | dn }

Esta opción asocia una sintaxis con un nombre de atributo. Por defecto un atributo tiene sintaxis cis. Se puede proporcionar a un atributo un nombre alternativo que es opcional.

Tipos de Atributos

Los tipos de atributos en el directorio forman un árbol de clases. Por ejemplo, el tipo de atributo "commonName" es una subclase del tipo de atributo "name".

Hay atributos obligatorios y opcionales como se indica en la siguiente figura:

Identificador de Atributo	**Descripción del Valor de Atributo**
NUMERICOID (obligatorio)	Identificador de Objeto Único (OID)
NAME	Nombre del Atributo
DESC	Descripción del Atributo
OBSOLETE	"true" si es obsoleto; "false" o ausente si no lo es
SUP	Nombre del tipo de atributo superior del que se deriva el tipo de atributo
EQUALITY	Nombre de la regla de correspondencia si la igualdad de correspondencia está permitida; ausente si no lo está
ORDERING	Nombre de la regla de correspondencia si está permitida la ordenación; ausente si no lo está.
SUBSTRING	Nombre de la regla de correspondencia si está permitida la correspondencia de sub-string ausente si no lo está.

Tabla 1.2: Los distintos tipos de atributos en un servidor LDAP.

1.5 Directivas de Bases de Datos.

Un gestor de base de datos es usado para procesar peticiones (queries) o actualizaciones a una base de datos relacional. Estas bases de datos pueden recibir varias órdenes de insertar, modificar o borrar en un período corto de tiempo.

Igualmente el servidor LDAP es usado para procesar peticiones (o queries) a un directorio LDAP. Pero LDAP procesa órdenes de borrar y actualización de una manera lenta.

En otro decir, LDAP es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente; como se menciono anteriormente, LDAP es una base de datos no relacional.

El servidor LDAP al no ser una base de datos relacional no cuenta con las siguientes características:

- Realizan operaciones de escritura intensivas: las bases de datos relacionales se preparan para realizar operaciones que implican modificación o borrado constante de los datos almacenados.

- Esquema específico para cada aplicación._ las bases de datos relacionales se crean para cada aplicación, siendo difícil adaptar los esquemas a nuevas aplicaciones.

- Modelo de datos complejo._ manejan modelos complejos de datos que requieren muchas tablas.

- Integridad de datos._ los componentes son desarrollados para mantener la consistencia de la información a todo momento, sobre todo operaciones de rollback, integridad referencial y operaciones orientadas a transacciones.

- Las transacciones se efectúan siempre aparte de las otras transacciones. De tal forma que si dos transacciones se ejecutan de forma concurrente la una transacción para inadvertida a la otra transacción y viceversa, hasta que ambas transacciones han sido completadas.

- Disponen de operaciones de *roll-back*.

El archivo de configuración del servidor LDAP (*slapd)* trabaja con tres diferentes bases de datos de backend (dorsal, o base de datos de segundo plano) entre las cuales se puede elegir. Se trata de LDBM, una base de datos de gran rendimiento basada en disco; SHELL, una interfaz de base de datos para dar órdenes arbitrarias o scripts del interpretador de órdenes (shell); y PASSWD, una sencilla base de datos de contraseñas.

La manera de funcionar de la base de datos LDBM es asignar un identificador compacto de cuatro bytes único para cada entrada de la base de datos. La base de datos utiliza este identificador para referirse a entradas en los índices. La base de datos está compuesta de un fichero índice principal, que mapea el identificador único de la entrada en representación en texto de esa entrada. También se da tareas de mantenimiento a otros ficheros índice.

1.6 Librerías.

Las librerías LDAP dan soporte a los programas de LDAP y proporcionan funcionalidad a otros programas que interactúan con LDAP.

Existen varias librerías de diversos tipos para el servidor LDAP entre algunas están las siguientes:

Librerías de autentificación pam-ldap y nss-ldap

La librería pam-ldap permite a las aplicaciones que usan PAM (Pluggable Authentication Modules) autentificarse, puedan hacerlo mediante un servidor LDAP. Para que Linux se autentifique mediante un servidor LDAP es necesario instalar esta librería ya que utiliza PAM. El archivo de configuración de ésta librería esta localizada en /etc/pam_ldap.conf para lo que se necesita instalar el paquete correspondiente. Hay otras aplicaciones y servicios que utilizan PAM para la autentificación y por lo tanto pueden gracias a la librería pam-ldap, autentificarse ante un servidor LDAP.

Para especificar el modo de autentificación de cada servicio es necesario configurar los archivos que están en la carpeta /etc/pam.d/**.**

La librería nss-ldap permite resolver nombres del sistema; permite que un servidor LDAP reemplace a los archivos /etc/passwd, /etc/group y /etc/shadow como bases de datos del sistema. En su archivo de configuración se define las fuentes de datos para los usuarios y grupos que será capaz de ver el sistema Linux. Se encuentra localizado en /etc/libnss-ldap.conf. Posteriormente debemos configurar el archivo /etc/nsswitch.conf para que LDAP sea usado como base de datos del sistema en lugar de los archivos passwd, group y shadow.

La instalación de ambas librerías se puede realizar mediante el comando apt-get.

Librería GLIBC._ Esta librería permite a los programas conocer los nombres de los usuarios, hosts o grupos.

Librería liblber._ Contiene funciones de decodificación, codificación y de operaciones de lectura, escritura.

Librería libldap._ Tiene funciones que implementan los APIs de LDAP, las cuales son responsables de pedir operaciones al servidor LDAP.

Librería libldif._ En esta librería están funciones que manipulan datos del archivo LDIF.

Librería libprldap._ Librería que une LDAP y NSPR.

Librería libslldap._ Librería que une LDAP con NSS.

Librerías de lenguaje C._ Permiten crear aplicaciones para acceder, manejar, actualizar y buscar información que se encuentra en directorios relacionados con LDAP o con directorios Novell, tales librerías son ldapsdk.dll, ldapssl.dll, ldapx.dll, etc. Entre las librerías usadas en Novell están delim.dll, dirload.dll, ldaphdlr.dll, ldif.dll, schhdlr.dll.

Librerías para Solaris._ Entre las librerías para Solaris se encuentra libldapsdk.so, libldapx.so, libldapssl.so, libldapgss.so, etc.

1.7 Introducción Slapd

Slapd es el archivo de configuración del servidor LDAP, el cual puede funcionar en muchas plataformas. Se puede utilizar para proveer un servicio de directorio como se desee. El directorio puede contener por decir lo que se desee colocar en el, se lo puede conectar al servicio de directorio LDAP global, o hacer funcionar un servicio por cuenta propia. Algunas de las características y capacidades más interesantes con las que cuenta *slapd* son las siguientes:

LDAPv3._ *slapd* tiene la implementación versión 3 de LDAP, igualmente tiene el soporte sobre IP versión 4 e IP versión 6, además de UNIX IPC.

Capa de seguridad y Autentificación simple._ *slapd* tiene fuerte soporte en servicios de integridad y confidencialidad en lo referente a seguridad de datos y también un alto nivel de autenticación a través del uso de SASL (*Simple Authentication and Security Layer).* Esta implementación utiliza el software CYRUS SASL el cual tiene soporte de algunos mecanismos como GSSAPI.

Seguridad de capa de transporte._ *slapd* tiene soporte de servicios de autenticación basada en certificados y seguridad de datos (confidencialismo e integridad) a través del uso de TLS (o SSL). Esta implementación utiliza el software OpenSSL.

Control de topología._ Este archivo puede ser configurado para restringir acceso a capas basadas sobre información topológica de red. Esta característica utiliza los envoltorios TCP.

Control de Acceso._ *slapd* provee una rica y fuerte facilidad de control de acceso, permitiendo al administrador controlar el acceso a la información en la base de datos. Se puede controlar el acceso a las entradas basadas en información de autorización de LDAP, direcciones IP, nombres de dominio y otros criterios. Tiene soporte de información de control de acceso ya sea dinámica o estática.

Internacionalización._ Tiene soporte UNICODE y etiquetas de lenguaje.

Elección de *Backends* de Bases de Datos._ Este archivo viene con una variedad diferentes *backends* de base de datos como BDB que es una base de datos transaccionales de alto desempeño, HDB que es un *backend* transaccional de alto desempeño jerárquico, LDBM que es un DBM ligero, entre otros.

múltiples instancias de base de datos._ Puede ser configurado para servir a múltiples bases de datos al mismo tiempo, esto quiere decir que un simple servidor puede responder a peticiones para muchas porciones diferentes lógicas del árbol LDAP, usando el mismo o diferentes *backends* de bases de datos.

Módulos Genéricos API._ Si se requiere más personalización, *slapd* permite escribir módulos propios fácilmente. Este archivo consiste de dos partes que son: un fin de frente que maneja comunicaciones del protocolo con clientes LDAP, y módulos los cuales manejan tareas especificas tales como operaciones de bases de datos. Debido a que estas dos piezas se comunican vía API bien definido, se puede crear módulos personalizados el cual extiende *slapd* en varias maneras; igual cierto numero de módulos de base de datos programables son provistas, esto permite exponer fuentes de datos externa a este archivo usando conocidos lenguajes de programación.

Hilos._ Este archivo tiene hilos para alto desempeño. Un sencillo proceso de *slapd* multi hilo maneja todas las peticiones entrantes usando una reunión de hilos. Esto reduce la cantidad de *overhead* requerido por el sistema.

Replica._ El archivo puede ser configurado para mantener copias sombra de la información del directorio. Este esquema de replica multi esclavo o maestro simple es vital en ambiente de alto volumen en donde un único archivo no provee la disponibilidad o fiabilidad necesaria. *Slapd* usa dos métodos de replica los cuales son: LDAP basado en sincronismo y basado en *slurpd.*

Cache Proxy._ El archivo puede ser configurado como un servicio de Proxy caché de LDAP.

Configuración._ Este archivo es altamente configurable a través de un simple archivo de configuración el cual permite hacer cambio sobre cualquier cosa que se desee cambiar. Las opciones de configuración tienen opciones por defecto razonables lo cual hace el trabajo más sencillo.

1.8 Introducción Slurpd

Slurpd es un dominio que con la ayuda de *slapd* provee servicio replicado. Este archivo es responsable de distribuir cambios hechos a la base de datos de *slapd* maestro hacia las diversas replicas *slapd.* El dominio libera el archivo *slapd* de tener que preocuparse de que algunas replicas puedan estar caídas, o no están accesibles cuando se viene un cambio; *slurpd* maneja automáticamente los reenvios de las peticiones que han fallado. *slapd* y *slurpd* se comunican a través de un simple archivo de texto, que es utilizado para almacenar los cambios ocurridos.

Slurpd brinda la capacidad a un archivo maestro *slapd* a que se propague los cambios que realiza a las diferentes instancias *slapd* esclavas, implementando el esquema de la replica maestro – esclavo. Este archivo funciona sobre el mismo *host* como sobre la instancia *slapd* maestro.

Conclusiones

Al concluir este capitulo tendremos conocimientos de los conceptos teóricos mas importantes relacionados con el servidor de directorios LDAP, de conceptos y archivos relacionados con este y con su configuración, cuando se pase a la parte practica se tendrá un nivel mayor de preparación y conocimiento para realizar las instalaciones, configuraciones y pruebas correspondientes al servidor de directorios LDAP.

CAPITULO 2: INSTALACION DEL SERVIDOR LDAP

2.1 Introducción

La instalación implica la correcta configuración y funcionamiento del servidor LDAP, para ello se debe trabajar correctamente en su archivo de configuración *slapd*. Con este archivo también se puede crear la base de datos correspondiente, con esto se puede manejar ya sea un directorio o un servidor de autenticación correctamente.

2.2 Instalación

Para realizar la instalación del servidor LDAP se debe seleccionar el paquete del servidor LDAP al momento de realizar la instalación del sistema operativo.

Al momento de seguir los pasos para la instalación del sistema operativo Linux, en la ventana que se muestra en el siguiente grafico se debe seleccionar la opción de "personalizar ahora" para que nos permita seleccionar los paquetes necesarios para poder contar con el paquete del servidor LDAP.

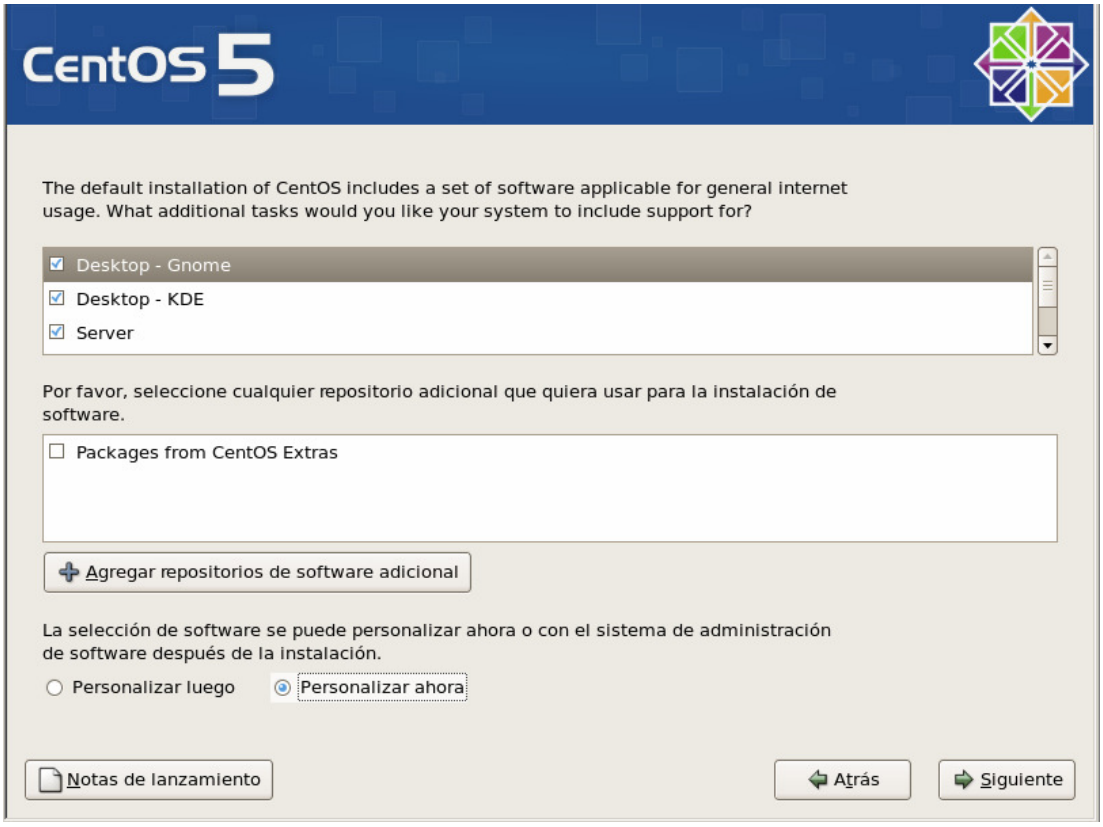

Figura 2.1:Vista previa a la selección de paquetes para la instalación

En la siguiente ventana aparece por categorías los paquetes a seleccionar para la instalación. Al hacer clic en la categoría de servidores aparece a la derecha una subcategoría de servidores. Se selecciona servidores de red y se da clic en el botón de paquetes opcionales y aparecerá la ventana de los paquetes y se selecciona "*openldap servers – 2.3.27-5.i386"* la cual es la versión que viene con *Centos* 5.

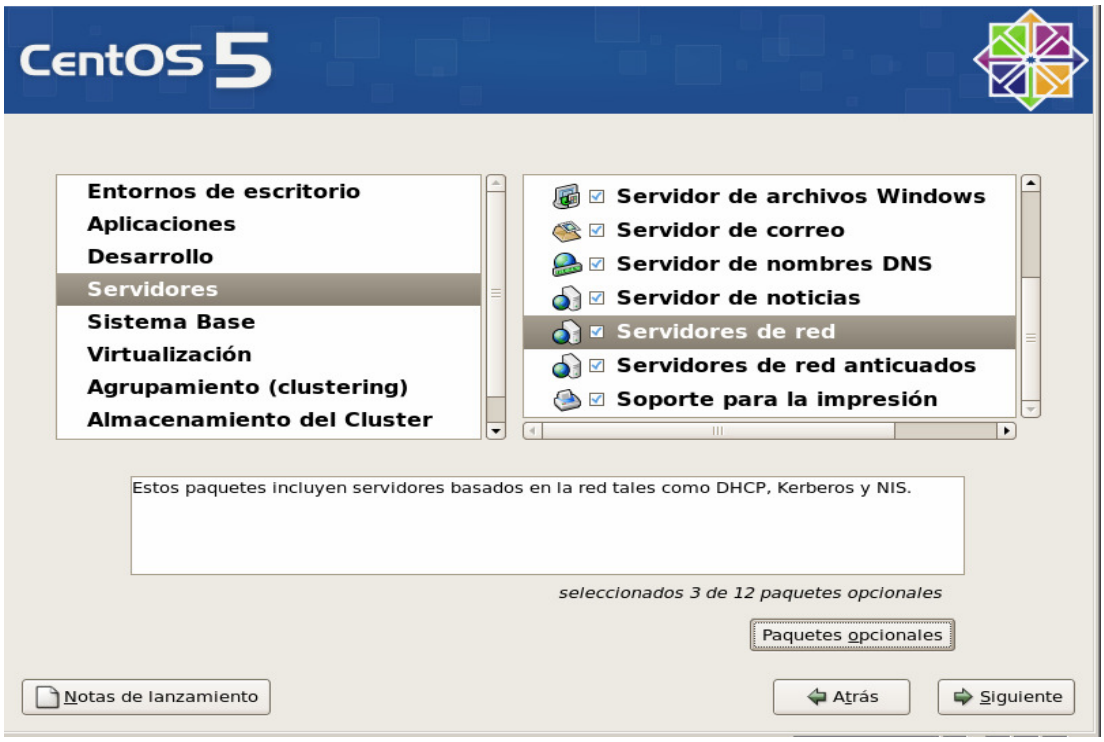

Figura 2.2: Cuadro de selección del paquete de instalación del servidor.

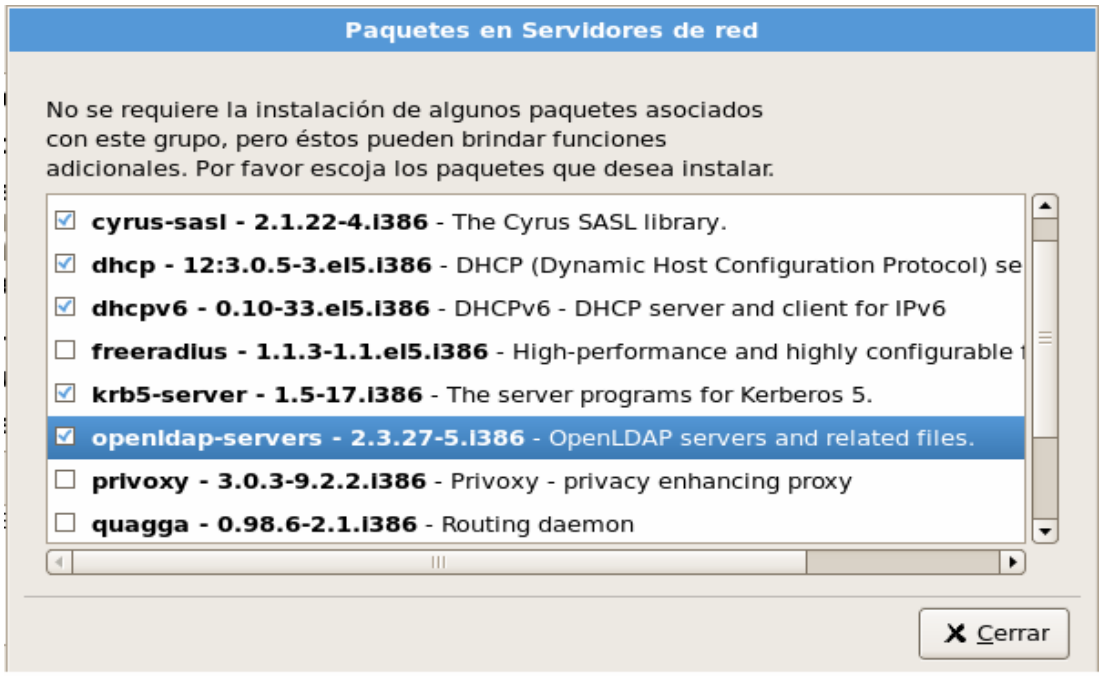

Figura 2.3: Paquetes en servidores de red

Es necesario realizar la instalación del paquete que contiene el cliente LDAP, para esto en la categoría “sistema base”, la que continua después de “servidores”, se selecciona la subcategoría “herramientas de sistema” y una vez ahí se selecciona el paquete “.

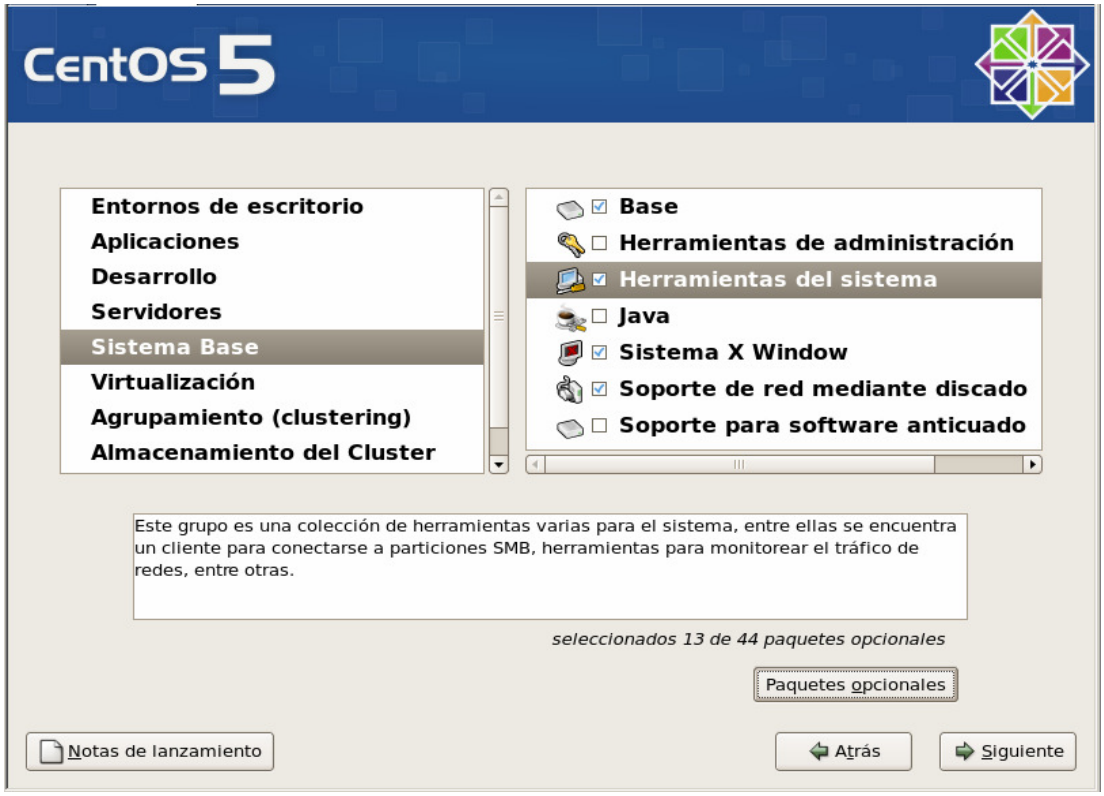

Figura 2.4: Cuadro de selección del paquete de instalación del cliente

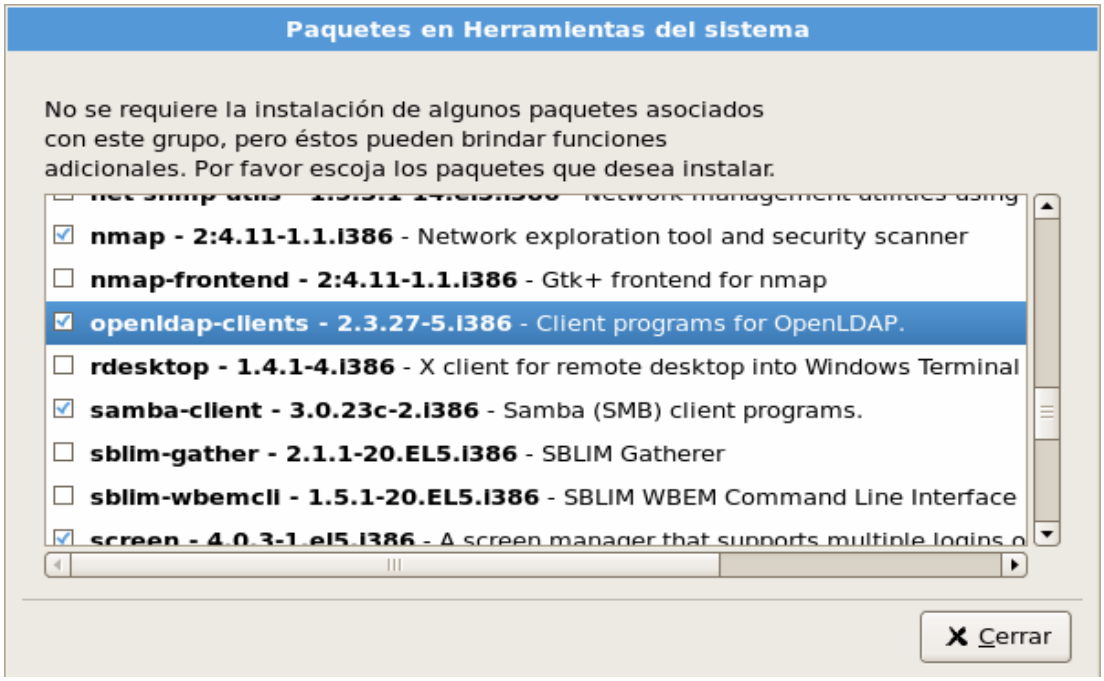

Figura 2.5: Paquetes en herramientas del sistema

Como paquetes adicionales que pueden ayudar con la aplicación del servidor y que también sirven para dar distintos tipos de soporte se recomienda realizar la instalación de los paquetes "*openldap–devel 2.3.47-5.i386"* y "*openssl-devel – 0.9.8b-8.3.el5.i386"* que se encuentra en la categoría "*desarrollo"* y "*compat-openldap – 2.3.27_2.2.29-5"* que se encuentra en la categoría de "Sistema Base".

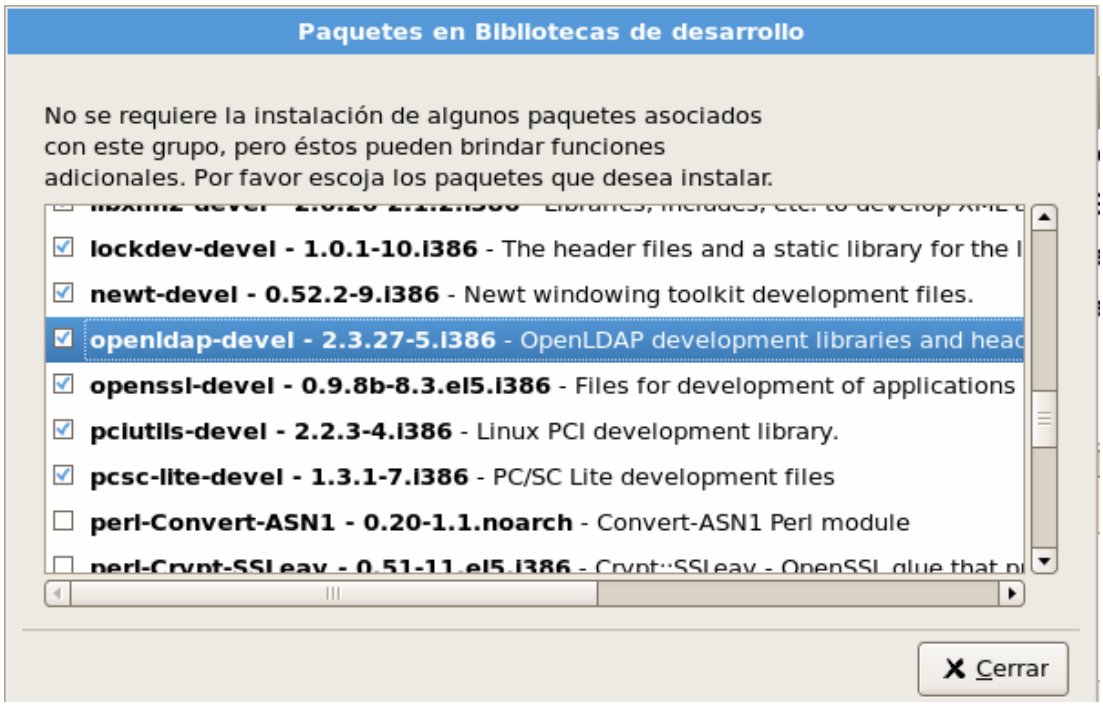

Figura 2.6: Paquetes en Bibliotecas de desarrollo

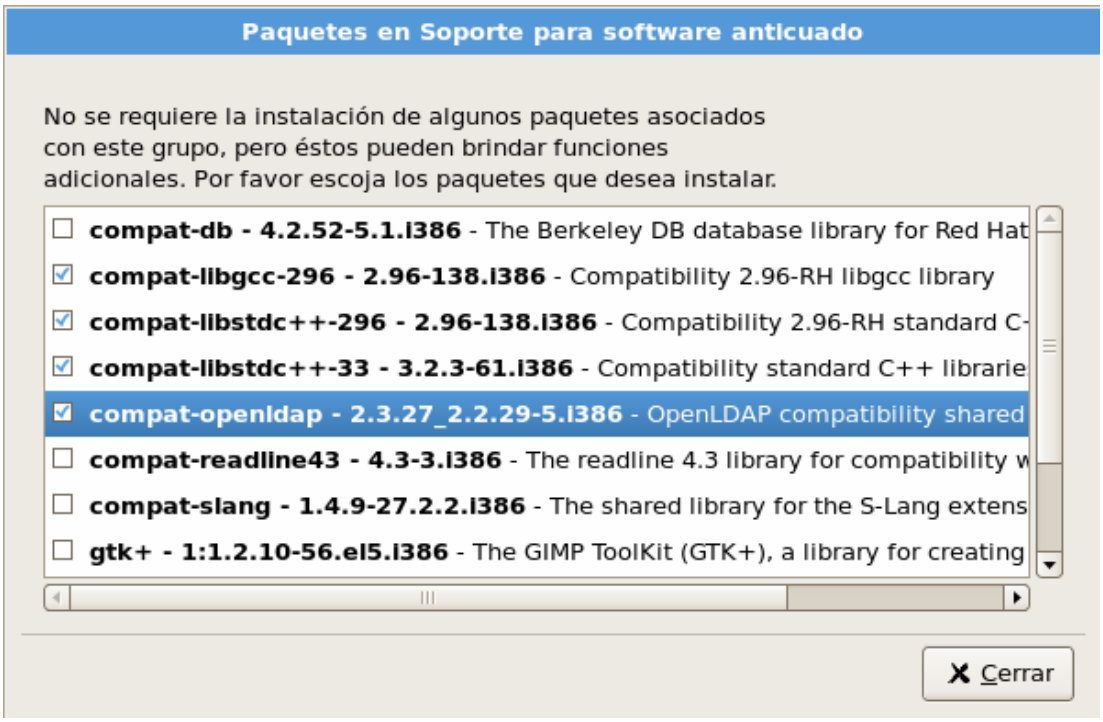

Figura 2.7: Paquetes en soporte para software anticuado

Luego de instalado el sistema operativo Linux y por ende el servidor se puede revisar la versión y paquetes instalados por medio del siguiente comando:
rpm -qa | grep openldap

Y como resultado de la ejecución de ese comando se vera la siguiente figura que indica los paquetes que se encuentran instalados:

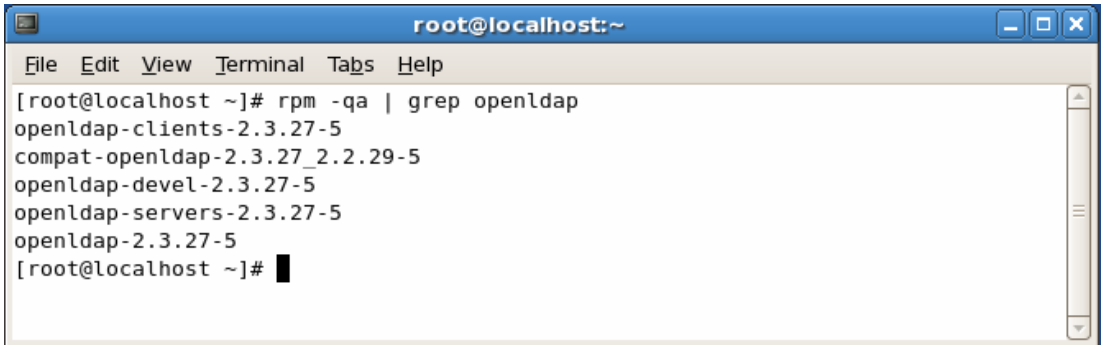

Figura 2.8: Revisando la versión del servidor LDAP instalado y sus paquetes

2.3 Configuración de LDAP como libreta de direcciones

Para configurar el servidor como libreta de direcciones se creara un directorio específico para el propósito dado con permiso de acceso para el usuario root, se lo hace de la siguiente manera:
Mkdir /servidor/libreta
Chmod 700 /servidor/libreta

Cabe indicar que esto se lo realiza bajo el usuario root por lo tanto el propietario de la carpeta es el usuario root y es este quien tiene todos los privilegios relacionados con este.

Luego se crea una clave de acceso que se asignara al usuario que es administrador del directorio, para esto se ejecuta el siguiente comando:
Slappasswd

En el grafico siguiente se puede ver lo que ocurre al ejecutar este comando que permite asignar clave:

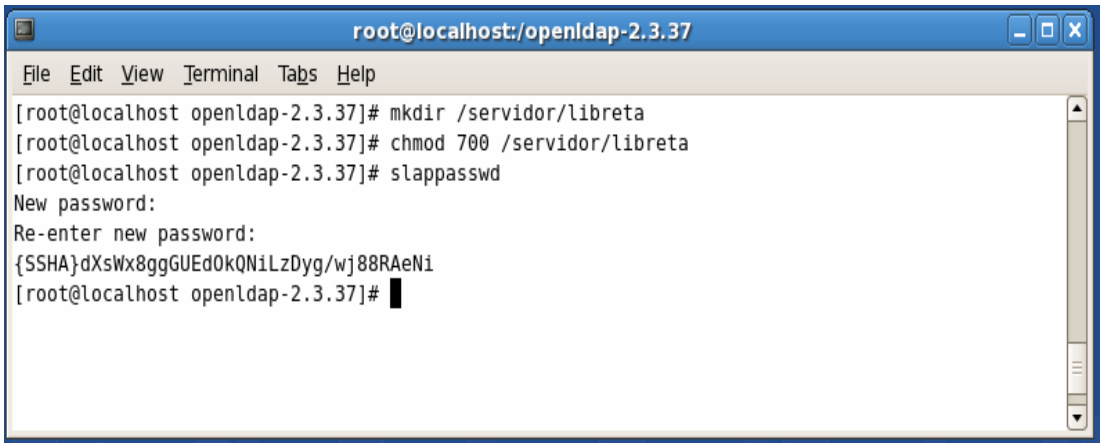

Figura 2.9: Ingreso de password por medio de slappasswd

El criptograma que sale como resultado de crear el password se utilizara después en el archivo /etc/openldap/slapd.config y el usuario root será el que tenga todos los privilegios para con el directorio.

Se copia el archivo de esquema de evolution-data-server dentro del directorio /etc/openldap/schema de la siguiente manera:

cp /usr/share/evolution-data-server-1.18/evolutionperson.schema \

/etc/openldap/schema/

En el siguiente grafico se puede ver mejor lo que se pretende hacer con la ejecución de este comando:

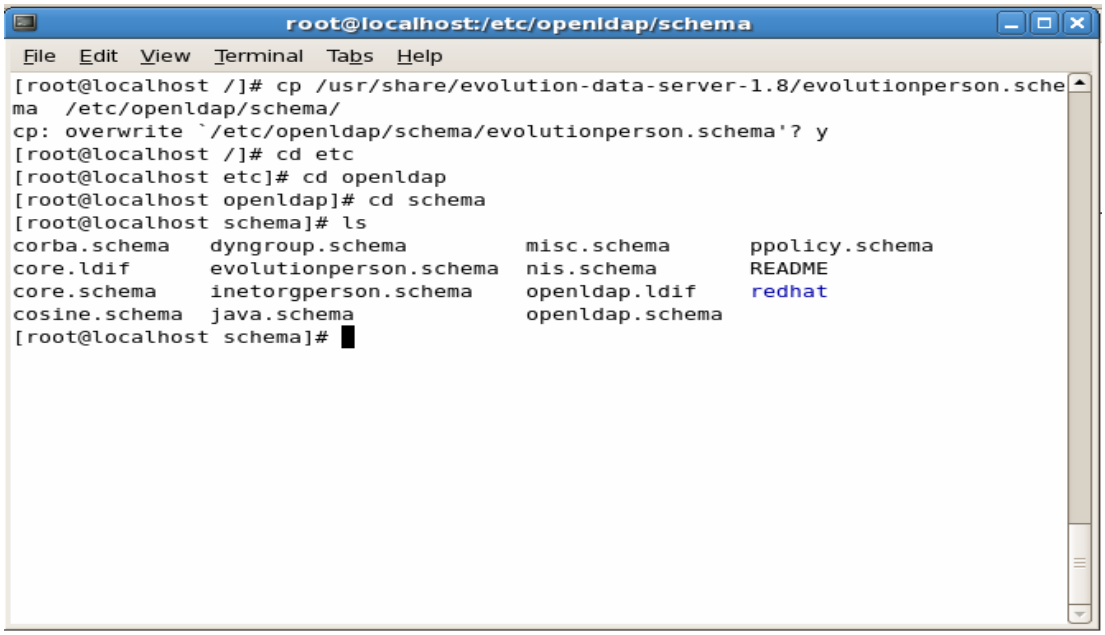

Figura 2.10: Uso del comando cp para copiar el archivo evolutionperson.schema

Luego se edita el archivo /etc/openldap/slapd.conf y se agrega el esquema de datos que viene agregado con evolution-data-server, la siguiente línea es agregada:
Include /etc/openldap/schema/evolutionperson.schema

En el grafico siguiente se muestra el archivo con la línea agregada descrita anteriormente:

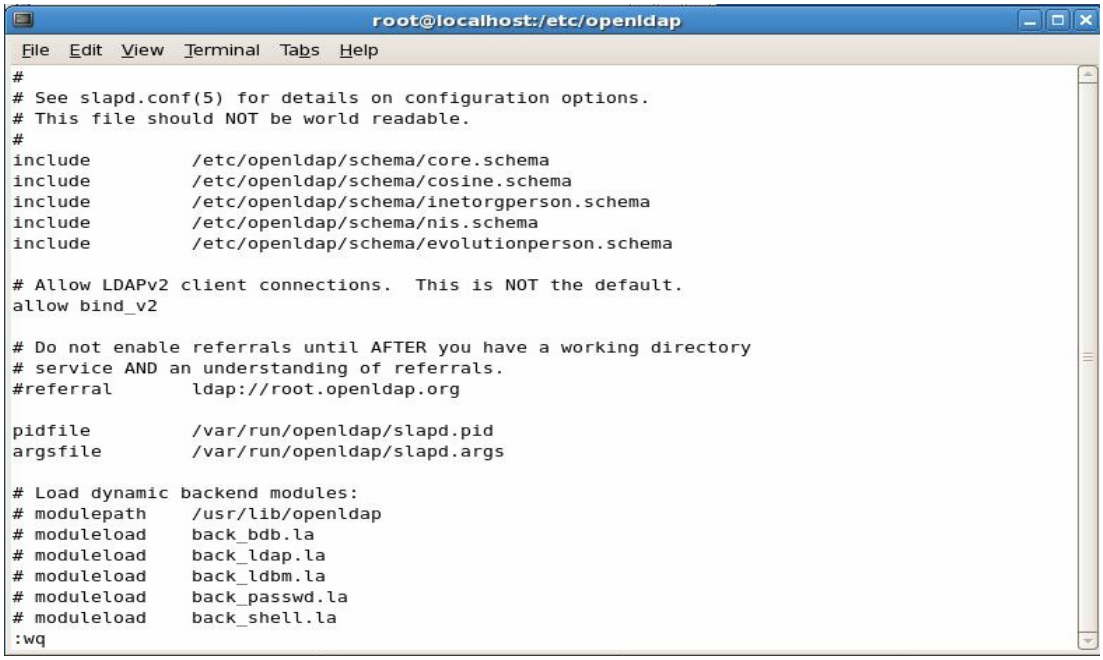

Figura 2.11: El archivo slapd con la inclusión del archivo evolutionperson.schema

Aparte de lo que se tenga configurado, al final del archivo *slapd.conf* se añade lo siguiente con el fin de definir el nuevo directorio que será utilizado como la nueva libreta de direcciones. Para este caso en la línea de contraseña se utilizara texto plano para mayor facilidad de manejo.

database bdb
suffix "dc=dominiouda,dc=edu"
rootdn "cn=jllerena,dc=dominiouda,dc=edu"
rootpw idroot
directory /servidor/libreta/

Índices a mantener para esta base de datos
index objectClass eq,pres
index ou,cn,mail,surname,givenname eq,pres,sub

index uidNumber,gidNumber,loginShell eq,pres

index uid,memberUid eq,pres,sub

index nisMapName,nisMapEntry eq,pres,sub

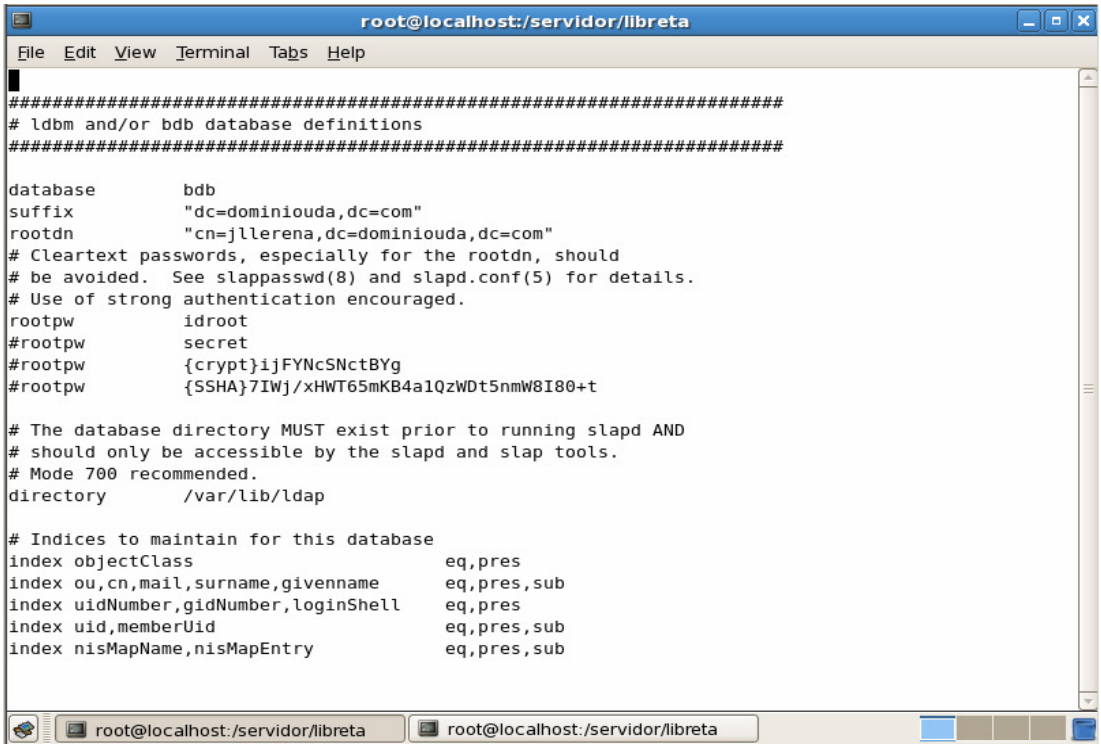

Figura 2.12: Definición de dominio e índices en el archivo *slapd*

Ahora se debe iniciar el servicio de LDAP y añadirlo a los demás servicios que arrancan junto con el sistema, se lo hace de la siguiente manera:

Service ldap Start

Chkconfig ldap on

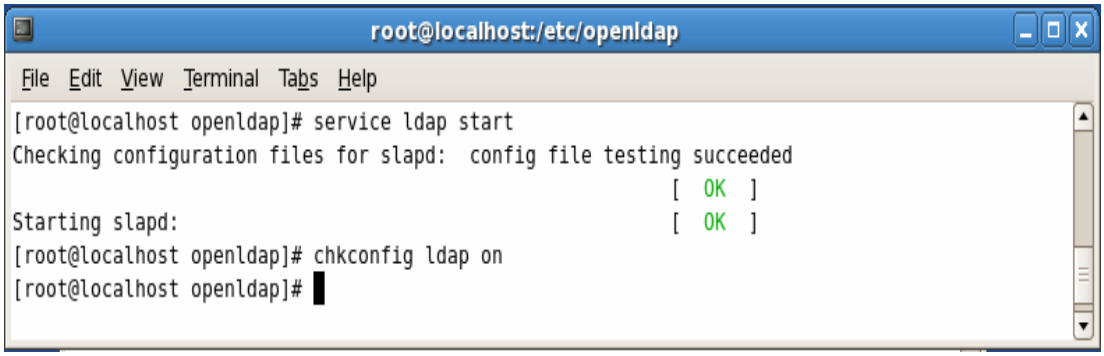

Figura 2.13: Inicio del servicio LDAP

A continuación hay que crear el objeto que a su vez contendrá el resto de los datos en el directorio. Hay que crear un archivo con la extensión .ldif , este archivo es un

archivo de texto sencillo en donde se escribe la información donde se almacenara los datos, puede tener un número arbitrario de pares de atributos y sus valores. Se creara un archivo .ldif que se lo llamara agenda.ldif y contendrá lo siguiente:

dn: dc=dominiouda, dc=edu
objectClass: top
objectClass: dcObject
objectClass: organization
o: UDA
dc: dominiouda

dn: ou=libreta, dc=dominiouda, dc=edu
ou: libreta
objectClass: top
objectClass: organizationalUnit

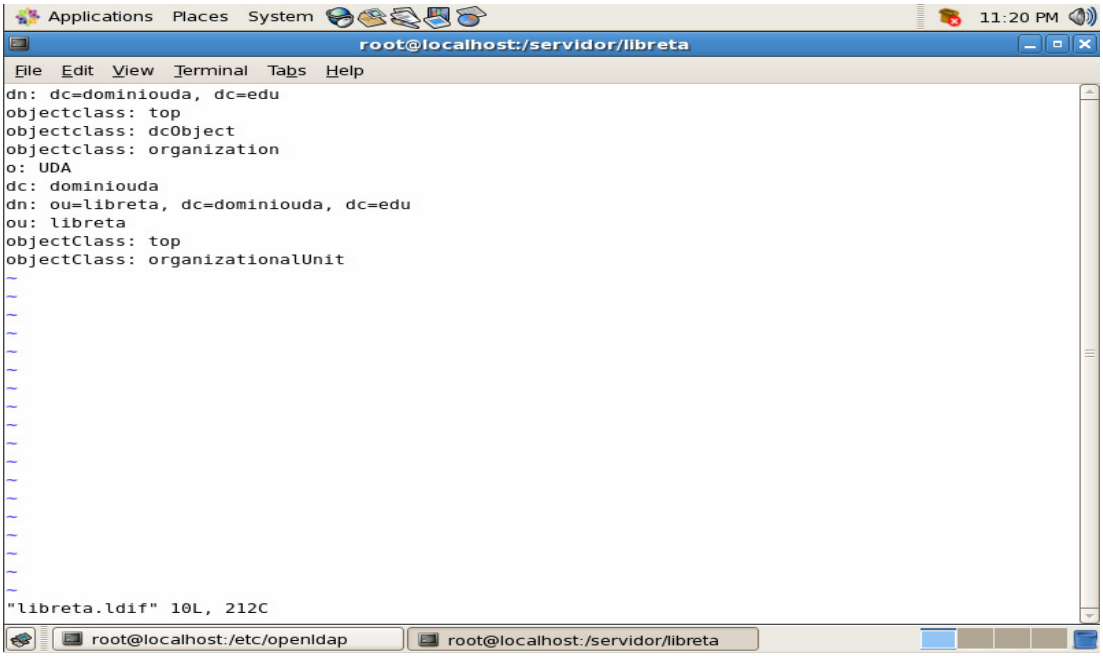

Figura 2.14: Archivo agenda.ldif

Se utilizará el comando **ldapadd** para ingresar los datos necesarios. Las opciones utilizadas con este comando serán las siguientes:

-x	autenticación simple
-W	solicitar clave de acceso

-D binddn Nombre Distinguido (dn) a utilizar

-f archivo Archivo a utilizar

Ahora se procede a ingresar la información generada en el directorio utilizando lo siguiente:

ldapadd -x -D 'cn=jllerena, dc=dominiouda, dc=edu' -W -f libreta.ldif

Luego de ejecutar el comando, el ingreso de una contraseña será requerido. La contraseña a utilizar será la especificada en el archivo de configuración la cual es idroot, luego de ingresada la contraseña el comando devolverá los siguientes mensajes:
Adding new entry “dc=dominiouda,dc=com”
Adding new entry “ou=libreta,dc=dominiouda,dc=com”

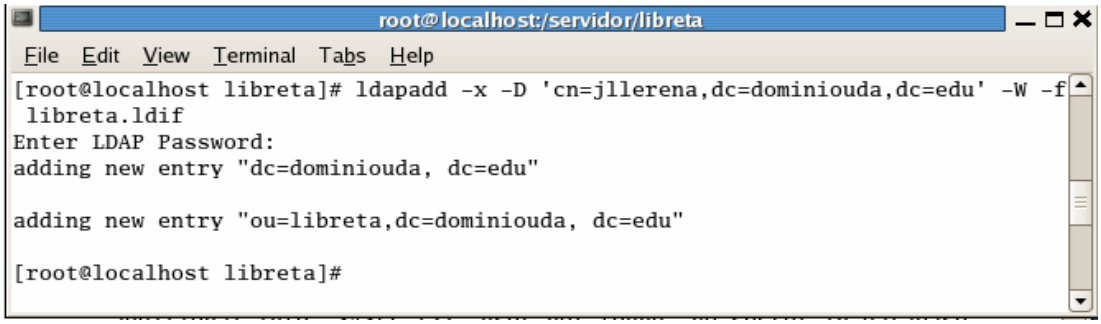

Figura 2.15: Ingreso de datos con el comando ldapadd

Si pretendemos ejecutar nuevamente el comando nos dará el mensaje de que los datos ya existen en el servidor.

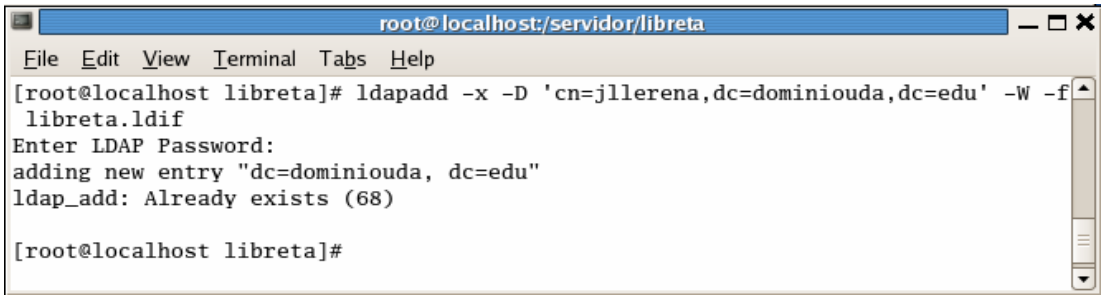

Figura 2.16: Mensaje de registro existente

Una vez realizado lo anterior, se puede empezar a llenar el directorio con información. Se realiza la creación de un archivo el cual se llamara usuarios.ldif.

Los campos vacíos o innecesarios deben ser eliminados debido a que si ocurre esto el servidor no le dejará insertar estos datos. Es importante que se incluya las clases top, person, organizationalPerson, inetOrgPerson y evolutionPerson, ya que de no ser así, no será posible utilizar los campos de información que se necesitan para que el directorio funcione como libreta de direcciones.

dn: cn=José Llerena, ou=libreta, dc=dominiouda, dc=edu
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: evolutionPerson
cn: Jose Llerena
givenName: Jose
sn quiere decir surname o apellido
sn: Llerena
displayName: Tigrinni
title: Ing.
mail: jllerena@dominiouda.edu
initials: JALLC
o: UDA
ou: libreta
Puesto que desempeña en su empresa
businessRole: gerente
#Domicilio
homePostalAddress: Rafael Fajardo 5-53
#Dirección de trabajo
postalAddress: Benigno malo 10-32
#Ciudad
l: cuenca
#Provincia
st: Azuay
Teléfono trabajo
telephoneNumber: 593-72853439

Teléfono principal

primaryPhone: 593-72863831

Teléfono móvil

mobile: 593-98528214

Teléfono hogar

homePhone: 593-72853431

Otro teléfono

otherPhone: 593-72844118

labeledURI: http://www.josellerena.com/

Su fecha de nacimiento

birthDate: 1982-03-06

Primero el apellido y de ahí el nombre

fileAs: Llerena Jose

category: Monografía

managerName: Alfredo Llerena

assistantName: Andrés Alves

Teléfono de su asistente,

assistantPhone: 593-72800090

Luego de llenar el archivo usuarios.ldif se ingresan estos al servidor con el comando ldapadd de la misma manera que se lo hizo anteriormente.

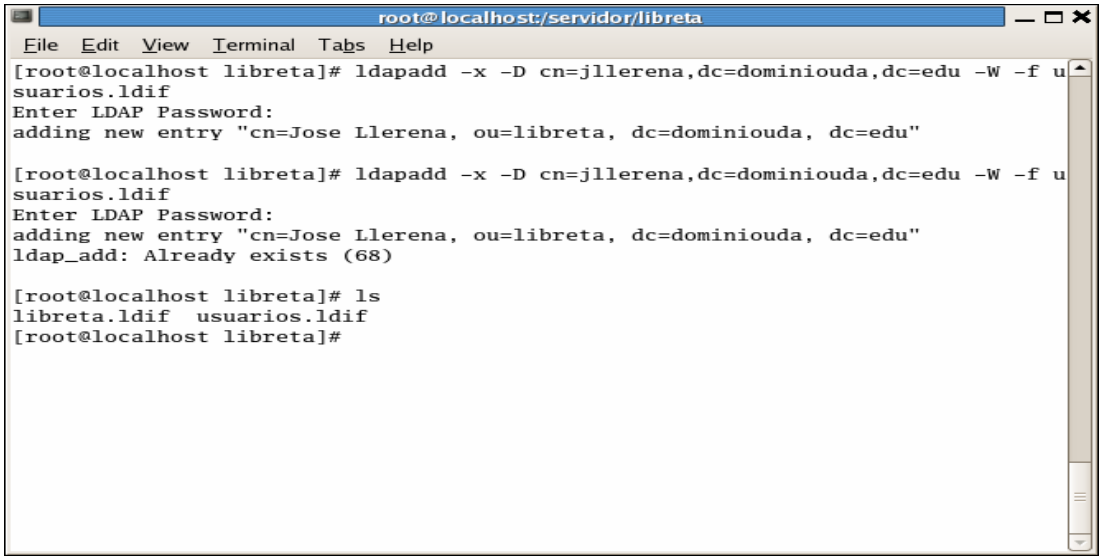

Figura 2.17: Ingreso de datos del archivo usuarios.ldif

Configuración de clientes.

Para realizar la configuración de clientes se debe en primer lugar configurar los dos archivos de configuración de cliente (*/etc/ldap.conf* y */etc/openldap/ldap.conf*). Como aplicación cliente se puede utilizar cualquier programa que cuente con esta opción, como ejemplo utilizado para la configuración de clientes se muestra el programa *mozilla thunderbird*.

Una vez ejecutado el programa mozilla thunderbird se procede a ir a hacer clic a la casilla de libreta de direcciones, una vez abierto la ventana de la libreta de direcciones se debe ir a:

Menú → Nuevo → Directorio LDAP

Una vez hecho esto aparece la ventana de propiedades de servidor de directorios en la que se debe llenar la información de la siguiente manera:

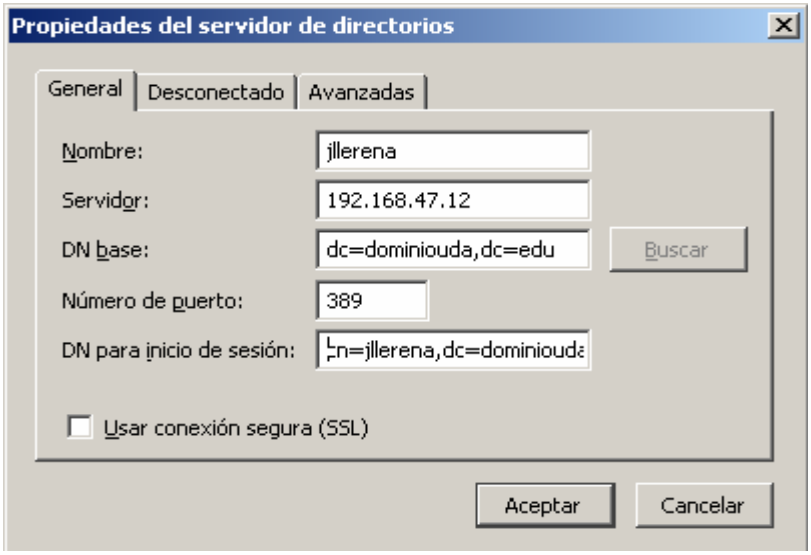

Figura 2.18: Ventana de las propiedades del servidor de directorios

Squirrelmail.

Hay que editar el archivo **/etc/squirrelmail/config.php** y añadir/editar:

```
$ldap_server[0] = array(
   'host' => '127.0.0.1',
   'base' => 'ou=libreta,dc=dominiouda,dc=edu',
   'name' >= 'libreta'  );
```

LDAP Browser/Editor 2.6.

Un buen programa cliente que nos permita visualizar los datos que hemos creado es el programa Softerra LDAP Browser/Editor 2.6.

Para el propósito de este punto se mostrara la configuración de este programa para visualizar la libreta de direcciones que se ha creado.

En la barra de menú se va a la opción File → *New Profile*, se asigna el nombre del perfil a crear y luego se incluye la información referente al servidor LDAP, cabe observar que la opción de usuario anónimo se habilita para conectarse como usuario anónimo.

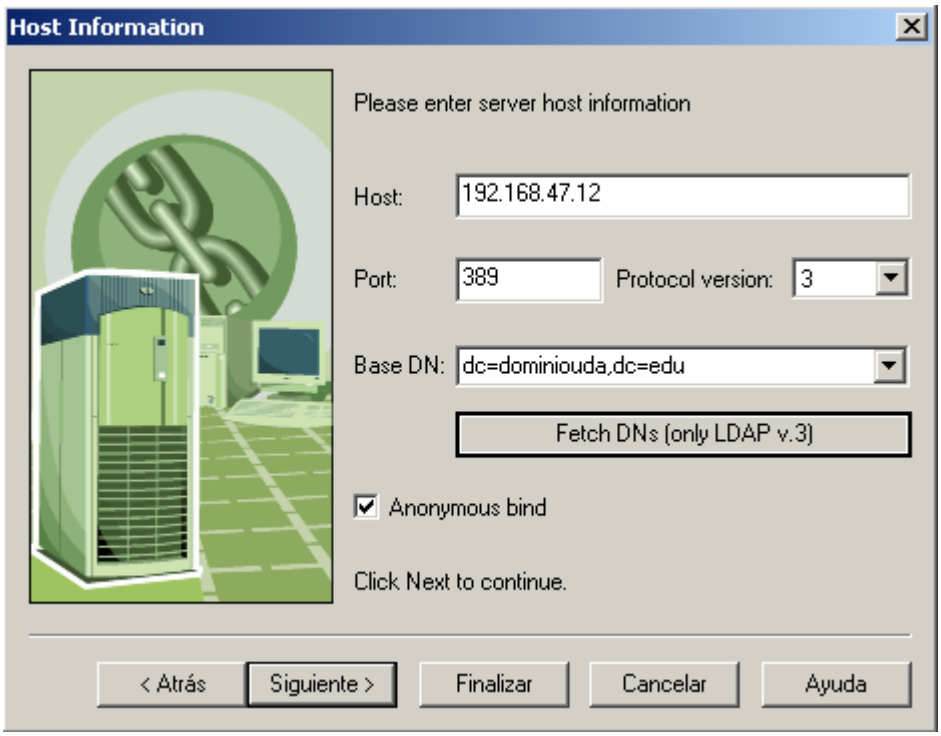

Figura 2.19: Información del servidor en LDAP Browser/Editor 2.6

Respaldo de datos.

Para poder respaldar los datos lo primero que debe hacerse es detener el servicio de LDAP (service LDAP stop).

Luego de detener el servicio se utiliza el comando *slapcat,* utilizando el archivo de configuración del servidor que se encuentra en la ruta /etc/openldap/slapd.conf, la manera de proceder es la siguiente:

slapcat -v -f /etc/openldap/slapd.conf -l respaldo-$(date +%Y%m%d).ldif

Después de haber respaldado los datos se puede iniciarse nuevamente el servicio.

Figura 2.20: Respaldo de datos con el comando *slapcat*

Restauración de datos.

De igual manera cuando se hace el respaldo de los datos, para restaurarlos se debe detener el servicio. Después de detener el servicio lo que se debe hacer es borrar los datos del directorio en el cual se desea restaurar los datos por medio del siguiente comando:

rm -f /var/lib/ldap/addressbook/*

De ahí se recurre al comando *slapadd* para recuperar la información desde un archivo ldif de respaldo, se lo hace de la siguiente manera:

slapadd -v -c -l respaldo-20070815.ldif -f /etc/openldap/slapd.conf

También es necesario ejecutar el comando *slapindex,* el cual es utilizado para regenerar los índices del servidor LDAP.

Concluido con el proceso de restauración de datos, se puede iniciar otra vez el servicio de ldap por medio se *service ldap Start*.

2.4 Configuración de LDAP como servidor de autenticación

Para crear un servicio de autenticación se procederá en primera instancia crear un directorio dedicado al propósito, y a su vez dar los permisos respectivos solamente al administrador (root). Por lo tanto se procede a realizar lo mencionado:

Mkdir /servidor/libreta
Chmod 700 /servidor/libreta

Luego se procede a crear la clave de acceso que asignara LDAP al usuario que administrara el directorio, se lo hace por medio del comando slappasswd y dará como salida un criptograma que será utilizado en el archivo de configuración del servidor *slapd.conf* (*/etc/openldap/slapd.conf*).

En el archivo *slapd.conf* debe estar presente los archivos de esquema requeridos se encuentren presentes, estos se pueden ver al inicio del archivo y en caso de que no se encuentren presentes, se debe agregar las líneas respectivas, de tal manera que el archivo de configuración quedara de la siguiente manera:

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

En este mismo archivo, sin importar las configuraciones que se tengan realizadas, las cuales no sufrirán modificación alguna, se agrega al final del archivo de configuración */etc/openldap/slapd.conf* lo siguiente, con esto se propone definir el nuevo directorio el cual será utilizado para autenticar a toda una red local:

```
database bdb
#en el suffix se describe el nombre de la red local
suffix          "dc=inicioms,dc=com"
rootdn          "cn=josellerena,dc=inicioms,dc=com"
rootpw      {SSHA}zydI3mdstya6fbTQre5kkUiQOYlsNRhz
directory /var/lib/ldap

# Indices to maintain for this database
index objectClass               eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid             eq,pres,sub
index nisMapName,nisMapEntry        eq,pres,sub
```

Luego de editar el archivo de configuración se puede proceder a iniciar el servicio (service ldap Start), o en el caso de que este iniciado el servicio se procede a reiniciar el servicio (*service ldap restart*).

Después de hacer esto, se debe editar el archivo migrate_common.ph, la ruta completa de este archivo es: */usr/share/openldap/migration/migrate_common.ph.* En este archivo se debe modificar los valores de las variables $DEFAULT_MAIL_DOMAIN y $DEFAULT_BASE con lo cual se conseguirá de que las variables queden del siguiente modo:

Default DNS domain

$DEFAULT_MAIL_DOMAIN = "inicioms.com";

Default base

$DEFAULT_BASE = "dc=inicioms,dc=com";

Ahora lo que se debe hacer es crear el objeto que contendrá todos los datos que irán en el directorio, para esto se debe crear un archivo ldif al cual se lo llamara *base.ldif,* este archivo se lo creara de la siguiente manera:

/usr/share/openldap/migration/migrate_base.pl > base.ldif

Con esto la información que esta en el archivo *migrate_base.pl* se lo copiara al archivo que hemos creado (*base.ldif*) con la información de nuestra red.

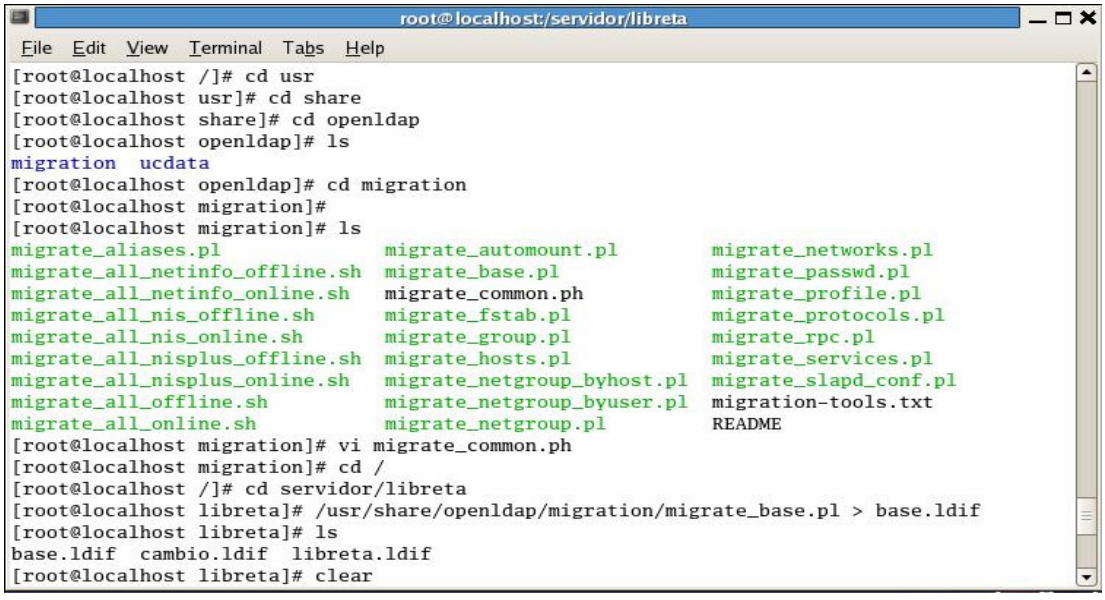

Figura 2.21: Directorio /usr/share/openldap/migration/

Luego de esto se utiliza el comando ldapadd para ingresar los datos, esto se lo hace de la siguiente manera:

Ldapadd –x –w secret –D ‘cn=josellerena,dc=inicioms,dc=com’ –h 192.168.47.11 –f base.ldif.

La opción –f especifica la dirección del servidor LDAP al cual se va a acceder.

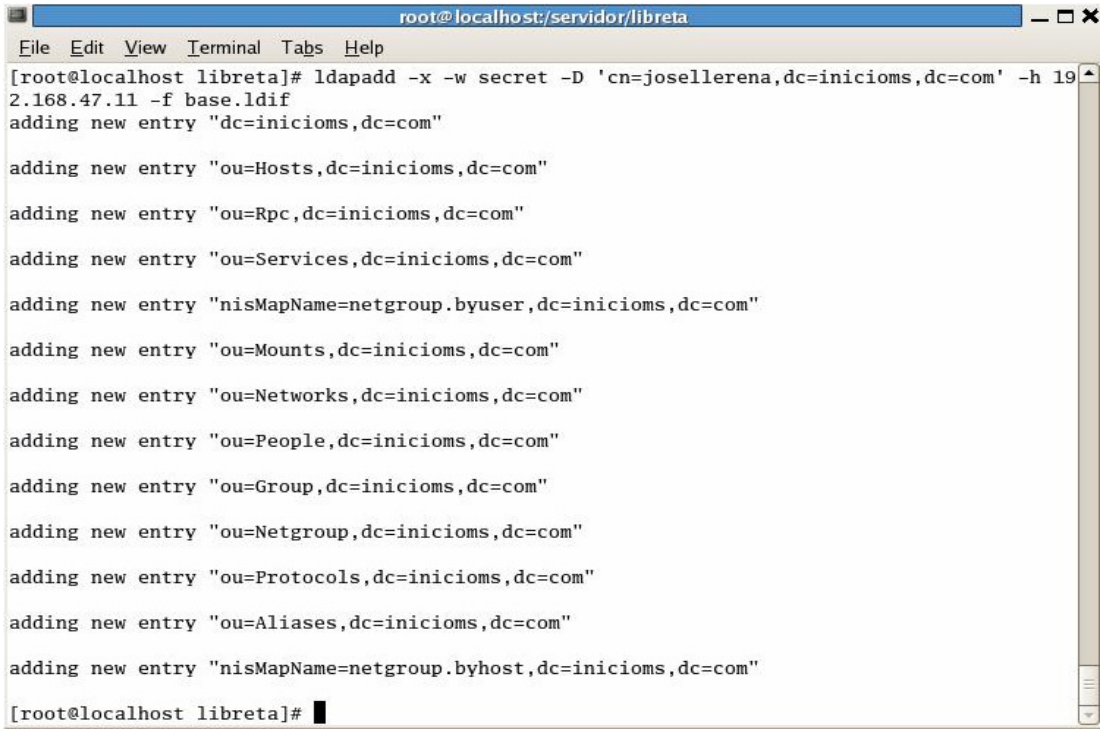

Figura 2.22: Ingreso de datos al servidor usando el archivo base.ldif

Luego de haber hecho lo mostrado anteriormente, se empieza a llenar el directorio con datos, primero se hace la importación de grupos y usuarios que existen en el sistema. La importación de usuarios se lo hace utilizando los guiones correspondientes de la siguiente manera:

/usr/share/openldap/migration/migrate_group.pl /etc/group group.ldif
/usr/share/openldap/migration/migrate_passwd.pl /etc/passwd passwd.ldif

Con esto se crea los archivos *group.ldif* y *passwd.ldif* los cuales van a incluir la información de los grupos y cuentas en el sistema, incluyendo las claves de acceso, entonces estos datos se insertaran de la siguiente manera:

ldapadd -x -w secret -D 'cn=josellerena, dc=inicioms, dc=com' -h 192.168.47.11 -f group.ldif

ldapadd -x –w secret -D 'cn=josellerena, dc=inicioms, dc=com' -h 192.168.47.11 -f passwd.ldif

Con esto se agregan todos los datos referentes a usuarios y grupos del sistema.

Comprobación de los datos.

Antes de poder configurar el sistema para autenticar con LDAP, es necesario verificar que todo este funcionando correctamente.

Esta comprobación se puede hacer con el comando *ldapsearch* de la siguiente forma:

Ldapsearch –h 192.168.47.11 –x –b ‘’ –s base ‘(objectclass=*)’ namingContexts

Si todo esta hecho correctamente la salida del comando debe dar algo parecido a lo siguiente:

```
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectclass=*)
# requesting: namingContexts
#
dn:
namingContexts: dc=dominiouda,dc=edu
namingContexts: dc=inicioms,dc=com
# search result
search: 2
result: 0 Success
# numResponses: 2
# numEntries: 1
```

Si se especifica el comando *ldapsearch* de cómo se muestra en el grafico a continuación, devolverá la información de todo el directorio que se solicite como ejemplo citaremos al directorio que hemos utilizado este rato (dc=inicioms,dc=com):

Ldapsearch –x –b ‘dc=inicioms,dc=com’ ‘(objectclass=*)’

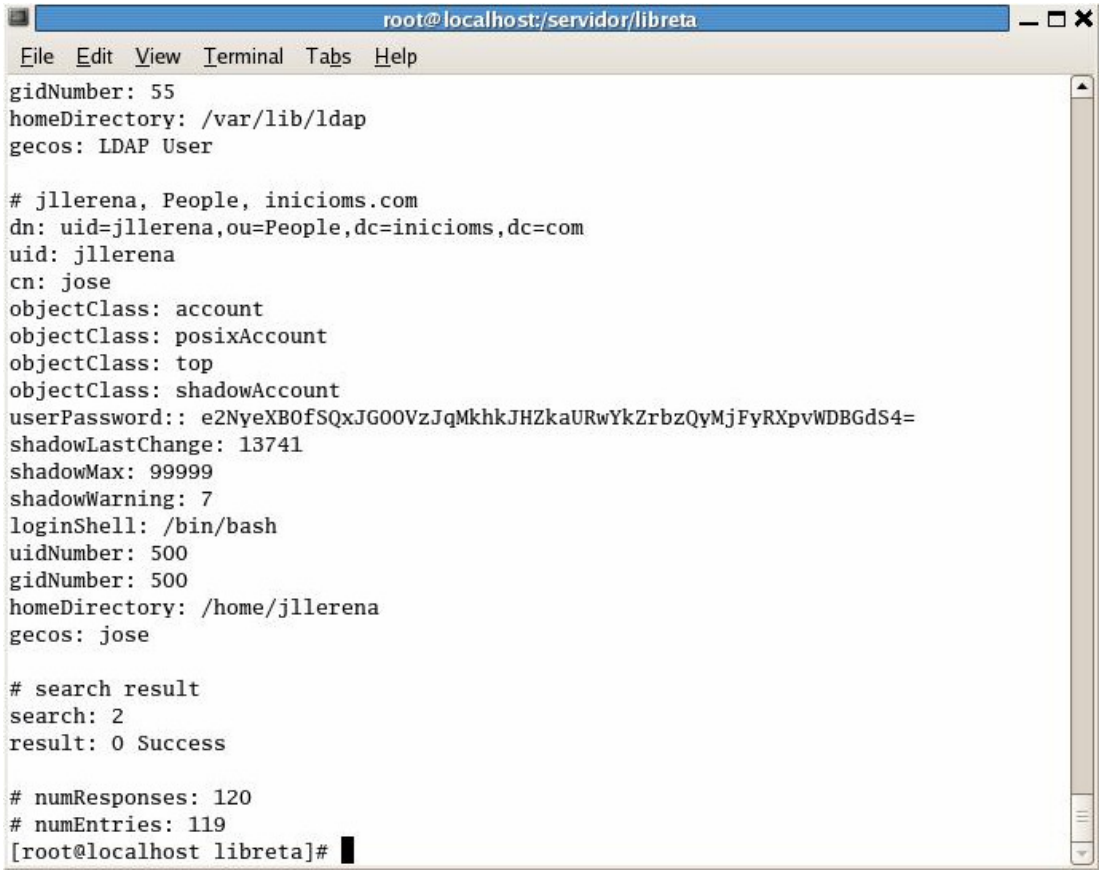

Figura 2.23: realización de búsqueda con el dominio inicioms.com

Como otro ejemplo se puede hacer una búsqueda en particular, usando como ejemplo a un usuario que tiene el sistema, en este caso se usara al usuario jllerena, por lo tanto el comando se ejecuta de esta manera:

Ldapsearch –x –b 'uid=jllerena,ou=people,dc=inicioms,dc=com'

El resultado de este comando dará como resultado lo siguiente:

extended LDIF

#

LDAPv3

base <uid=jllerena,ou=people,dc=inicioms,dc=com> with scope subtree

filter: (objectclass=*)

requesting: ALL

#

jllerena, People, inicioms.com

dn: uid=jllerena,ou=People,dc=inicioms,dc=com

uid: jllerena

cn: José
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword::
e2NyeXBOfSQxJGOOVzJqMkhkJHZkaURwYkZrbzQyMjFyRXpvWDBGdS4=
shadowLastChange: 13741
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 500
gidNumber: 500
homeDirectory: /home/jllerena
gecos: jose
search result
search: 2
result: 0 Success
numResponses: 2
numEntries: 1

Configurando un cliente LDAP.

El archivo de configuración del cliente ldap se encuentra en la ruta /etc/ldap.conf, en este archivo se debe definir los parámetros para el host y base con el propósito de definir hacia que servidor y que directorio conectarse, para esto caso se definirá los parámetros de igual manera que se lo hizo en el archivo de configuración del servidor en la parte de suffix, así que los valores quedaran así:

Host 192.168.47.11

Base dc=inicioms,dc=com

En la parte del host se pueden especificar varios host, los cuales deben estar separados por un espacio. En la maquina cliente se puede hacer el uso del comando *slapcat* igual que antes. La configuración normalmente permite que se lean varios

campos por cualquiera, aun si no se ve la contraseña se puede ver otra información del usuario.

Luego se configura el sistema utilizando los comandos *authconfig* para configurar por comandos, el comando *authconfig-tui* que permite hacerlo en modo de texto o el comando *authconfig-gtk* para el modo grafico.

En esta parte se utilizara el comando *authconfig-gtk* para realizar la configuración por modo grafico, lo que se pretende es habilitar las casillas de 'utilizar LDAP' y ‘utilizar autenticación LDAP’, se debe hacer clic en ‘configurar LDAP’ y verificar que los datos del servidor y del directorio a utilizar sean los correctos, es decir los datos que hemos estado utilizando (dc=inicioms,dc=com) luego de que este correcta la información se hace clic en aceptar.

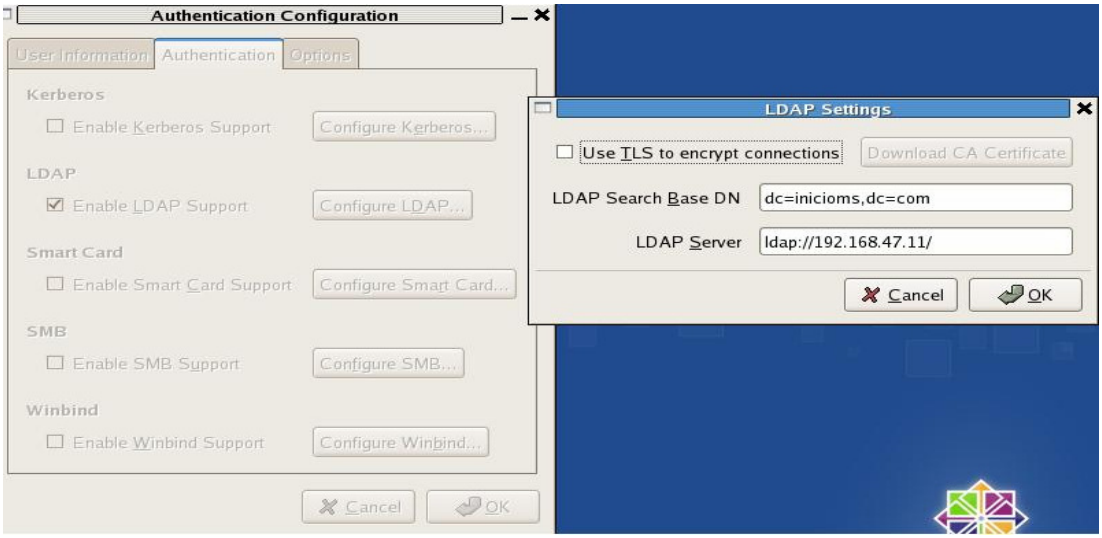

Figura 2.24: Configuración de autenticación en modo grafico

A continuación se muestra como se configura el cliente por modo texto en la que se utiliza el comando *authconfig-tui* en la cual la configuración es exactamente la misma, lo único que cambia en la configuración en modo de texto es la visualización que presenta luego de escribir el comando *authconfig-tui,* luego de hacerlo se nos presentara la ventana de configuración en modo texto.

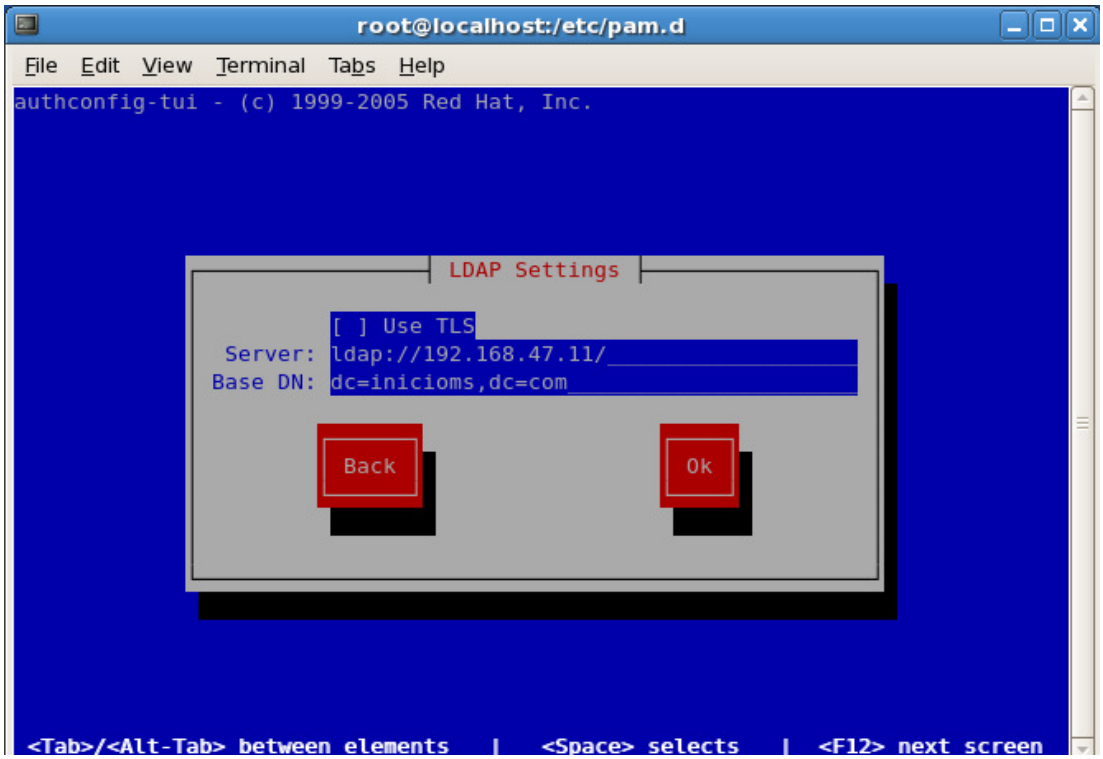

Figura 2.25: Configuración de autenticación en modo texto

Configuración de un cliente nsswitch.

Al ejecutar el comando ls –l lo que hace el sistema operativo es mostrarnos los nombres de los propietarios de los archivos existentes, lo que no se muestra es el numero de ID único que posee el usuario dado (UID). Así que los programas para poder saber el nombre que corresponde al numero de ID único del usuario, a los hosts, grupos, etc; se hacen llamados a funciones de la librería GLIBC y esta librería averigua la relación que existe entre las partes.

En el archivo nsswitch.conf que se encuentra bajo la ruta /etc/, y aquí se le especifica al sistema de donde averigua al propietario conociendo el número de ID único, el archivo contiene algo parecido a lo siguiente:

passwd: compat
group: compat
shadow: compat
hosts: files dns
networks: files

La parte mas importante de este archivo es la sección de passwd, group y shadow. Luego de las modificaciones realizadas quedara de este modo:

passwd: compat ldap
group: compat ldap
shadow: compat ldap

Por lo tanto si un programa pide a la librería GLIBC el nombre del usuario numero 950, la librería en primer lugar revisara el archivo passwd en /etc/passwd, caso contrario hará la consulta al servidor de directorios LDAP.

Para que el archivo nsswitch pueda realizar las diferentes consultas en LDAP se tendrá el archivo libnss-ldap ubicado en la ruta /etc/libnss-ldap.conf de la siguiente manera:

host 192.168.47.11
base dc=inicioms,dc=com

Esta es la información que se necesita para llegar al servidor LDAP y realizar la consulta deseada por el usuario.

Configurando el cliente PAM

Para poder configurar el cliente PAM se debe instalar el paquete libpam-ldap. Actualmente existen muchos programas que pueden usar y de hecho lo hacen un método de autentificación que es centralizado y es por módulos que son llamados PAM (Pluggable Authentication Modules). Aquellos son librerías que los programas pueden soportar y que sirven de "interfaz" contra muchos métodos de autentificación tal es el caso de LDAP.

Si se necesita tener conexión con privilegios, se puede usar la contraseña que se encuentre en la ruta /etc/ldap.secret, y que estará con permisos 700.

El contar con la contraseña para poder autentificarse es necesario utilizar la configuración por defecto del archivo de configuración del servidor slapd.conf cuando root quiere cambiar la contraseña de algún otro usuario, si la conexión no es autentificada, el servidor LDAP no permitirá cambiar la contraseña. De otra forma

cualquier usuario podría cambiar la contraseña del usuario que desee con solo lanzar la consulta al servidor LDAP.

pam-ldap supone a las cuentas del sistema como objetos los cuales tienen estos atributos: *uid* y *userPassword*. Los atributos se permiten debido a las clase objeto (objectClass) *posixAccount*.

Por lo tanto el archivo /etc/pam_ldap.conf quedara configurado de la siguiente manera:

host 192.168.47.11
base dc=inicioms,dc=com
ldap_version 3

rootbinddn cn=josellerena,dc=inicioms,dc=com
don't forget /etc/ldap.secret
A partir de este punto ya se cuenta con la configuración general de PAM para que funcione con el servidor LDAP.

SSH

El archivo que permite configurar esto esta en la ruta /etc/pam.d/sshd y se debe agregar las siguientes líneas al comienzo del archivo:
auth sufficient pam_ldap.so
account sufficient pam_ldap.so
session sufficient pam_ldap.so
password sufficient pam_ldap.so

Para que se pueda hacer la autenticación de forma correcta se debe hacer una pequeña modificación en el archivo sshd_config que esta en la ruta /etc/ssh/sshd_config, lo que se debe hacer es habilitar la autentificación PAM, puede darse el caso que ya se encuentre habilitado la autentificación PAM, pero siempre es recomendable revisar y asegurarse de esto.

SU

Aquí es posible poder ejecutar el comando su con aquellos usuarios que se encuentran están dados de alta y habilitados en el servidor LDAP.

Para poder realizar esto debemos irnos al archivo /etc/pam.d/su y se lo configurara de la siguiente manera:

```
auth       sufficient pam_rootok.so
auth       sufficient pam_ldap.so
auth       required   pam_unix.so use_first_pass

account    sufficient pam_ldap.so
account    required   pam_unix.so

session    sufficient pam_ldap.so
session    required   pam_unix.so
```

Passwd

Aquí se permite cambiar las contraseñas de los usuarios. El archivo de configuración se encuentra en la ruta /etc/pam.d/passwd La configuración se puede dejar de la siguiente manera:

```
password       sufficient      pam_ldap.so
password       required        pam_unix.so nullok obscure min=4 max=8
```

Es muy útil dar de alta a todos los usuarios de forma normal y cambiar la contraseña con el mismo passwd como root.

login

Como la gran mayoría de los archivos, este archivo se encuentra en la misma ruta que los otros archivos descritos anteriormente, es decir en /etc/pam.d/login, y la configuración se la puede dejar de la siguiente manera:

```
auth       required      pam_nologin.so
auth       sufficient    pam_ldap.so
auth       sufficient    pam_unix.so shadow use_first_pass
auth       required      pam_deny.so
```

Hay otras formas en las que se puede configurar este archivo, pero se debe tener bastante cuidado con la línea use_first_pass, caso contrario si no se escribe esa línea los usuarios que están habilitados en el servidor LDAP serian requerido doblemente la solicitud de contraseña, la una se validaría con /etc/passwd, y al no ser encontrado este usuario pediría nuevamente la contraseña para validarlo contra LDAP.

De igual manera es fácil modificar los archivos common-account common-auth common-password common-session, con esto no se toca el archivo para cada servicio.

Algo recomendable de hacer es contar con certificados y así no habrá nadie que sea capaz de reemplazar al servidor. Con esto la información circula de una manera segura. Esto se hace todavía mas si el cliente LDAP y el servidor LDAP no se encuentran en la misma red. Una forma de hacer eso es por medio de freeswan la cual es una implementación de IPSEC.

Un caso común que ocurre es el hecho de migrar a los usuarios con los cuales ya se cuentan en el sistema a OpenLDAP. Esto se puede conseguir con el paquete de migrationtools.

Otro paquete útil con el que se debe contar es nscd. Este paquete hace de caché para OpenLDAP en una máquina local. Así al ejecutar el comando "ls -l" el sistema preguntara al servidor LDAP el nombre de cada ID de usuario único que tiene dentro del sistema.

Softerra LDAP Browser/Editor 2.6.

En esta aplicación para habilitar la autentificación de usuario se debe deshabilitar la casilla de usuario anónimo para ingresar la información del mismo, el nombre distintivo debe ser el mismo que el o los que están definidos en el archivo de configuración del servidor LDAP (*/etc/openldap/slapd.conf*). Tanto el archivo de configuración del servidor al igual que el del cliente deben estar configurados correctamente para que pueda conectarse la aplicación correctamente al servidor LDAP.

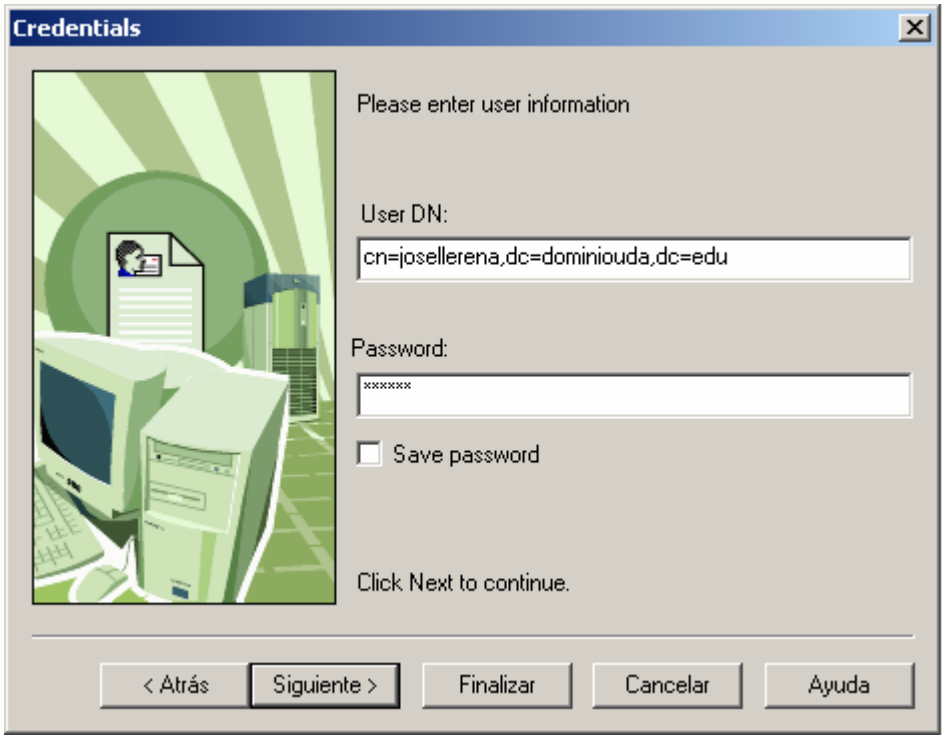

Figura 2.26: Autentificación de usuario en LDAP Browser/Editor 2.6

Una vez ingresado el *password* correctamente el usuario tendrá el acceso al directorio.

2.5 Configuración de LDAP con soporte SSL-TLS

Lo que hace comenzar una operación de inicio TLS en un servidor LDAP es lo que establece la comunicación TLS (Transport Layer Security, o Seguridad para Nivel de Transporte en español) por medio de un mismo puerto que es el numero 389 por vía TCP. Permite contar con privacidad en la transportación de datos y cuida de la integridad de los datos.

Cuando ocurre la negociación, el servidor envía su certificado con una estructura X.509 para poder verificar su identidad. Adicionalmente es posible que establezca comunicación. Cuando una conexión da lugar en el puerto 389 y 636 radica su diferencia en lo siguiente:

Cuando ocurre la conexión por medio del puerto 636, tanto el cliente como el servidor establecen el TLS antes de que se de una transferencia de cualquier otro

dato, sin la necesidad de utilizar la operación StatTLS. así que la conexión a través del puerto 636 debe de terminarse al cerrar TLS.

También existe un algoritmo para poder realizar cifrados de claves publicas que salio por primera vez en 1977, mas conocido por RSA debido al apellido de sus creadores. Su principal uso que es en todo el mundo es para protocolos que son destinados en lo que es el comercio electrónico.

En el segundo párrafo de este punto se menciono el X.509 que es un estándar de la ITU-T (estandarización de Telecomunicaciones de la Internacional Telecommunication Union) para lo que es infraestructura de claves publicas, lo que hace es establecer estándares para sacar certificados de claves públicas y a su vez genera algoritmos para validar rutas de certificación, se encarga de hacer la verificación de rutas validas de un certificado y que sea válida bajo una infraestructura de una clave pública determinada; es decir, a partir de un certificado inicial, pasando por medio de certificados intermedios hasta llegar a un certificado de confianza que es emitido por una Autoridad Certificadora (CA, o Certification Authority).

Una implementación que tiene relación con el soporte TLS-SSL es OpenSSL, que como cualquier programa de Linux es de código abierto, proviene de los protocolos SSL (secure sockets layer o nivel de zócalo seguro) y también TLS (transport layer security, o seguridad para nivel de transporte en español).

Procedimientos para la configuración con soporte TLS-SSL.

En primer lugar lo que se debe hacer es generar la clave y el certificado, para esto se debe ir hacia la ruta /etc/openldap/cacerts.

La creación de la llave y el certificado para OpenLDAP requiere utilizar una clave que contenga un algoritmo RSA de 1024 octetos y estructura x509. Como ejemplo se hará una validez por 731 días (dos años) para el certificado que crearemos.

openssl req -x509 -nodes -newkey rsa:1024 -days 731 -out slapd.crt -keyout slapd.key

El ingresar el comando anterior nos solicitara el ingreso de algunos datos, estos son los siguientes:

- País: Con un máximo de dos letras de largo, por lo tanto el ingreso es de la abreviación del país.
- Estado o Provincia: El nombre completo de la provincia o del estado.
- Ciudad o localidad: De igual manera el nombre completo de la ciudad o localidad.
- Nombre de la compañía u organización: Nombre completo de la organización.
- Nombre de la unidad organizacional o sección: Nombre de la sección o departamento de la organización.
- Nombre común, es decir el nombre de uno o el host del servidor.
- Dirección de correo electrónico.

Luego de haber ingresado el comando req lo que nos muestra como salida es lo siguiente:

Generating a 1024 bit RSA private key

.....++++++

…….++++++

writing new private key to 'slapd.key'

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) [GB]:Ec

State or Province Name (full name) [Berkshire]: Azuay

Locality Name (eg, city) [Newbury]: Cuenca

Organization Name (eg, company) [My Company Ltd]: Casa Llerena

Organizational Unit Name (eg, section) []: Ventas

Common Name (eg, your name or your server's hostname) []: inicioms.com

Email Address []: josellerena@inicioms.com

En el siguiente grafico se puede ver lo escrito recientemente:

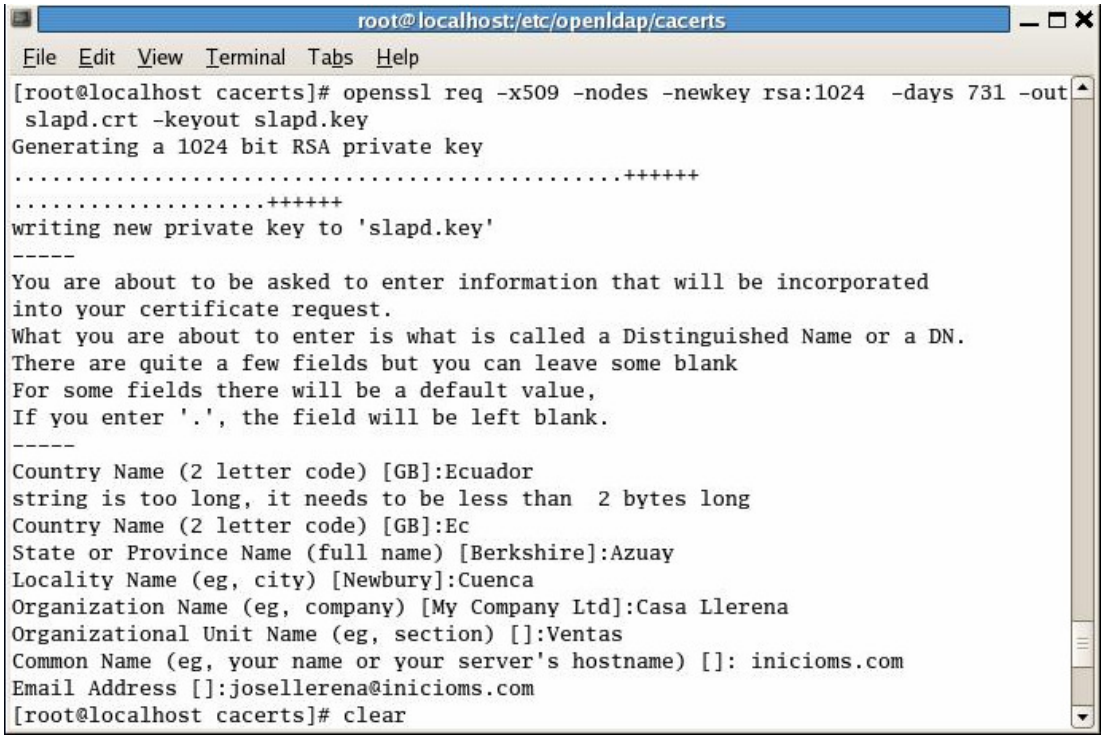

Figura 2.27: Generación de un certificado TLS-SSL

El certificado no solamente es válido cuando el servidor LDAP sea llamado con el nombre que es definido en el campo Common Name; es decir, solo se puede usar cuando se define inicioms.com como servidor LDAP con soporte SSL/TLS. No va a funcionar si se llama al servidor con otro nombre diferente por ejemplo libreta.dominiopublico.edu.ec.

Es de suma importancia que todos los archivos relacionados con las claves y certificados sean otorgados permisos de acceso de solo lectura para los usuarios en general, en nuestro caso se dará permiso de solo lectura al usuario jllerena, se lo hará de esta manera:

chown jllerena /etc/openldap/cacerts/slapd.*

chmod 400 /etc/openldap/cacerts/slapd.*

Además de lo que se ha realizado es necesario marcar ciertos parámetros en el archivo de configuración del servidor (etc/openldap/slapd.conf). Lo que se tiene que hacer es en este archivo descomentar los parámetros TLSCACertificateFile,

TLSCertificateFile y TLSCertificateKeyFile y a su vez establecer las rutas en donde se encuentran los certificados y claves. También hay la opción de poder descomentar la directiva de referencia para indicar el URI (Uniform Resource Identifier o Identificador Uniforme de Recursos en español) del servicio de directorio superior como ldaps en lugar de ldap. A continuación se muestra como quedan las líneas al hacer lo que se ha comentado:

TLSCACertificateFile /etc/openldap/cacerts/slapd.crt

TLSCertificateFile /etc/openldap/cacerts/slapd.crt

TLSCertificateKeyFile /etc/openldap/cacerts/slapd.key

referralldaps://inicioms.com

Además si se desea que el cliente necesite autenticación se debe descomentar la siguiente línea:

TLSVerifyClient Demand

Si el caso es el opuesto la línea iría de esta manera:

TLSVerifyClient Never

Esto no es esencial ya que con borrar esa línea no pide al cliente autentificación.

Luego de haber realizado todo esto, se debe reiniciar el servicio (service ldap restart) para que los cambios que hemos realizado en todo este tiempo sufran los cambios debidos y que hemos hecho.

La directiva TLSCACertificateFile lo que hace es especificar el archivo de tipo PEM que tiene los certificados para CA (certificate autorization o autorización de certificado) que el servidor confiara. El certificado para el CA que firmo el certificado del servidor tiene que ser incluido entre aquellos certificados del archivo de configuración del servidor. Si el CA firmante no es un CA de alto nivel (para eso debe trabajarse con el usuario root), certifica para la secuencia entera del CA que firma hacia el CA de alto nivel.

La directiva TLSCertificateFile especifica al archivo que contiene el certificado del servidor *slapd.* Los certificados son por lo general información publica y no requieren de una protección especial.

La directiva TLSCertificateKeyFile especifica al archivo que tiene la llave privada que concuerda con la certificada que esta guardada en el archivo TLSCertificateFile. Las llaves privadas son datos sensibles y son normalmente encriptadas para protección, pero la implementación actual no tiene el soporte de llaves encriptadas, por lo tanto las claves no se han encriptado así que el archivo debe mantenerse con mucho cuidado. Además de estas directivas que se han mencionado se cuentan con otras que son las siguientes:

TLSCACertificatePath <ruta>: Esta directiva especifica la ruta que tiene certificados de CA en archivos separados, a este directorio se debe manejar especialmente usando el utilitario OpenSSL *c_rehash,* este es usado para generar enlaces simbólicos, esta opción solo puede usarse con un sistema de archivos que tenga soporte de enlaces simbólicos, en todo caso es mucho mas sencillo utilizar la directiva TLSCACertificateFile.

TLSCipherSuite <espec-cipher-suite > Esta directiva configura los cifrados que serán aceptados y el orden preferencial, la especificación **<espec-cipher-suite >** debe ser precisamente una especificación de cifrado para OpenSSL, se puede usar para ello el siguiente comando:

```
openssl ciphers -v ALL
```

Con esto se obtiene una lista de varias especificaciones de cifrados. Además de los nombres de cifrados individuales, los especificadores HIGH, MEDIUM, LOW, EXPORT, y EXPORT40 pueden ser útiles con TLSv1, SSLv3 y SSLv2.

TLSRandFile <nombre del archivo> La directiva TLSRandFile especifica el archivo del cual se obtendrán bits randómicos cuando no este disponible la ruta /dev/urandom. Si el sistema provee esta ruta, entonces esta opción no será necesaria caso contrario una fuente de datos randómicos debe ser configurado. Algunos sistemas Linux lo proveen por defecto mientras otros caso de Solaris, requieren la instalación de un parche que lo pueda proveer, y otros sistemas no lo soportan del todo, siendo el caso que se necesite los archivos EGD o PRNGD deben instalarse, y esta directiva debe especificar el nombre de los sockets EGD/PRNGD. La variable ambiental RANDFILE se puede usar también para especificar el nombre del archivo. también en la ausencia de estas opciones, el archivo con extensión .rnd en el

directorio base del usuario con slapd puede ser usado si es que existe. Para usar el archivo .rnd solo se debe crear el archivo y copiar unos cuantos centenares de bytes de datos arbitrarios en el archivo, este archivo solo se usa para proveer una semilla para el generador de número pseudo-randómico, y no necesita muchos datos para poder funcionar.

TLSEphemeralDHParamFile <nombre del archivo> Esta directiva especifica el archivo que contiene parámetros para intercambio de llaves. Esto es requerido para usar un certificado DSA en el lado del servidor (TLSCertificateKeyFile apunta a la llave DSA). Varios grupos de parámetros pueden ser incluidos en el archivo, todos estos serán procesados. Los parámetros pueden ser generados usando el siguiente comando:

openssl dhparam [-dsaparam] -out <archivo> <numbits>

TLSVerifyClient { never | allow | try | demand } Esta directiva cuenta con cuatro opciones que son nunca, permitir, intentar y demanda, especifica que se revisa para hacer certificados de clientes en una sesión TLS entrante. Esta opción tiene el valor de 'nunca' por defecto, en tal caso el servidor nunca pregunta al cliente por un certificado. Con la opción de 'permitir' el servidor solicita un certificado de cliente, si tal no es provista, la sesión procede normalmente. Si un certificado es entregado y el servidor no puede verificar, entonces dicho certificado es ignorado y la sesión procede normalmente como si nunca se hubiera dotado de un certificado.

Con la opción de 'intento' el certificado es requerido y si no es provisto, la sesión inicia de manera normal. Si es provisto y no puede verificar la sesión es terminada inmediatamente.

Con la opción de demanda el certificado es requerido y un certificado valido debe ser provisto, caso contrario la sesión termina.
El servidor debe pedir un certificado al cliente en orden de usar el mecanismo de autentificación externa SASL con una sesión TLS.

Además del servidor, el archivo de configuración del cliente cuenta con directivas que son paralelas con las del servidor. Los nombres son diferentes y van en el

archivo *ldap.conf,* y no en *slapd.conf,* aunque su funcionalidad es en su mayoría la misma.
Entre las directivas de cliente se cuentan con las siguientes:

TLS_CACERT <nombre de archivo > Es el equivalente a la opcion de servidor TLSCACertificateFile. Como nota se menciona que un cliente necesitaría conocer más de certificados de autentificación que un servidor.

TLS_CACERTDIR <ruta> Es el equivalente a la opcion del servidor TLSCACertificatePath. Igualmente el directorio especificado debe ser manejado con la utilidad de OpenSSL *c_rehash.*

TLS_CERT <nombre de archivo> Esta directiva lo que hace es especificar el archivo que contiene el certificado del cliente. Este es una directiva solamente de usuario y solamente puede ser especificado en un archivo de usuario *.ldaprc*

TLS_KEY <nombre de archivo> La directiva TLS_KEY específica el archivo que contiene la llave privada que concuerda con el certificado guardado en el archivo TLS_CERT**.** Los mismos criterios que se han mencionado para la opcion TLSCertificateKeyFile. Este es también una directiva solamente de usuario.

TLS_RANDFILE <nombre de archivo> Esta directiva es la misma de la directiva del servidor TLSRandFile.

TLS_REQCERT { never | allow | try | demand } Esta directiva es la equivalente a la opcion del servidor TLSVerifyClient. En esta opción, para los clientes el valor por defecto es 'demanda' (demand) y en lo general no hay un motivo razonable para lo cual se debería cambiar esta opción.

Para que sea posible configurar cualquier cliente LDAP con el soporte SSL, se lo debe hacer con el puerto 636 después de aceptar el certificado, si se da el caso de que éste no tenga una firma de un RA (Registration **A**uthority o Autoridad de Registro), el servidor LDAP debe permitir que se complete la conexión y realizar cualquier tipo de consulta y/o manipulación de registros.

Si se tiene activado el firewall, además del puerto 389 de TCP, se debe abrir el puerto 636 por TCP (LDAPS), en el archivo de configuración de cliente se especifica

los puertos a utilizar, ambos puertos pueden ser utilizados para trabajar con el soporte TLS-SSL.

2.6 Creación y pruebas de un directorio

Para la creación del directorio se tomara en cuenta el uso de una empresa como ejemplo, con sus diferentes departamentos y jerarquías, con los diferentes cargos que tiene una empresa y los nombres de los empleados que ocupan cada uno de los cargos. Como dato adicional el servidor esta configurado con soporte TLS-SSL lo cual se realizo en el punto anterior.

El primer paso a realizar es el de definir ciertos atributos que serán utilizados para la creación del directorio para eso editamos el siguiente archivo:
/etc/openldap/schema/core.schema

En este archivo añadiremos los siguientes atributos que necesitaremos para el propósito, estos atributos son los siguientes:

- Nombre completo: a utilizarse en el rootdn del archivo de configuración del servidor.
- Apellido
- Nombre
- Cedula de identidad
- dirección
- teléfono
- Cargo
- Departamento
- Jefe o supervisor
- Salario que percibe
- Estado Civil
- Nombre de la Empresa

En el siguiente grafico se puede apreciar como se definen estos atributos dentro del archivo core.schema:

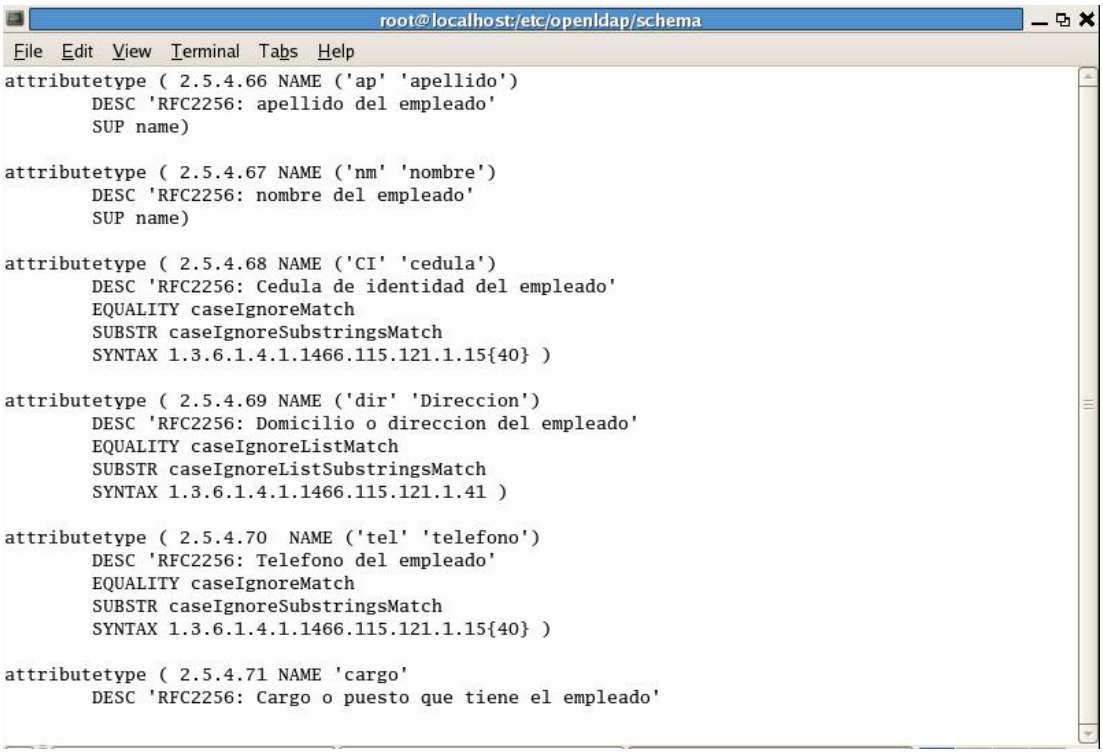

Figura 2.28: El archivo /etc/openldap/schema/core.schema

De acorde a lo que se ve en el grafico, en la definición de los atributos en la primera línea lo que se ve es el número de identificación único del atributo (2.5.4.67 usado para definir el atributo “nombre”) y luego se asigna un nombre a esa variable.

En la segunda línea se describe al atributo. A partir de la siguiente línea se detallan características que tengan los atributos. En el caso del atributo 2.5.4.69 perteneciente al atributo “dirección” se usan las líneas “EQUALITY caseIgnoreMatch” y “SUBSTR caseIgnoreSubstringsMatch” para permitir el ingreso de caracteres y números.

Además de los atributos también se van a definir dos objetos que se van a utilizar para poder usarlos en el momento de ingresar los datos, estos objetos serán los siguientes:

- Departamentos
- Empresa

Las características que tienen estos dos objetos que se van a utilizar en el directorio se ven en el siguiente grafico:

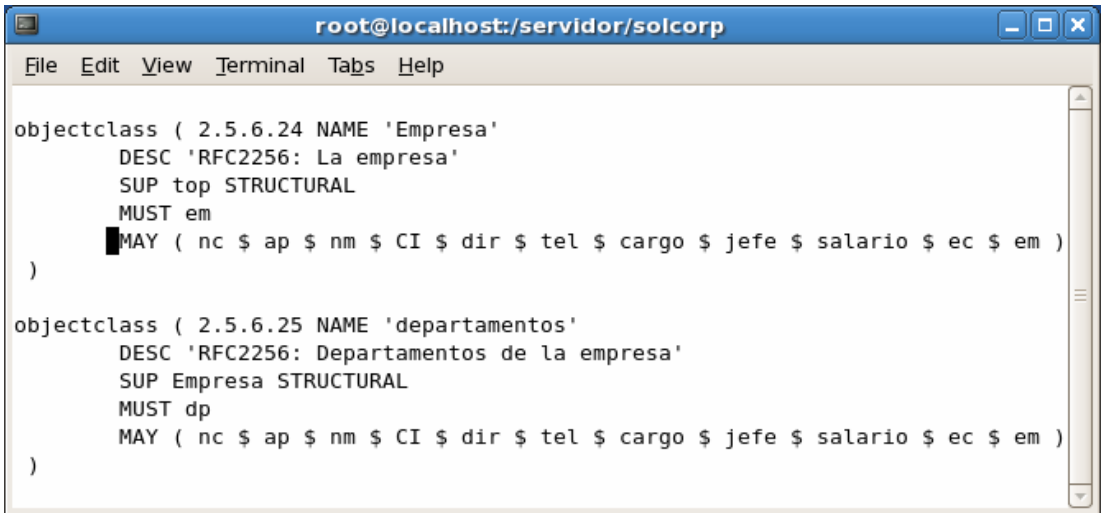

Figura 2.29: Definición de objetos en el archivo core.schema

Luego como se ha realizado anteriormente se definirá un nuevo directorio para la empresa en cuestión de la manera siguiente dentro del archivo *slapd.conf* se agrega la nueva información que se usara para el directorio:

Database	bdb
Suffix	“dc=SolCorp,dc=sc”
Rootdn	“nc=jllerena,dc=SolCorp,dc=sc”
Rootpw	secret
Directory	/var/lib/ldap
Index	dp,nc,mail,apellido,nombre

Las otras líneas de index van de la misma manera que han ido en las otras definiciones de directorios. En las líneas 2 y 3 donde se define el suffix y el rootdn, las siglas sc que es parte del dominio es la abreviación de SolCorp (sc).

Se debe reiniciar el servicio LDAP para que los cambios tengan efecto (*service ldap restart*). También se creara un directorio en donde se guardara todos los archivos relacionados con este directorio, y se dará permisos al usuario root.

Mkdir /servidor/solcorp

Chmod 700 /servidor/solcorp

Se procederá a crear un archivo que se llamara solcorp.ldif que tendrá los datos sobre el directorio y en donde ira la información de cada uno de los empleados de la empresa.

dn: dc=SolCorp, dc=sc
objectclass: top
objectclass: dcObject
objectclass: Empresa
em: Sol Corp
dc: SolCorp

dn: dp=sistemas, dc=SolCorp, dc=sc
dp: sistemas
objectClass: top
objectClass: departamentos

dn: dp=finanzas, dc=SolCorp, dc=sc
dp: finanzas
objectClass: top
objectClass: departamentos

dn: dp=administración, dc=SolCorp, dc=sc
dp: administración
objectClass: top
objectClass: departamentos

Con estos datos ya ingresados en el archivo solcorp.ldif se puede hacer la inserción de datos en el servidor.

Ldapadd –x –w secret –D ‘nc=jllerena,dc=SolCorp,dc=sc’ –f solcorp.ldif

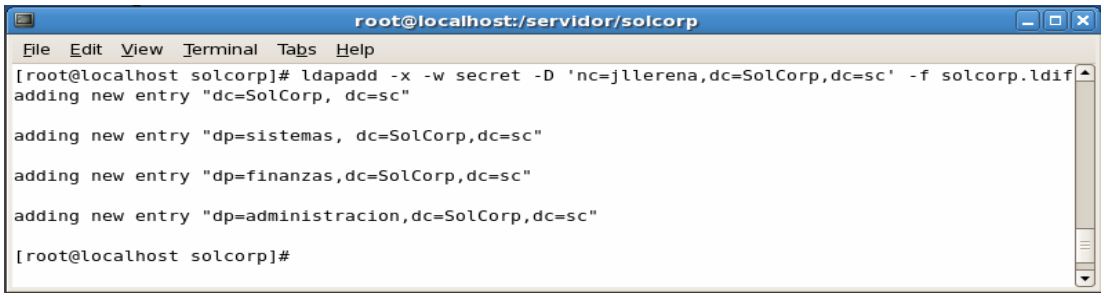

Figura 2.30: Ingreso de los datos de SolCorp en el servidor

El siguiente paso es ingresar la información de todos los empleados de la empresa al directorio que se ha creado recientemente, a manera habitual, se creara otro archivo ldif que contendrá toda la información de los empleados, se lo llamara *empleadossolcorp.ldif*.

Entre algunos de los datos que contendrá este archivo son los que se muestran a continuación y la manera en la que irán definidos van de la siguiente manera:

Dn: nc= Juan Andrés Vélez, dp=Sistemas, dc=SolCorp,dc=sc

objecClass: top

objectClass: person

objectClass: Empresa

objectClass: Departamentos

nc: Juan Andres Vélez

ap: Vélez

nm: Juan Andres

CI: 0374832918

Dir: Av Elia Liut

Tel: 2845023

Cargo: Técnico de computadoras

Dp: Sistemas

Jefe: Juan Veira

Salario: 400

Ec: Soltero

Em: SolCorp

Cada registro va separado por medio de un espacio en blanco y se repite las mismas sentencias con la información del siguiente empleado. De manera idéntica se hará el ingreso de datos con el comando *ldapadd* e ingresara todos los registros que hayamos ingresado en el archivo *empleadossolcorp.ldif.*

Asumiendo que se desea ver la lista de todos los empleados de la empresa, para ello se hace una búsqueda general con el comando *ldapsearch,* la sintaxis iría de la siguiente manera:
Ldapsearch –x –b dc=SolCorp,dc=sc –LLL "(em=SolCorp)"

La opcion –LLL se usa para que nos muestre el resultado de la búsqueda, o sino si se desea averiguar la dirección y teléfono del empleado Malo se puede hacer una búsqueda mas especifica usando filtros.
Ldapsearch –x –b dc=SolCorp,dc=sc –LLL "(ap=Malo) dir tel

Los atributos dir y tel se escriben al final de la línea de comando, así se hace la filtración de la búsqueda y en el resultado solo nos mostrara esa información.

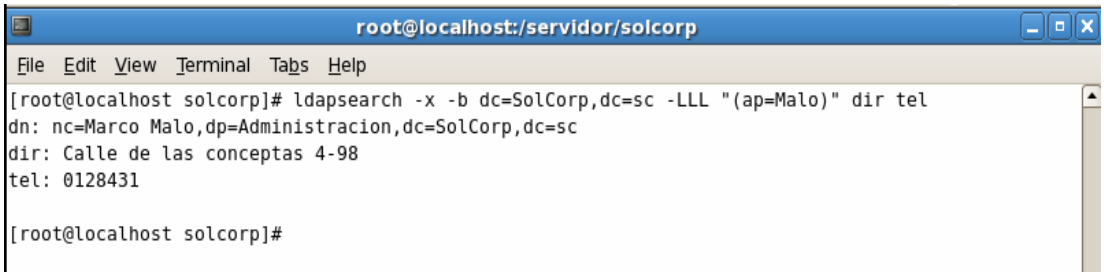

Figura 2.31: Búsqueda de dirección y teléfono del empleado Marco Malo

Si la empresa toma la decisión de contratar a un nuevo empleado y se desea actualizar el directorio LDAP, lo único que se debe hacer para actualizar el directorio es creando una nueva ficha de este empleado, se lo hace tal y como se muestra en la pagina anterior, se lo guarda en un nuevo archivo ldif que se llamara *nuevoempleado.ldif*.

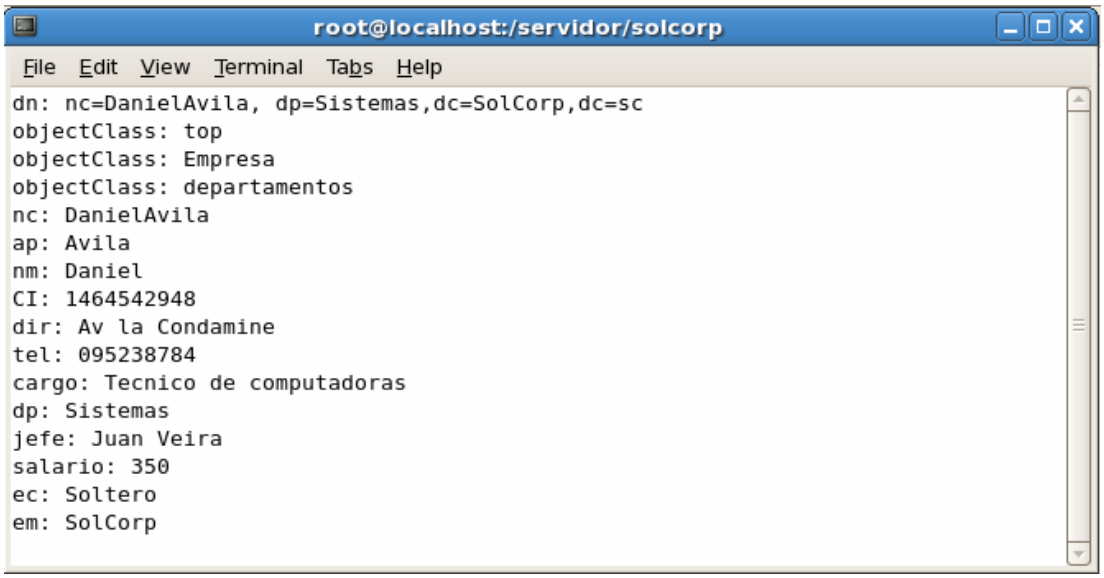

Figura 2.32: Archivo *nuevoempleado.ldif*

Luego con el comando habitual se hace el ingreso del nuevo empleado en el directorio.

Ldapadd –x –w secret –D 'nc=jllerena,dc=SolCorp,dc=com' –f nuevoempleado.ldif

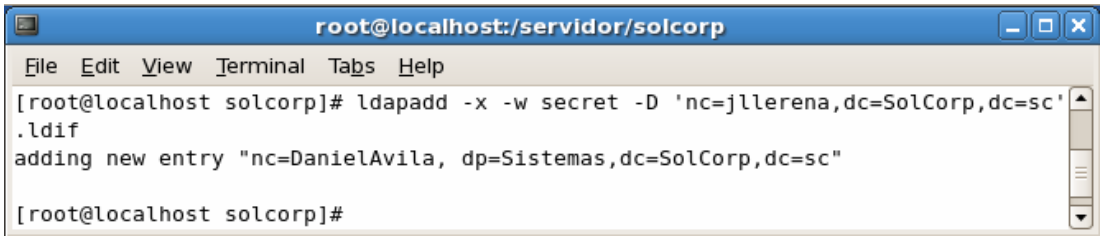

Figura 2.33: Ingreso de la información del nuevo empleado en el directorio

El directorio mantendrá actualizándose a medida que vayan ocurriendo cambios dentro de la empresa, por ejemplo si ocurriera la situación que el gerente de Sistemas renunciara a su cargo habría que remover su ficha del directorio, se lo hará con el comando *ldapdelete* de la siguiente manera.

Ldapdelete –x –D nc=jllerena,dc=SolCorp,dc=sc –w secret "nc=Juan Veira,dp=Sistemas,dc=SolCorp,dc=com".

La parte de la sintaxis que va entre comillas, se lo hace debido a que si no lleva las comillas dará un mensaje de error debido a que dentro de nc=Juan Veira se encuentra un espacio y LDAP no toma el nombre completo sino solamente lo tomara como

nc=Juan, si el nombre no se encuentra separado por medio de espacios no será necesario el uso de comillas.

Y al asignar el cargo vacante a un empleado del mismo departamento se deberá hacer modificaciones en su ficha, para poder modificar los datos de un directorio se debe crear un archivo con extensión .ldif que contendrá los datos a ser modificados, se llamara *cambios.ldif*. El archivo va estructurado de la siguiente manera:

```
dn: nc=Juan Andrés Velez,dp=Sistemas,dc=SolCorp,dc=sc
changetype: modify
replace: cargo
cargo: Desarrollador Web

dn: nc=Mauricio Alvarez,dp=Sistemas,dc=SolCorp,dc=sc
changetype: modify
replace: cargo
cargo: Gerente de Sistemas

dn: nc=Juan Andrés Velez,dp=Sistemas,dc=SolCorp,dc=sc
changetype: modify
replace: jefe
jefe: Mauricio Álvarez

dn: nc=Mauricio Alvarez,dp=Sistemas,dc=SolCorp,dc=sc
changetype: modify
replace: jefe
jefe: José Llerena

dn: nc=DanielAvila,dp=Sistemas,dc=SolCorp,dc=sc
changetype: modify
replace: jefe
jefe: Mauricio Álvarez

dn: nc=Mauricio Alvarez,dp=Sistemas,dc=SolCorp,dc=sc
changetype: modify
```

replace: salario
salario: 550

dn: nc=Juan Andres Velez,dp=Sistemas,dc=SolCorp,dc=sc
changetype: modify
replace: salario
salario: 500

Cuando se termina de editar el archivo se ejecuta el comando *ldapmodify* con el fin de realizar los cambios que se pretenden hacer, la sentencia es la misma que de agregado.
Ldapmodify –x –w secret –D 'nc=jllerena,dc=SolCorp,dc=sc' –f cambios.ldif

Los datos modificados pueden comprobarse usando una búsqueda con el fin de ver los cambios realizados, se lo hace con el comando *ldapsearch* de la manera siguiente:
Ldapsearch –x –b dc=SolCorp,dc=sc –LLL dp=sistemas nm ap dir tel cargo salario dp jefe ec CI

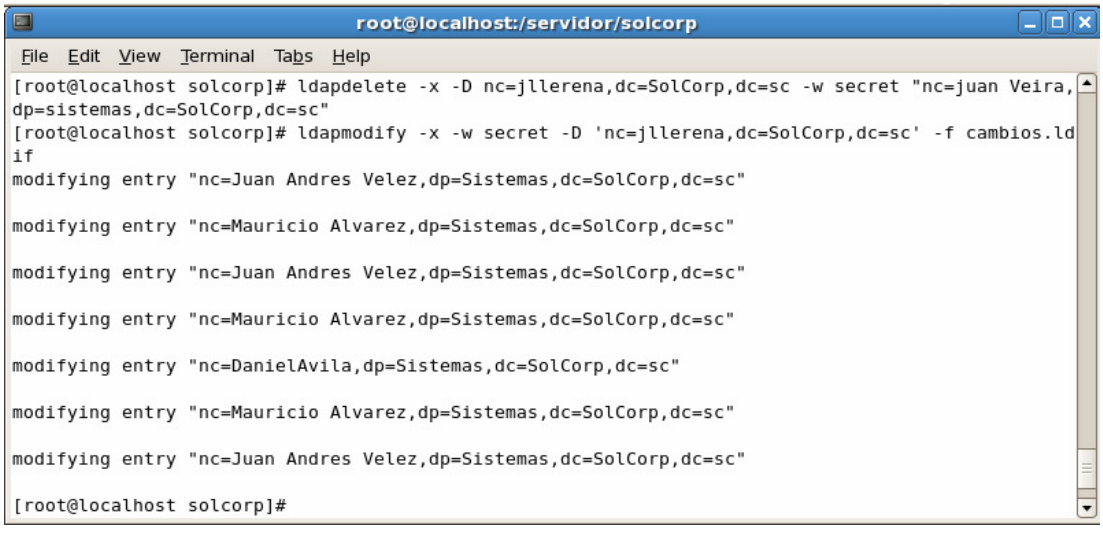

Figura 2.34: Eliminación y modificación de registros

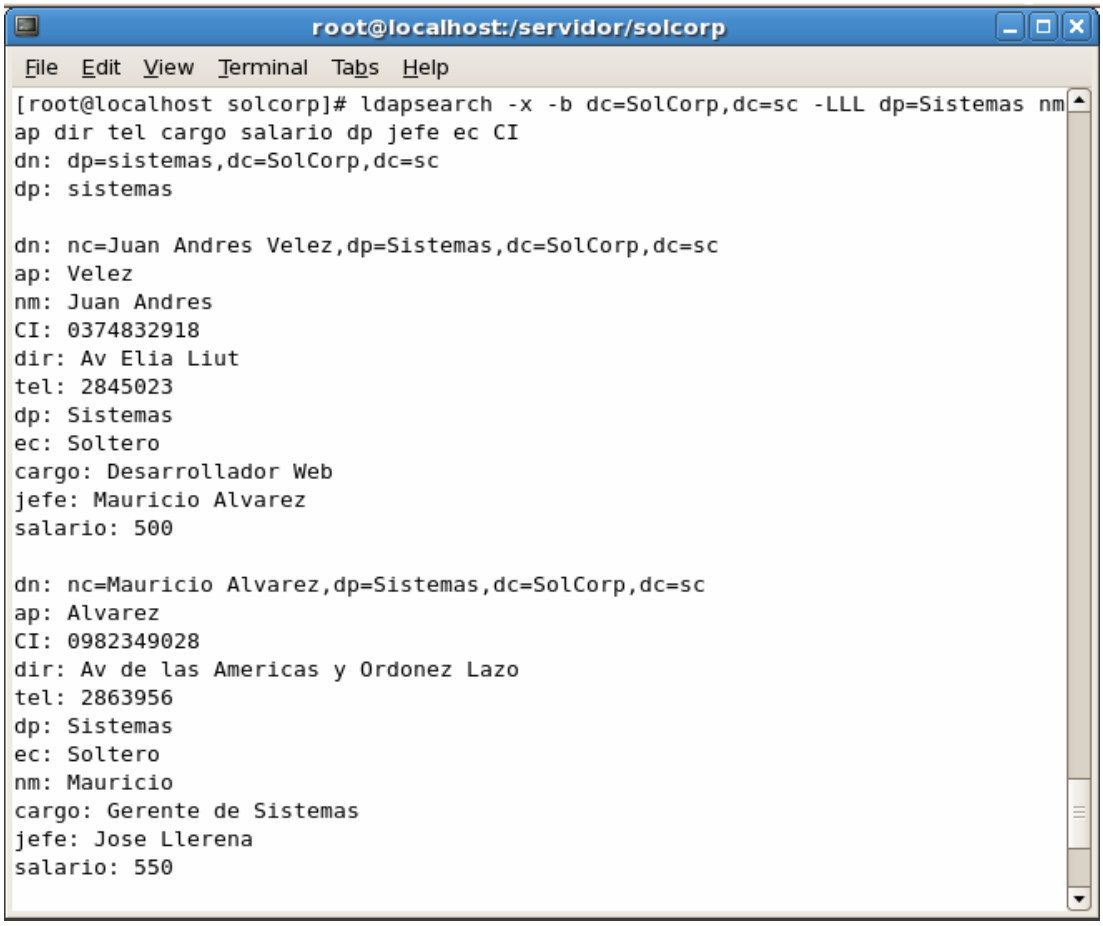

Figura 2.35: Búsqueda de empleados del departamento de Sistemas

Los datos que han sido modificados se muestran en las ultimas líneas de la ficha, la opcion –LLL hace que la ficha se muestre de manera idéntica a un archivo LDIF, y el detallar los atributos al final permite la visualización de esos atributos en el registro del directorio.

Manejo del directorio por medio de un administrador Windows.

Para manejo del directorio con un cliente Windows se utilizara el programa *Softerra LDAP Administrator 3.4*, su configuración de autentificación e información del servidor es de la misma manera que se vio en los puntos 2.3 y 2.4 con el programa *LDAP Browser/Editor 2.6*, el cual solo permite visualizar la información que esta en un directorio mientras que en este programa administrador tiene mayores funciones, las cuales permite trabajar con el directorio ya sea agregando entradas o atributos, crear un nuevo directorio, modificar y eliminar entradas o atributos, una visión general del directorio en este programa se muestra en el grafico que esta a continuación:

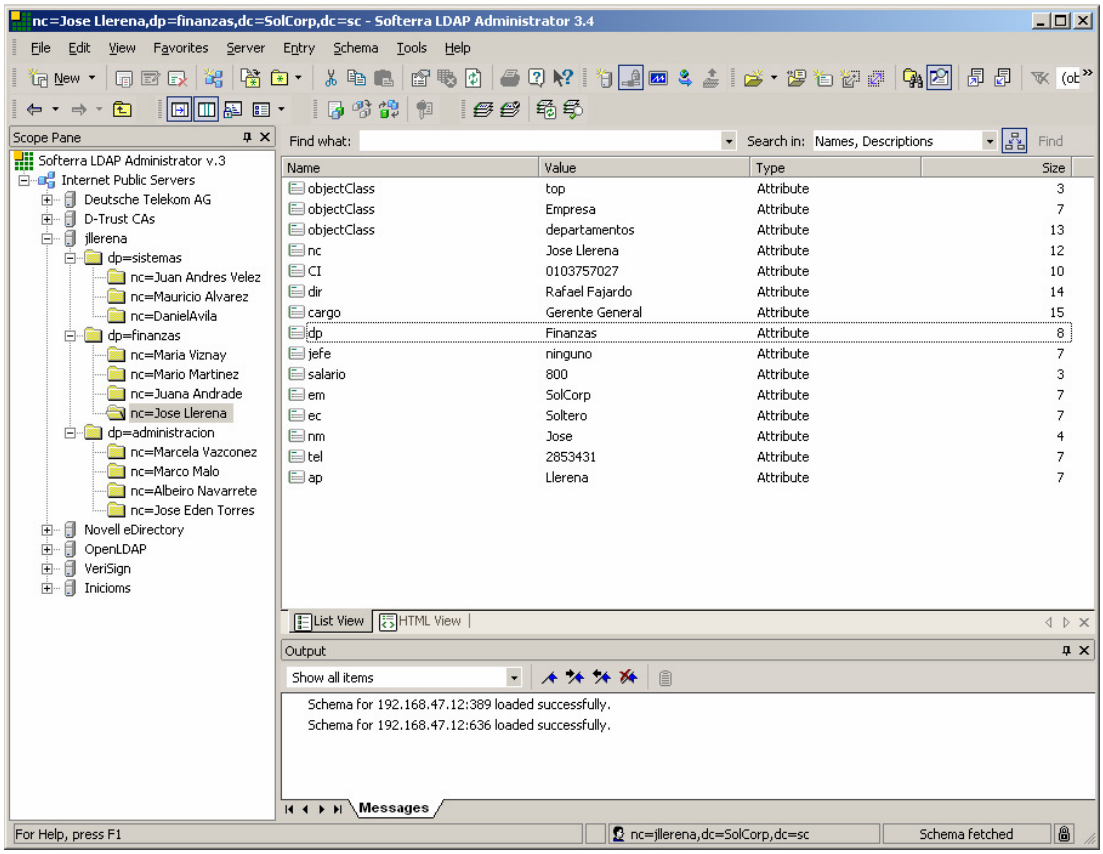

Figura 2.36: visión general del cliente Windows LDAP administrador 3.4

Si se desea crear un nuevo registro en el directorio, se sitúa en el departamento donde se desea que este el nuevo registro, con clic derecho se va a la primera opción que dice *new* y luego se selecciona *new entry*, también se puede crear un nuevo atributo, pero este debe crearse dentro de una entrada, si se lo intenta crear dentro de la rama de departamentos, dará error de violación de objeto, debido a que se lo debe hacer dentro de la parte de la estructura jerárquica debida que debe estar de acorde con el árbol jerárquico. Dentro de la rama dp=departamento se deben crear entradas enteras, por lo tanto dentro de cada entrada (nc=nombre completo) es donde se puede crear o agregar nuevos atributos al directorio, los atributos deben ser permitidos por las clases objetos correspondientes, si se desea agregar otro atributo aparte, se debe ir a la opción de *Entry* en la barra de herramientas y situarse en la opción de agregar o quitar clases objetos.

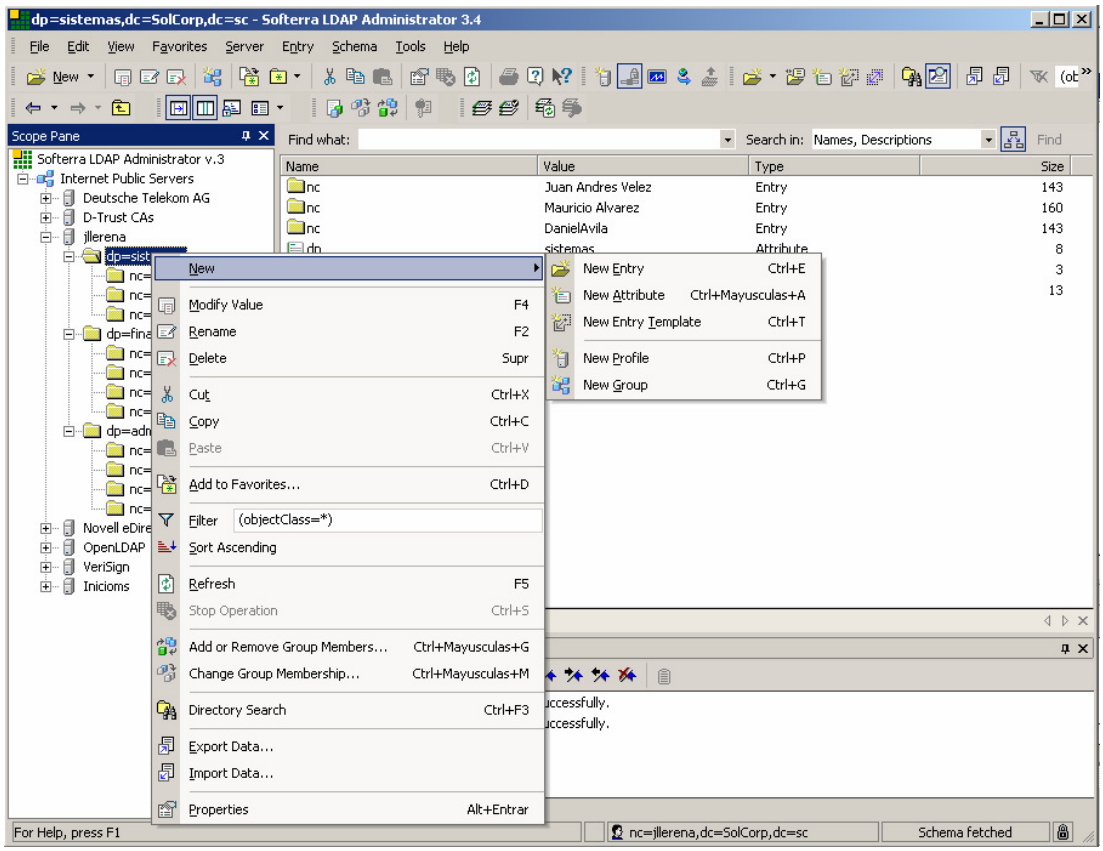

Figura 2.37: Visualización de opciones en el cliente Windows LDAP Administrator

Para poder crear una nueva entrada se debe seguir los pasos del asistente. En la primera ventana para el propósito se selecciona la opción de entrada basada en esquema. En la siguiente ventana se selecciona los objetos clase que utilizaremos para el nuevo registro, debe incluir un objeto abstracto, para el caso se utilizara el objeto *top,* luego se debe seleccionar los objetos estructurales del cual va a ser parte la entrada que será creada. En la siguiente ventana se selecciona un nombre distintivo relativo, se pueden utilizar hasta 6 atributos para utilizarlos como nombre distintivo relativo, para el ejemplo se utilizara solo el atributo nc (nombre completo), en el programa el nombre distintivo relativo se muestra en la carpeta principal de la entrada.

Figura 2.38: Indicación de un nombre distintivo relativo

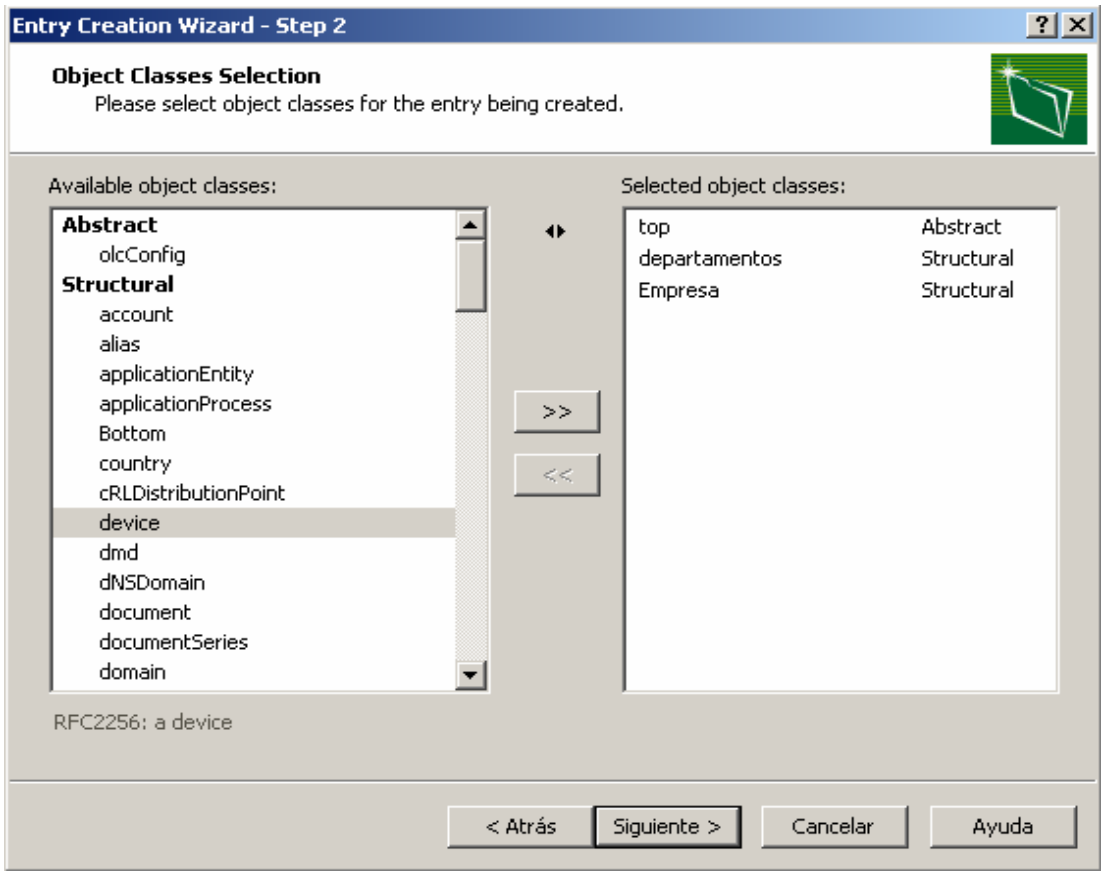

Figura 2.39: Selección de clases objeto.

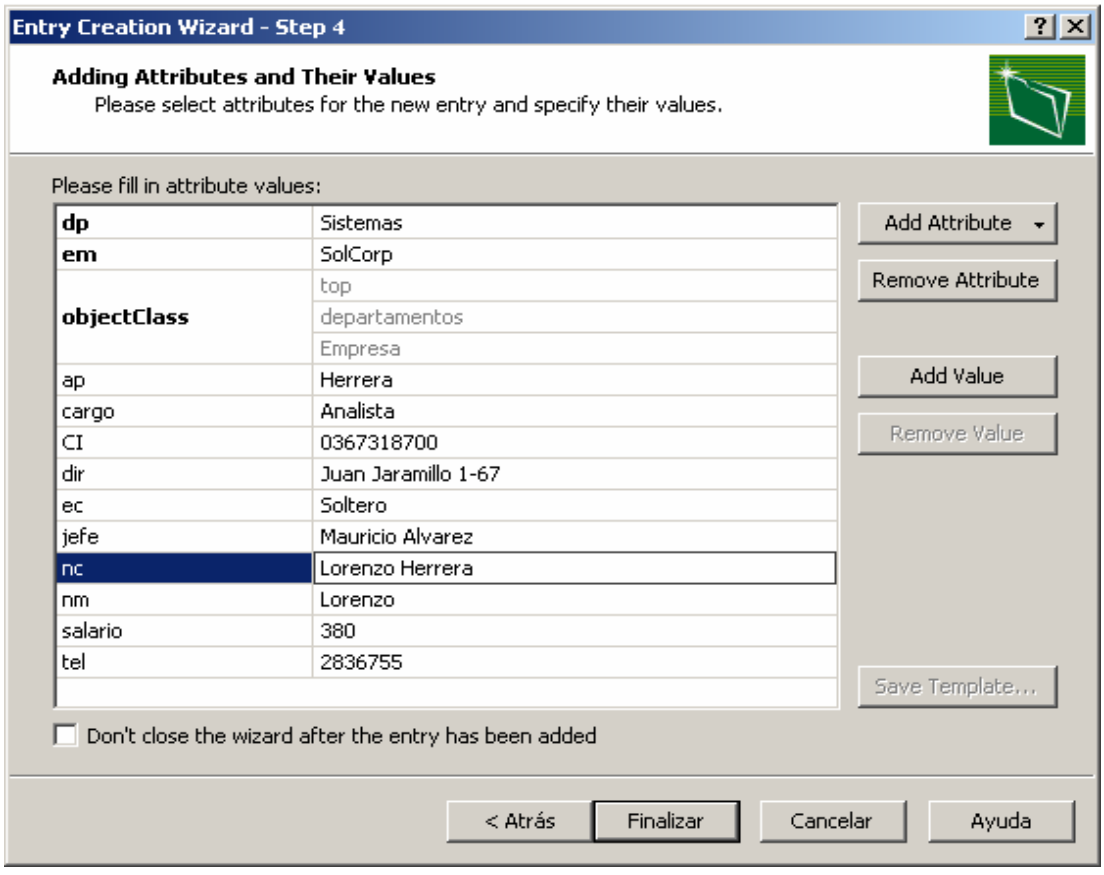

Figura 2.40 Selección de atributos de la nueva entrada del directorio.

Haciendo clic con el botón derecho ya sea en un atributo o en la entrada entera también se puede modificar y eliminar datos, para poder hacer esto se debe estar conectado al servidor con las credenciales correctas, si se esta conectado como un usuario anónimo no se podrán alterar datos, solamente se podrá ver los datos del directorio, para poder conectarse al servidor con las credenciales correctas se debe ingresar el nombre del usuario, los datos del dominio y el password que están especificados en el archivo */etc/openldap/slapd.conf* caso contrario no se autentificara correctamente y no permitirá conectarse al servidor LDAP.

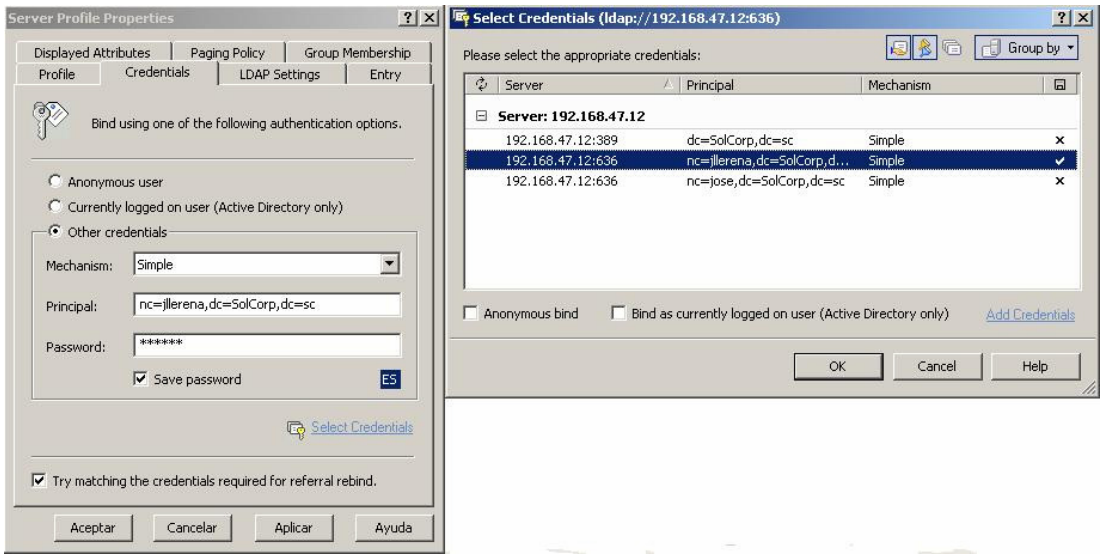

Figura 2.41: Pantalla de configuración y selección de credenciales para autentificación de usuario.

También se cuenta con la opción de usar conexión segura (SSL) para conectarse al servidor, debido a que en el punto anterior se configuró al servidor para que cuente con esta opción, se podrá habilitar esa característica y a continuación se vera como trabaja el cliente con esta opción.

Lo que hace el servidor es acceder al certificado que se creo en el punto anterior y luego de que lo valida a este da un mensaje de que no es un certificado de confianza debido a que no se cuenta con un proveedor de confianza y que si se desea proseguir, pero al ser un certificado conocido se procede a continuar con la conexión y nos dará un resultado de conexión exitosa.

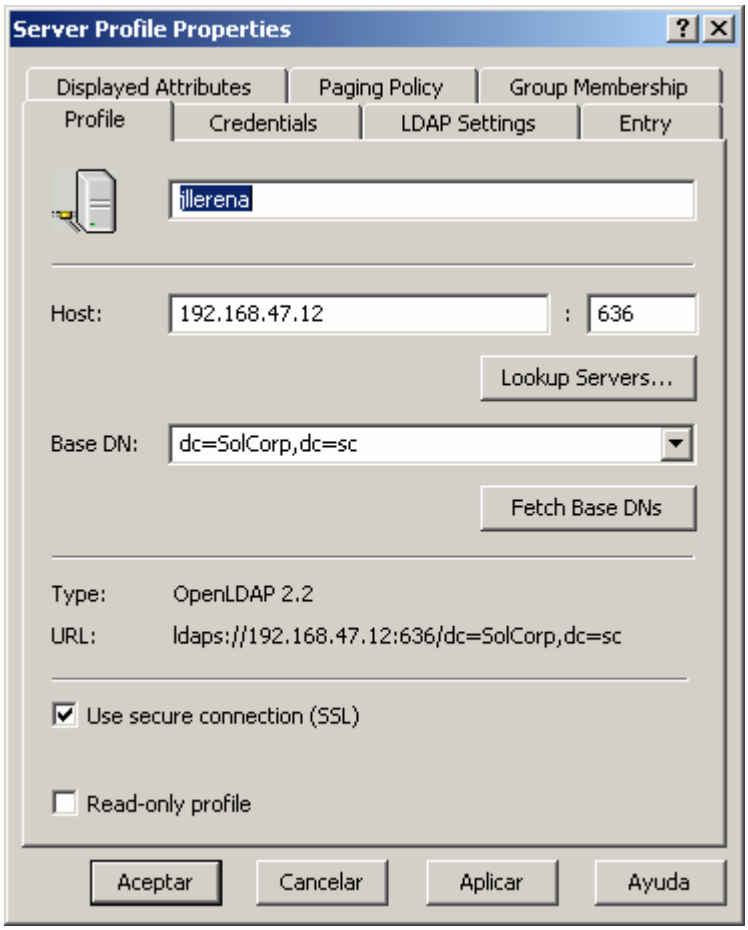

Figura 2.42: Pantalla de configuración del servidor con la casilla de conexión segura habilitada.

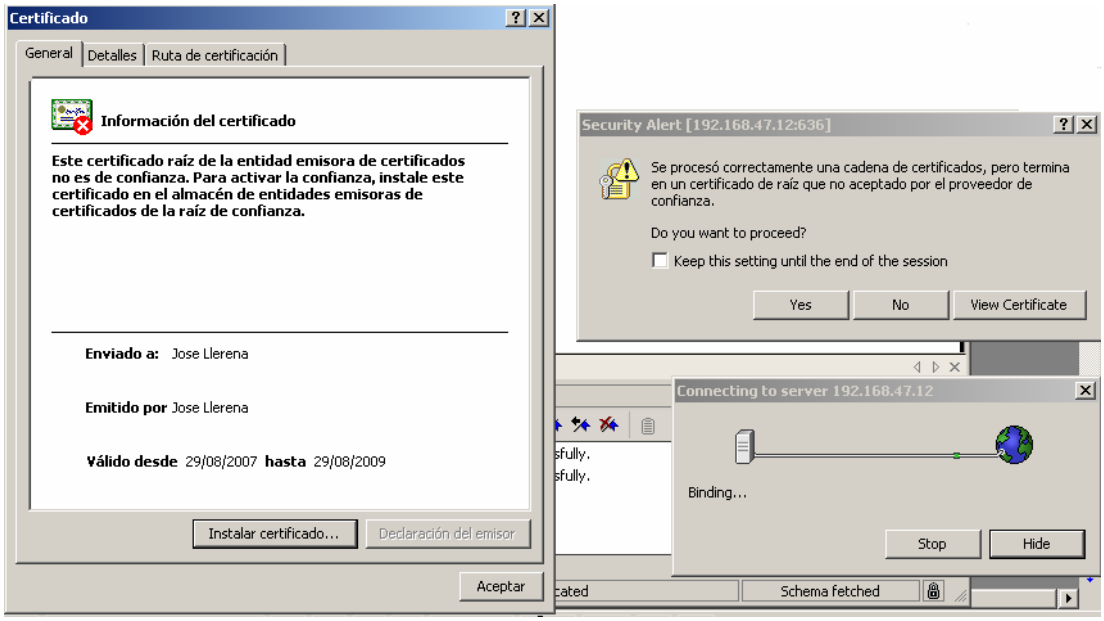

Figura 2.43: Ventana de validación de certificado para autentificación de usuario

2.7 Configurando y ejecutando Slapd

El archivo de configuración slapd cuenta con varias opciones de configuración, entre esas opciones están las siguientes:

-4 Hace caso solamente de direcciones IP versión 4

-6 Hace caso solamente de direcciones IP versión 6

-T {a|c|d|i|p|t|acl|auth} Funciona en modo de herramienta. Los argumentos adicionales se seleccionan si es que funciona con algunos de los comandos slapadd, *slapcat*, *slapdn*, *slapindex*, *slappasswd*, o *slaptest*. Los comandos *slapacl* y *slapaut*h necesitan la opcion "**acl**" y "**auth**". Estas opciones deben especificarse primero, las opciones restantes serán interpretadas por la herramienta *slap* correspondiente. Estas herramientas son enlaces simbólicos hacia slapd. Esta opcion se usa para situaciones en donde los enlaces simbólicos no son posibles de usar.

-d nivel-de-depuración

Habilita el nivel de depuración que se definió Si esta opcion se especifica incluso con un valor de 0, slapd no desasociara desde la terminal que invoca. Algunas operaciones y estados generales son impresas por cualquier valor de uno de los niveles de depuración, el cual es tomado como una cadena de bits, con cada bit correspondiendo a un diferente tipo de información de depuración.

-s nivel-syslog

Esta opcion indica a slapd a que nivel de depuración debería relacionarse la facilidad del syslog.

-n nombre-servicio

Especifica el nombre del servicio para conectarse.

-l usuario-local-syslog

Selecciona al usuario local de la facilidad de syslog. Los valores pueden ser desde LOCAL0 hasta LOCAL7, también USER (usuario) y DAEMON(demonio). El valor por defecto es LOCAL4. Esta opcion solo se permite en sistemas que tienen el soporte de usuarios con la facilidad de *syslog*.

-f archivo-configuración-slapd

Específica cual es el archivo de configuración. Por defecto la ruta es /etc/openldap/slapd.conf.

-F slapd-config-directory

Especifica el directorio del archivo de configuración. Por defecto el directorio es /etc/openldap/slapd.d. Si ambas opciones –f y –F son especificadas, entonces el archive de configuración será leído y convertido a formato de directorio de configuración y escrito al directorio especificado. Si ninguna opcion se especifica, *slapd* tratara de leer el directorio de configuración por defecto antes de intentar usar el archivo de configuración por defecto. Si un directorio de configuración valido existe, entonces el archivo de configuración por defecto es ignorado. Todas las herramientas slap que usan opciones de configuración actúan basados en el mismo criterio.

-h ListaURL

Slapd por defecto se fijara en la nomenclatura **ldap:///**. Y lo unirá usando el puerto 389 y la opcion INADDR_ANY. Puede ser usada para especificar URL's sobre los cuales trabajara. Los URL's se los separa por medio de un espacio. Los mismos deben ser de esquemas LDAP, LDAPS o LDAPI y generalmente sin un nombre distinguido o algún otro parámetro opcional.

Los *host* pueden especificarse por nombre o por formato de dirección IPv4 o IPv6. Si se especifican los puertos, estos deben ser numéricos. El Puerto por defecto de ldap:// es 389 y para ldaps:// es 636 también utilizado cuando se quiere configurar con soporte TLS-SSL.

Los permisos para escuchar son indicados por medio de "x-mod=-rwxrwxrwx", "x-mod=0777" o "x-mod=777", donde las letras "rwx" pueden reemplazarse por "-" para quitar el permiso relacionado.

-r directorio

Especifica un directorio cualquiera para que este se convierta en el directorio raíz. Cuando esta opción se usa como un mecanismo de seguridad, se debería usar con las opciones –u y –g.

-u usuario

Slapd funcionara con el nombre de usuario especificado o con su id, y su lista de acceso de grupo suplementario. El id de grupo también se cambia al gid del usuario especificado al menos que la opcion –g se utilice. Cuando se utiliza con la opcion –r, *slapd* usara la base de datos del usuario en el cambio de raíz.

-g grupo

Slapd funcionara con el nombre de grupo especificado o con su id. Como la opcion de usuario, si se lo usa con la opcion –r, *slapd* usara la base de datos de ese grupo.

-c cookie

Esta opcion provee una cookie para la replicación "syncrepl". La cookie es una lista separada por comas de pares nombre=valor. Los campos de coolíes soportados son rid y csn, el primero identifica un hilo de replicación en el servidor del consumidor y es usado para encontrar la especificación "syncrepl" en el archivo *slapd.conf* y teniendo la identificación de replicación en su definición, "rid" debe ser provisto con el fin de usar valores especificados. Csn es el numero de secuencia de un *commit* recibido por una sincronización previa y representa el estado del contenido de la replica del consumidor el cual el motor del *syncrepl* sincronizara al contenido del proveedor actual.

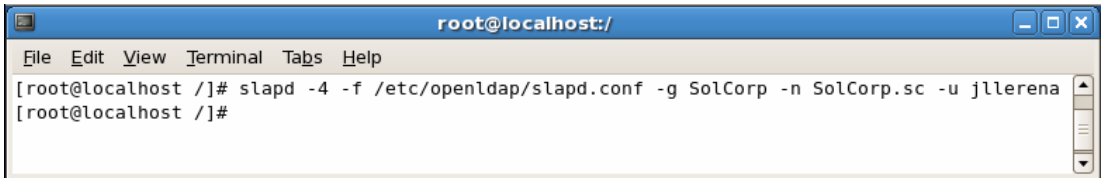

Figura 2.44: Configuración de LDAP con el comando Slapd

El formato del archivo de configuración consta de ciertas opciones de configuración globales que se aplican a *slapd* como un todo, además de contar con ninguna o varias

definiciones de bases de datos que contienen información específica sobre una instancia de bases de datos.

Si una línea comienza con un espacio en blanco se considera la continuación de la línea anterior. Cuando comienza con numeral, todo lo que le sigue se ignora. El formato general de configuración es el siguiente:

#Se acostumbra a describir lo que se configura el las líneas subsiguientes
<opciones de configuración global>
#Primera definición de base de datos y opciones de configuración
<opciones de configuración especificas para esta base de datos>
#Más definiciones de bases de datos si es que las hay

Los argumentos de configuración en cada línea son separados por un espacio en blanco. Si un argumento contiene un espacio en blanco, el mismo debe ser puesto entre comillas dobles. Si un argumento contiene comilla dobles o un backslash, el carácter debe ser precedido por el backslash.

Entre las opciones globales están las siguientes:
Access to <atributo u objeto> [by <usuario> <nivel de acceso>]
Esta opcion otorga acceso a un grupo de entradas o atributos por medio de uno o más solicitadores.

Attribute <nombre> [<nombre2>] {tipo de sintaxis}
Esta opcion asocia una sintaxis con un nombre de atributo. Por defecto el atributo asume la sintaxis cis (punto 1.4 de este documento se puede encontrar mas detalles). Además se puede contar con un nombre alterno para el atributo.

defaultaccess <nombre> [<nombre alterno>] { none | compare | search | read | write }
Esta opcion especifica que tipo de acceso se les da a los usuarios por defecto.

Include <nombre del archivo>

Esta opcion hace que se lea información adicional de configuración de dicho archivo especificado antes de continuar con la siguiente línea. El archivo debe seguir el mismo formato de configuración

Loglevel <numero>
Esta opcion especifica el nivel al cual los estatutos de depuración deberían trabajar con el sistema.

Objectclass <nombre>
[MUST <atributos>]
[MAY <atributos>]
Esta opcion define las reglas de esquema para el objeto dado. Puede contar con las opciones de requerir un atributo o de permitir ciertos atributos.

Referral <url>
Esta opcion especifica la referencia para pasar cuando *slapd* no puede encontrar una base de datos local para manejar un requerimiento.

Schemacheck { on | off }
Esta opcion habilita o deshabilita la revisión de esquema. Si esta habilitado, las entradas agregadas o modificadas será revisadas para asegurarse que estas obedezcan las reglas de esquema impuestas por su clase objeto tal y como se definió en la opcion objectclass.

Sizelimit <numero>
Especifica el número máximo de entradas que muestra cuando se hace una operación de búsqueda (*ldapsearch*). La opcion por defecto es 500

Srvtab <archivo>
Especifica el archivo *srvtab* en el cual *slapd* puede encontrar las llaves de *kerberos* necesarias para autentificar clientes.

Timelimit <numero>

Se especifica el numero máximo de segundos en el cual se tomara el servidor para responder a una petición. Si una petición no se termina en el tiempo máximo, un mensaje mostrando que se ha excedido el tiempo aparecerá. El valor por defecto es 3600.

Opciones generales de backend.

Estas opciones tienen soporte para cualquier tipo de base de datos.

Database <tipo de base de datos>

Esta opcion define el inicio de una base datos, por lo general el tipo de base de datos que se utiliza es bdb.

Lastmod { on | off }

Esta opcion controla si es que el servidor automáticamente mantiene los atributos *modifiersName, modifyTimestamp, creatorsName* y *createTimestamps* por entradas.

Readonly { on | off }

Esta opcion habilita o deshabilita la opcion de solo lectura, el mismo dará un mensaje de error si se pretende hacer una operación de escritura cuando este habilitado el modo lectura.

Replica host=<nombre de host> [:<Puerto>]
"binddn=<DN>"
bindmethod={ *simple* | *kerberos* }
[credentials=<*password*>]
[srvtab=<*filename*>]

Esta opción especifica un sitio de replicación para esta base de datos. El parámetro host= especifica un host y opcionalmente un puerto donde la instancia *slapd* esclava puede ser encontrada, para esto se puede usar un nombre de dominio o una dirección IP. Si no se especifica el puerto, el puerto estándar (389) será el utilizado.

El parámetro binddn= da al DN (nombre distinguido) la posibilidad de buscar actualizaciones.

El parámetro de credenciales es solo requerido si se usa autentificación simple, otorga el password para *binddn* en el *slapd* esclavo.

Replogfile <nombrearchivo>
Esta opcion especifica el nombre del archivo log de replicación al cual *slapd* notifica los cambios, es usualmente escrita por *slapd* y leída por *slurpd*.

Rootdn <dn>
Especifica el nombre distinguido de una entrada que no esta sujeta a control de acceso o restricciones de límites administrativos. La sinopsis va de la siguiente manera:
Rootdn "nombre-atributo=usuario", dc=dominio"
Ejm: rootdn "nc=andres59,dc=uazuay,dc=edu,dc=ec"

Rootpw <password>
Esta opcion especifica un password para el nombre distinguido que se detalla arriba, puede ser el texto plano, los caracteres encifrados o se deja con el valor de "secret".

Suffix <suffix del dn>
Esta opción especifica los sufijos del DN de las peticiones que serán pasadas al *backend* de la base de datos. Pueden haber varias líneas de sufijo, pero al menos una es requerida para cada definición de base de datos.
Update <dn>
Se aplica solo a un *slapd* esclavo. Especifica el DN permitido para hacer cambios a la replica.

Control de Acceso
Los accesos a las entradas y atributos de *slapd* son controlados por la directiva del archivo de configuración de acceso.
Algunos de los ejemplos de control de accesos se puede describir los que están a continuación:
Access to * by * read
Esta directiva de acceso da acceso de lectura a todos.

El siguiente ejemplo muestra el uso de una expresión regular para seleccionar entradas por medio de DN en dos directivas de acceso en donde el orden es significante.

```
Access to dn=".*, em=SolCorp"
By * search
Access to dn=".*, ap=Llerena"
By * write
```

El acceso a escritura se otorga solamente a quien tenga el apellido Llerena, ap es un atributo creado previamente, caso contrario dará error, mientras que todos los que trabajen en la empresa SolCorp podrán hacer operaciones de búsqueda.

El archivo *slapd.conf* para las diferentes tareas que se han realizado esta configurado de la siguiente manera:

```
# See slapd.conf(5) for details on configuration options.
# Las siguientes líneas permite la inclusión de los esquemas
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/evolutionperson.schema

# Permite la conexión de clientes LDAP versión 2
allow bind_v2

# Es la referencia del directorio
referralldaps://solcorp.sc

pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args

# Las siguientes 3 líneas son las rutas  de los archivos que se necesitan para hacer la
# certificación TLS-SSL
TLSCACertificateFile /etc/openldap/cacerts/slapd.crt
```

```
TLSCertificateFile /etc/openldap/cacerts/slapd.crt
TLSCertificateKeyFile /etc/openldap/cacerts/slapd.key

# A partir de aquí son las definiciones de base de datos que se han utilizado
database        bdb
suffix          "dc=dominiouda,dc=edu"
rootdn          "cn=jllerena,dc=dominiouda,dc=edu"
rootpw          secret
directory       /var/lib/ldap

# Indices to maintain for this database
index objectClass                       eq,pres
Index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub

database        bdb
suffix          "dc=inicioms,dc=com"
rootdn          "cn=josellerena,dc=inicioms,dc=com"
rootpw          secret
directory       /var/lib/ldap

#índices a mantener en esta base de datos
index objectClass               eq,pres
index ou,cn,mail,surname,givenname eq,pres,sub
index uidNumber,gidNumber,loginShell      eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry                eq,pres,sub

database        bdb
suffix          "dc=SolCorp,dc=sc"
rootdn          "nc=jllerena,dc=SolCorp,dc=sc"
rootpw          secret
```

```
directory       /var/lib/ldap
index dp,nc,apellido,nombre eq,pres,sub
index objectClass       eq
index uid       pres,sub,eq
index displayName    pres,sub,eq
index uidNumber              eq
index gidNumber              eq
index memberUID              eq
index default sub
```

Cabe indicar que el resto de líneas del archivo de configuración se encontraban entre comentarios y se procedió a eliminarlas, tal es el caso de la replicación con *slurp* o los controles de acceso que para esta configuración no se ha tomado en cuenta.

Ejecutando el servicio ldap

Como se ha visto la manera de hacer funcionar al servidor ldap es con el comando *service* ldap [Start | Stop | Status | Restart]

La opcion de *Start* inicia el servicio cuando se encuentra detenido. La opción de *Stop* detiene el servicio

La opción de *Status* muestra el estado del servicio, ya sea si esta detenido o esta funcionando, si se encuentra detenido muestra un mensaje como el siguiente:
Slapd is stopped

Si esta funcionando da un mensaje como este:
Slapd (pid 6619) is running

La opcion de restart, reinicia el servicio cuando se encuentra funcionando, esto se hace normalmente cuando se efectúa cambios en la configuración y se pretende hacer que los cambios realizados entren en efecto.
Si todo esta correcto el servicio se reiniciara, caso contrario dará el error correspondiente.

2.8 Creación de una base de datos con Slapd

En esta sección se mostrara como crear una base de datos a partir de cero y como trabaja una base de datos no relacional con el servidor LDAP.

El primer método para crear una base de datos es crearla on-line usando LDAP. De esta manera se inicia *slapd* y se añaden entradas usando el cliente LDAP de elección. Este método es recomendable para base de datos relativamente pequeñas (por decir de unas pocas entradas, como unas cien por ejemplo).

Este método es utilizado para base de datos que tiene soporte de actualizaciones. El segundo método es crear la base de datos off-line usando utilidades especiales provistas con *slapd*. Este método es mas recomendado si se cuenta con miles de entradas para crear, el cual tomara bastante tiempo usando el método de LDAP, o si se quiere asegurar que la base de datos no será acezada mientras se esta creando. Aunque no todos los tipos de base de datos soportan estas utilidades.

Creando una base de datos sobre LDAP

Al usar este método de creación de base de datos, se utiliza el cliente LDAP de preferencia para añadir entradas, tal y como se hace una vez que la base de datos esta creada. El orden para crear la base de datos es la siguiente, las opciones a continuación son requeridas y necesarias para la creación de la base de datos.
Database <base de datos>

La primera línea que define una creación de base de datos es la mencionada, y además debe indicarse el tipo de base de datos que se utiliza, en el caso es bdb (Berkeley Data Base), esta es la utilizada por defecto.

suffix <dn>

Como se ha mencionado el sufijo define las entradas que va a usarse para la base de datos a crearse. Se debe definirlo en base al DN del root (rootdn), es decir dentro del dc van los mismos valores en el suffix y en rootdn.

Es necesario especificar un directorio en donde los archivos de índices van a ser creados, el directorio por defecto y el usado en este documento es el siguiente:

Directory /var/lib/ldap

Este directorio debe tener los permisos apropiados para que *slapd* pueda acceder a este directorio. Los permisos de directorio están establecidos de la siguiente manera:

Chmod 744 /var/lib/ldap

Slapd debe configurarse de tal manera que se pueda conectar como un usuario de directorio con permisos para agregar entradas. Al trabajar todo bajo usuario root se ha podido contar con todos los privilegios para trabajar sobre cualquier directorio. Esto se logra gracias a las dos opciones que están a continuación:

rootdn <dn>

rootpw <passwd>

Si a rootdn se lo asocia con root y el rootpw tiene la opción secret, entonces se podrán utilizar para autenticarse como un súper usuario para esta base de datos, por lo tanto se podrá hacer cualquier tipo de operación. Este DN y contraseña funcionaran siempre sin importar si la entrada llamada exista o tenga la contraseña dada. Esto resuelve el problema de autenticar y añadir entradas antes de que cualquier entrada siquiera exista.

Además la definición de la base de datos debe asegurarse que cuenta con las definiciones de índices que se desean.

index {<lista de atributos> | default} [pres,eq,approx,sub,none]

Los atributos van separados por coma además de los valores de los índices. Los valores de los índices que serán creados pueden ser de presencia (pres), igualdad (eq), aproximación (approx), sub cadenas (sub) o ninguna.

En el ejemplo con el que se ha estado trabajado, las siguientes directivas o reglas se han utilizado para indexar los siguientes atributos.

```
index dp,nc,apellido,nombre eq,pres,sub
index objectClass       eq
index uid       pres,sub,eq
index displayName    pres,sub,eq
index uidNumber              eq
index gidNumber              eq
index memberUID              eq
```

Eso quiere decir que para los atributos dp, nc, apellido, nombre, uid y displayName se ha creado índices de presencia, igualdad y sub cadenas. Para los atributos objectClass, uidNumber, memberUID y gidNumber se han creado indices de igualdad. No todos los tipos de índices están disponibles para todos los tipos de atributos.

Terminado de configurar *slapd* e iniciar el servicio, se hace la conexión con el cliente y se empieza a añadir los registros, esto se hace con el comando *ldapadd* el cual se ha mostrado ejemplos anteriormente y se detallara un poco mas adelante, que por supuesto se requiere de un archivo LDIF que también se cuenta con ejemplos en puntos anteriores.

Este método de creación de bases de datos es el que se ha estado utilizando en todos los ejemplos anteriores.

Creación de una base de datos off-line.

Como en el otro caso, este método no cambia las directivas a utilizarse, es decir utiliza la misma sintaxis y orden. Las mismas definiciones para los sufijos, dominios índices y todo lo demás que se utiliza son de la misma manera.

Para este método de creación de base de datos la diferencia radica en que se utilizan algunas herramientas de bases de datos de *slapd* que se detallaran mas adelante. Este método es recomendable si se cuenta con muchos registros para ser creados y que tomarían bastante tiempo en agregarlos si se utiliza el método anterior. Estas

herramientas leen el archivo de configuración *slapd* y un archivo de entrada que contenga una representación de texto de las entradas que se agregaran. Para los tipos de bases de datos que tienen soporte de esas herramientas, producen los archivos de base de datos directamente.
Las diferentes herramientas que pueden utilizarse para crear una base de datos off-line están las siguientes:

El comando slapadd
Esta herramienta se utiliza para añadir entradas especificadas en el archivo de formato LDIF a una base de datos.

Este comando abre la base de datos dada determinada por el suffix y añade las entradas correspondientes al archivo LDIF provisto de la base de datos. Esta diseñada para aceptar los LDIF en orden de base de datos, no verifica que entradas superiores existan antes de agregar un registro, no realiza todas las revisiones de usuario y esquemas de sistemas, y no mantiene atributos operacionales.
Tiene el limitante de que el servidor no debe estar en funcionamiento cuando se realice la acción de agregado, debido a que se pretende asegurar consistencia a la base de datos.
El formato para utilizar este comando es el siguiente:

slapadd -l <archivo ldif> -f <archivo slapd>
[-d <nivel depuración>] [-n <numero>|-b <sufijo>]

Los argumentos tienen los siguientes significados:
-c Habilita el modo de ignorar errores

-g Ignora los subordinados solo la base de datos especifica será procesada y no sus subordinados si es que los hay

-u Habilita un modo en el que no escribe sobre el *backend*

-q habilita modo rápido, es decir solo revisa unas pocas tareas de integridad, las cuales revisa los datos entrantes y no revisión de consistencia cuando se escribe a la

base de datos. Mejora el tiempo de respuesta pero si algún error o interrupción ocurre, la base de datos no será usable.

-w Escribe información de contexto de replicación y sincronización.

-d <nivel de depuración>

Activa el modo de depuración. Los niveles de depuración posible son los siguientes:

Nivel	**Descripción**
-1	Habilita todas las depuraciones
0	Sin depuración
1	Llamada a función de rastreo
2	Manejo de paquetes de depuración
4	Depuración de rastreo pesado
8	Administración de conexión
16	Imprime paquetes enviados y recibidos
32	Procesamiento de filtrado de búsqueda
64	Procesamiento de archivo de configuración
128	Procesamiento de lista de control de acceso
256	Muestra estado de conexiones/operaciones/resultados
512	Muestra estado de registros enviados
1024	Imprime la comunicación con los backends de shell
2048	Imprime entradas de depuración

Tabla 2.1: Distintos niveles de depuración

-l <archivo ldif>

Especifica el archive LDIF que contiene las entradas para agregar en modo de texto.

-f <archivo de configuración >

Especifica el archivo de configuración que indica donde crear los índices y que índices crear.

-F <directorio de configuración >

Aplica el mismo criterio al especificado con *slapd* en el punto 2.7.

-n <numero de base de datos>

Es un argumento que especifica que base de datos modificar. La primera base de datos definida en el archivo de configuración es 1, la siguiente 2 y así sucesivamente. Por defecto la primera base de datos en el archivo de configuración es la usada. Este argumento no debe ser usado con –b.

-b <sufijo>

Especifica la base de datos a modificar. El sufijo provisto se revisas en la base de datos que concuerde para determinar su número. Esta opcion no debe usarse con –n.

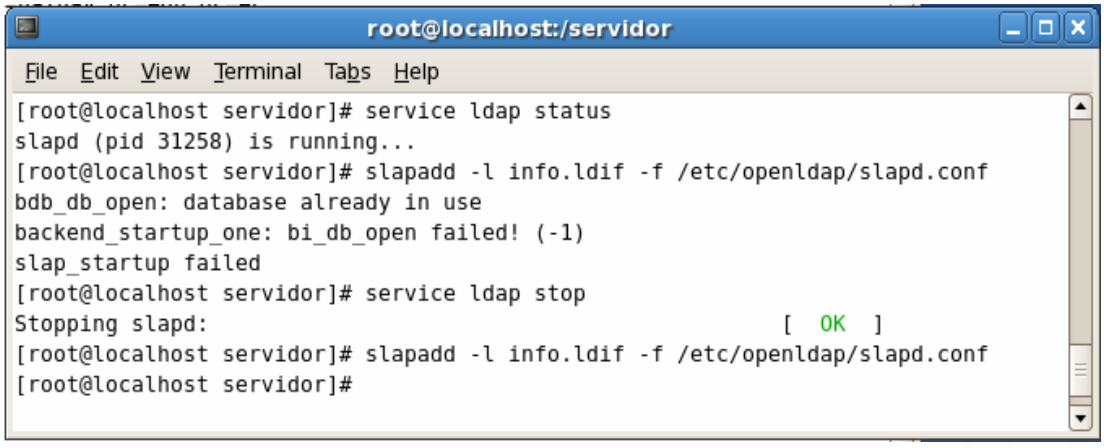

Figura 2.45: Uso del comando *slapadd*

En la figura 2.45 se puede observar como funciona el comando *slapadd* en el cual da mensaje de error, indica que la base de datos esta abierta para lo cual se necesita detener el servicio LDAP para poder usar el comando, una vez detenido los datos del archivo info.ldif se insertan en la base de datos.

El comando slapindex

En muchos casos es necesario regenerar índices sobre todo después de modificar el archivo de configuración de servidor. La forma en la que se usa este comando es la siguiente:

slapindex -f <archivo slapd> [-d <nivel de depuración >] [-n <numero de base de datos >|-b <sufijo>]

Todas las opciones de este comando aplican el mismo criterio que se menciono para el comando *slapadd*. Este comando lo que hace es reconstruir todos los índices basados en lo que se definió en la base de datos.

El comando slapcat.

Este comando lo que hace es mover el contenido de la base de datos a un archivo LDIF. Este comando es mas utilizado cuando se pretende hacer un respaldo en el cual se pueda leer el contenido de la base de datos o cuando se quiere editar la base de datos off-line. La manera de usar este comando es la siguiente:

slapcat -l <nombre de archivo> -f <archivo de configuración slapd >
[-d <nivel de depuración >] [-n <numero de base de datos >|-b <sufijo>]

Las opciones –n o –b igualmente como el comando *slapadd* se usa para seleccionar la base de datos del archivo de configuración *slapd* que se especifica con la opción –f. El archivo LDIF especificado es a donde se copiara la información de la base de datos que se especifico.

CONCLUSIONES

Luego de la instalación, pruebas, configuraciones y creaciones de directorios se puede entender y conocer lo importante, útil y practico que es el tener un directorio personal de diferentes personas ya sea como en el caso dado de una empresa, o como de cualquier otro tipo de información como de productos de un almacén o información mas detallada sobre un producto en particular.

Además se conoció la manera con la cual LDAP funciona y como interactúa con la base de datos, y se puede ver que es de una manera muy práctica y que no implica mayores complicaciones para los usuarios y para el administrador del servidor.

CAPITULO 3 Uso de LDAP

INTRODUCCION

En este capitulo se vera con un poco mas de detalle los distintos tipos de operaciones que pueden realizar los clientes LDAP, y cuales son los comandos que se utilizan para realizar las distintas operaciones con LDAP, las características, opciones, argumentos, entre otras cosas con las que cuenta cada uno de estos comandos utilizados dentro de LDAP.

3.1 Añadiendo datos

El añadir datos implica pasar información desde un archivo LDIF el cual debe estar correctamente establecido como se ha mostrado en los capítulos anteriores, es decir con la sintaxis correcta y que los objetos estén dentro de una estructura de árbol, por lo tanto un objeto necesariamente tiene que ser subordinado del otro, se aplica el método de jerarquía.

Para poder empezar a añadir datos el archivo de configuración *slapd* debe estar correctamente configurado, por lo tanto las entradas para *suffix, directory, rootdn, rootpw* e *index*. Los comandos que se han utilizado para agregar datos son *ldapadd* y *slapadd*, el primero es común para agregar un numero bajo de entradas y cuando el servidor LDAP se encuentra en funcionamiento, el segundo como se ha visto recién se utiliza para mayores números de entradas y cuando el servidor LDAP se encuentra detenido.

3.2 Modificando datos

La tarea de modificar datos es muy similar a la de añadir datos en el sentido de que la base de datos trabaja de manera similar, la diferencia radica en el contenido del archivo LDIF, mientras que para agregar los datos se define todo el registro entero, es decir, el DN, el dominio, los atributos y objetos; para las tareas de modificación de datos solo se especifica la primera línea que contiene el DN, dentro del cual se encuentra el dominio y atributos para los casos dados, se especifica el atributo que se desea cambiar y el nuevo valor que este tendrá, como se vio en el punto 2.6 el valor

modificado se visualizara al final del registro cuando se realiza una operación de búsqueda.

El formato de un archivo LDIF cuando se quiere modificar datos es el siguiente:
dn: nc=José Llerena,dp=Sistemas,dc=SolCorp,dc=sc
changetype: modify
replace: salario
salario: 880

Si se desea cambiar otro valor de un atributo ya sea para el mismo DN o para un DN diferente, se repite la misma sentencia indicada con la diferencia de que en vez de "salario" se escribirá el nombre del atributo que se desee cambiar. Cada descripción de DN va separado por medio de un espacio.
El comando utilizado para modificar datos es *ldapmodify*.

3.3 Borrando datos

El borrado de datos permite eliminar entradas que no se deseen y que no sean necesarias en el directorio LDAP, para lograr esto se lo realiza con el comando *ldapdelete*, en el cual se debe especificar en que dominio, es decir en que base de datos se quiere hacer la operación y además detallar en registro que se desea borrar para lo cual se debe detallar el DN completo del registro que se desea eliminar, el DN que se detalla es el mismo que se definió en el archivo LDIF que se utilizó para hacer el ingreso del registro dado.

3.4 Buscando datos

La búsqueda de datos permite buscar un registro o un atributo dado, para lo cual se debe de igual manera especificar el dominio sobre el cual se desea realizar la búsqueda.

LDAP permite usar varios filtros de búsqueda, en los cuales el usuario puede especificar lo que desea buscar y que atributos desea que el filtro de búsqueda visualice, además de que se puede especificar si se desea ver los resultados de igual manera que un archivo LDIF o no.

Con una búsqueda o lectura es la mejor manera de verificar si un registro ha sido ingresado o modificado correctamente, caso contrario la operación de búsqueda no mostrara ningún registro. El comando que permite realizar una búsqueda dentro de un directorio LDAP es el comando *ldapsearch.*

3.5 Árbol de directorios

En el directorio LDAP el modelo de información se basa en entradas. Estas entradas son una colección de atributos que tienen el nombre distinguido (*distinguished name)* el cual es utilizado para referirse a la entrada dada, los nodos simples a lo largo de la ruta de la entrada son llamados "relative distinguished name (RDN)" o nombre distinguido relativo en español. Cada una de los atributos de las entradas tiene un tipo de datos y uno o más valores. Los tipos son típicamente cadenas como por ejemplo "cn" para *common name* (nombre común), "mail" para la dirección de correo. La sintaxis de los valores depende del tipo del atributo, es decir un atributo cn puede tener valores como "José Llerena"; un atributo "mail" puede contener el valor jllerena@midominio.com; un atributo "jpegphoto" tuviera una fotografía en el formato binario JPEG.

Un directorio LDAP tiene una estructura en forma de árbol. Todas las entradas (o bien llamadas objetos) del directorio tienen una posición definida dentro de esta jerarquía la cual lleva el nombre de "Directory information tree (DIT)" en español árbol de información de directorio.

A los objetos se los puede asignar generalmente uno o dos tipos posible que pueden ser por ejemplo:

Contenedor: Estos objetos pueden tener otros objetos. Tales clases de objetos son *root*, cuyo elemento de un árbol de directorio no existe en realidad, c (*country* o país), ou (*organizacional unit* o unidad organizacional) y dc (*domain component* o componente de dominio). Este modelo es comparable con los directorios en un sistema de archivos.

Hojas: Estos objetos se sitúan al final de la rama y no tiene objetos subordinados. Como ejemplo se puede mencionar *person, InterOrgPerson,* o *groupofName.*

La cima de la jerarquía del directorio tiene un elemento root, este puede tener ya sea c (*country* o país), ou (*organizacional unit* o unidad organizacional) y dc (*domain component* o componente de dominio) como elementos subordinados. La relación dentro de un árbol de directorio LDAP se explica más claramente en el siguiente ejemplo que se muestra a continuación:

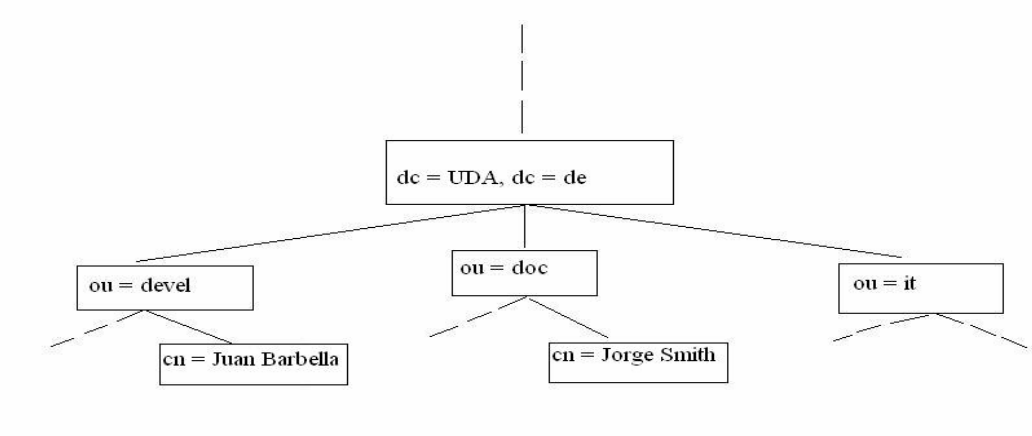

Figura 3.1: Estructura de un directorio LDAP

El diagrama muestra un árbol de información de un directorio. Cada entrada corresponde a una cuadro en la figura, el nombre distinguido completo y valido para en este caso empleado ficticio de la UDA Jorge Smith, en este caso es cn= Jorge Smith, ou = doc, dc = UDA, dc = de. Esta compuesto por la adición del nombre distinguido relativo cn = Jorge Smith al nombre relativo de la entrada precedente ou = doc, dc = UDA, dc = de.

En otro ejemplo con una representación diferente en este caso entradas representando países los cuales están en la parte superior del árbol. Debajo de aquellas están entradas representando provincias y organizaciones nacionales, y debajo de estas están entradas representando unidades organizacionales, gente, impresoras, documentos, etc; en la siguiente figura se aprecia mejor lo dicho.

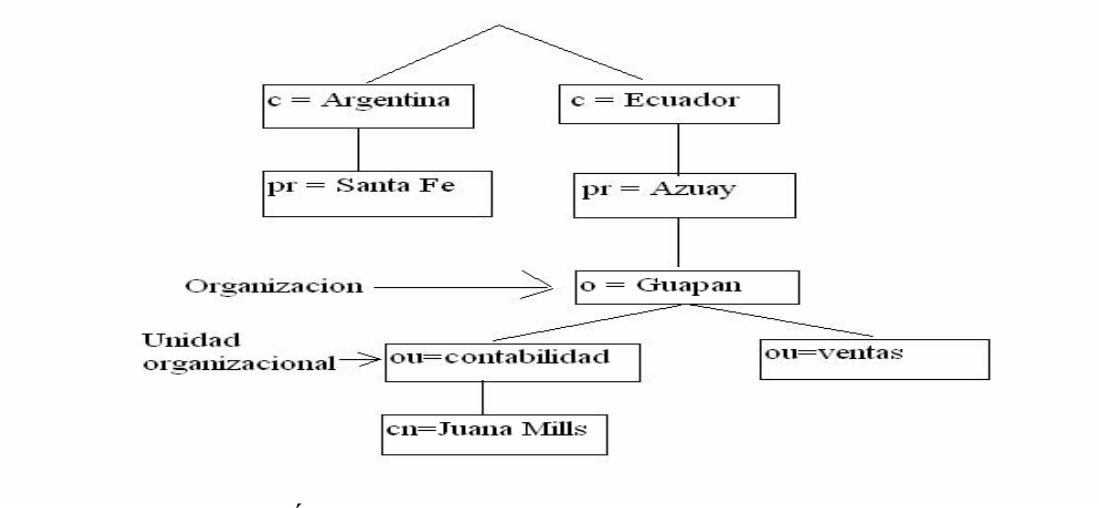

Figura 3.2: Árbol de nombre tradicional de un directorio LDAP.

3.6 ldapadd

Como se ha mencionado, el comando *ldapadd* es utilizado para agregar las entradas a un directorio ldap, este comando es fuertemente similar al comando *ldapmodify,* la diferencia esta en que cuando se utiliza el comando ldapadd, se activa la bandera que permite el agregado de una nueva entrada, la sintaxis y las opciones disponibles a usar con este comando son las detalladas a continuación:

Ldapadd [-c] [-S archivo] [-n] [-v] [-M[-M]] [-d nivel depuración] [-D dn de enganche] [-W] [-w password] [-y archivo donde se ubica el password] [-h host ldap] [-p puerto ldap] [-P 2|3] [-O propiedades-de-seguridad] [-I] [-Q] [-U autCID] [-R dominio] [-x] [-X idaut] [-Y mecanismoSASL] [-Z[Z]] [-f archivo]

-c: Es un modo de operación continua. Los errores son reportados, por defecto cuando hay errores el comando hace la operación de salida.

-S archivo: Agrega o cambia registros los cuales donde se omiten debido a algún error, son escritos a un archivo y el mensaje de error retornado por el servidor es agregado como un comentario. Mas útil si se usa con la opción –c

-n: Muestra que es lo que va a hacer el comando, pero realmente no hace la operación en realidad, esta opción es útil para depurar en conjunto con la opción –v.

-v: Esta opción usa el modo verbal, con muchos diagnósticos escritos a una salida estándar.

-M[M]: Habilita cierto tipo de control de manejo, si se especifica –MM, quiere decir que hace control crítico.

-d: Nivel de depuración, en la figura 40 se puede ver más detalles sobre esta opción que se utiliza en otros comandos de igual manera.

-D dn de enganche: Use el nombre distinguido de enganche para engancharlo al directorio LDAP.

-W Se utiliza para autentificación simple, se utiliza esta opción para no tener que especificar el password.
-w password: Usa el password que se almacena en la línea de passwd en el archivo del servidor *slapd.conf* cuando se crea una base de datos para realizar una autentificación simple.

-y archivo: Usa todo el contenido del archivo passwd para autentificación simple.

-h host ldap: Especifica al host en donde se desea hacer la operación.

-p: Especifica el puerto donde se va a trabajar.

-P 2|3 : Especifica la versión del protocolo ldap a utilizar.

-O propiedades de seguridad: Especifica propiedades de seguridad SASL.

-I: Habilita el modo interactivo de SASL. Siempre impulsando, el valor por defecto es de impulsar siempre.

-Q: Habilita el modo quieto de SASL, nunca impulsa.

-U idaut: Especifica el Id de autentificación para el enganche de SASL. La forma de identificarse depende del actual mecanismo de SASL usado.

-R dominio: Especifica el dominio del ID de autentificación para el enganche de SASL. La forma del dominio depende igualmente del actual mecanismo de SASL que se utilice.

-x: Como se ha dicho y es en otros comandos, esta opción usa autenticación simple, al usar esto lo hace en vez de la autentificación SASL.

-X idaut: Especifica el ID de autorización requerida para el enganche de SASL. También su forma depende del mecanismo actual usado.

-Y mecanismo: Especifica el mecanismo de SASL que se usara para la autentificación. Si no se especifica, el programa elegirá el mejor mecanismo que el servidor conozca.

-Z[Z]: Emite la operación extendida de iniciar la seguridad de capa de transporte (TLS). Si se usa en el modo –ZZ, el comando va a requerir que la operación sea exitosa.

3.7 ldapdelete

El comando *ldapdelete* borra las entradas de un directorio, lo que hace el comando es abrir la conexión hacia el servidor LDAP, se engancha a este y borra una o mas entradas. Si uno o mas argumentos DN son detallados, entonces las entradas con los nombres distinguidos que se han especificado serán eliminados. Cada entrada debe especificarse usando la representación de cadena para la versión 3 del protocolo LDAP. Para poder eliminar un registro antes debe especificarse el dominio de donde se va a eliminar el registro, el mismo que esta definido en la línea de *rootdn* en el archivo de configuración del servidor.

La sintaxis para utilizar este comando es la siguiente:
Ldapdelete [-n] [-v] [-c] [-v] [-M[-M]] [-d nivel depuración] [-f archivo] [-D dn de enganche] [-W] [-w password] [-y archivo donde se ubica el password] [-H URIldap] [-h host ldap] [-p puerto ldap] [-P 2|3] [-O propiedades-de-seguridad] [-U autCID] [-R dominio] [-r] [-x] [-I] [-Q] [-X idaut] [-Y mecanismoSASL] [-Z[Z]] [dn]…..

Las opciones –n, -v, -M, -f, -x, -D, -w, -W, -y, -h, -p, -P, -O, -I, -Q, -U, -R ocupan el mismo criterio que el comando *ldapadd.*

-c: El modo de operación continua de este formato radica en que los errores son reportados pero el comando continuara borrando los registros, por defecto la operación finaliza cuando se reporta un error.

-d: *ldapdelete* debe compilarse con la opción LDAP_DEBUG definida para que esta opción tenga efecto.

-f: Lee una serie de DN's del archivo, uno por línea, realizando una operación de borrado para cada línea.

-H: URIldap: Especifica el URI referente al servidor ldap dado, solo los campos de puerto, host y protocolo son permitidos, los URI se los separan ya sea con comas o con espacio en blanco.

-r: Realiza un borrado recursivo. Si el DN especificado no es una hoja del árbol, sus hijos, y los hijos de cada uno de estos hijos serán borrados del árbol de directorios. No se hace algún tipo de verificación, el uso de esta opción puede implicar el borrado de varios registros del árbol.

-X idauth: La idauth debe ser usada con alguno de los siguientes formatos: dn: nombre distinguido o u: nombre de usuario.

3.8 ldapmodify

Este comando al igual que *ldapadd* es una interfaz de shell accesible a los llamados de librería de estos dos comandos.

Ldapmodify abre una conexión a un servidor LDAP, se engancha y modifica o agrega entradas o también las puede eliminar. La información de las entradas se lee desde un archivo con el uso de la opción –f.

Este comando no funciona si se cambia el contenido del archivo LDIF sobre el cual se hizo las operaciones de inserción de datos, para poder realizar una modificación exitosamente se debe en un nuevo archivo LDIF editar lo que se desea cambiar (en el punto 2.6 se puede ver un ejemplo de modificación de datos) y en base a ese archivo con la opción –f, se invoca al comando *ldapmodify.*

La sintaxis de este comando es bastante similar a la de *ldapadd*, tiene pocas diferencias, la sintaxis de este comando es la siguiente:
Ldapmodify [-a] [-c] [-S archivo] [-n] [-v] [-M[-M]] [-d nivel depuración] [-D dn de enganche] [-W] [-w password] [-y archivo donde se ubica el password] [-H URIldap] [-h host ldap] [-p puerto ldap] [-P 2|3] [-O propiedades-de-seguridad] [-I] [-Q] [-U autCID] [-R dominio] [-x] [-X idaut] [-Y mecanismoSASL] [-Z[Z]] [-f archivo]

Ldapmodify al ser muy parecido a *ldapadd* las opciones aplican el mismo criterio, la diferencia esta en que *ldapmodify* tiene dos opciones más que son las que se muestran a continuación:

-a Agrega nuevas entradas. Si se utiliza el comando *ldapadd* esta opción siempre esta habilitada, por lo tanto no es necesario especificar con este comando.

La opción [–H URIldap] aplica el mismo criterio que la que utiliza el comando *ldapdelete.*

Un ejemplo de cómo se puede editar un archivo LDIF para luego usar el comando *ldapmodify* es el siguiente:

Dn: nc= Juan del Monte, dc=uazuay, dc=edu, dc=ec
Changetype: modif.
Replace: dirección
dirección: Gran Colombia 7-34

Add: Edad
Edad: 29

Delete: Nacionalidad

Luego de invocar al comando *ldapmodify*, este comando lo que va a hacer es reemplazar el atributo dirección con el nuevo valor del atributo dirección que esta descrita en el archivo, además agrega un nuevo atributo que se llama Edad, y el atributo Nacionalidad es completamente borrado del registro.

Dn: cn=Juan Rodas,cn=uazuay,dc=edu,dc=ec
Changetype: delete

Al ejecutar el comando *ldapmodify* lo que ocurrirá es que la entrada con cn=Juan Rodas, dc=uazuay, dc=edu, dc=ec será eliminado del directorio.

3.9 ldapsearch

Este comando permite hacer la búsqueda de registros y diferentes tipos de filtrados para cada caso, funciona como una interfase accesible al shell cuando se hace el llamado a la librería. El filtrado se conforma de una representación de cadenas que el comando utiliza para realizar su búsqueda, si no se especifica ningún filtrado de búsqueda, entonces el comando utilizara el filtrado por defecto el cual es (objectClass=*).

Si *ldapsearch* encuentra una o mas entradas, los atributos especificados son mostrados. Si se usa el asterisco, todos los atributos del usuario serán mostrados, si se utiliza el signo mas, todos los atributos operacionales serán mostrados.
El formato del comando *ldapsearch* es el siguiente:

Ldapsearch [-n] [-u] [-v] [-t] [-A] [-L[-L[-L]]] [-M[-M]] [-d nivel depuración] [-f archivo] [-D dn de enganche] [-W] [-w password] [-y archivo donde se ubica el password] [-H URIldap] [-h host ldap] [-p puerto ldap] [-b base de búsqueda] [-s base | one | sub | children] [-a never | always | search | find] [-l tiempo limite] [-z limite de tamaño] [-O propiedades-de-seguridad] [-I] [-Q] [-U autCID] [-R dominio] [-x] [-X idaut] [-Y mecanismoSASL] [-Z[Z]] filtro [atributos…]

Las opciones –n, -v, -M, -d, -x, -D, -W, -w, -y, -H, -h, -p, -P, -O, -I, -Q, -U, -R, -X, -Y, -Z aplican los mismos criterio que en los otros comandos, las opciones distintas con las que cuenta este comando son las siguientes:

-u: Incluye la forma del nombre del usuario amigable del DN en la salida.

-t: Escribe valores no imprimibles retenidos en un grupo de archivos temporales. Esta opción es útil cuando se trabaja con valores que contengan datos que no sean caracteres como por ejemplo una foto de formato JPEG o audio.

-A: Retiene solo el nombre de los atributos y no sus valores, es útil utilizar esta opción cuando solo se desea saber si un atributo se encuentra presente en una entrado o si es que no esta presente, y además que no este interesada en su valor especifico.

-L: Los resultados de búsqueda son mostrados en formato de intercambio de datos LDAP, es decir en un archivo LDIF. El uso de una L, restringe la salida a LDIF versión 1. Una segunda –L deshabilita los comentarios y la tercera L deshabilita las impresiones de la versión LDIF. Por defecto se usa una versión extendida de LDIF.

-S atributo: Los tipos de entrada que son retornados son basados en atributos. Por defecto no se clasifican las entradas que son retornadas. Si el atributo descrito es de longitud cero (especificado por “”), las entradas serán clasificadas por componentes o por su nombre distinguido (DN). Normalmente el comando imprime entradas como igual las recibe, el usar esta opción rompe este comportamiento causando que todas las entradas sean retenidas, de ahí clasificadas y por ultimo impresas.

-f Archivo: Lee una serie de líneas del archivo efectuando un *ldapsearch* para cada línea. En este caso, el filtro especificado en la línea del comando es tratada como un patrón en donde la primera ocurrencia de %s es reemplazada con una línea del archivo. Si el archivo es un simple carácter “-“, entonces las líneas son leídas desde a entrada estándar.

-b base de búsqueda: Una el valor de la base de búsqueda como un punto de inicio para la búsqueda en vez de actuar por defecto.

-s base | one | sub | children: Especifica el alcance de la búsqueda a una de las opciones especificadas como objeto base, nivel uno, sub árbol o búsqueda de hijos, por defecto es *sub*. El alcance para búsqueda de hijos requiere características de extensión de LDAP versión 3.

-a never | always | search | find: Especifica como la des referencia de los alias es hecha, una de estas cuatro opciones debe especificar que aliases son des referenciados ya sea nunca, cuando se busca, o cuando se esta localizando el objeto base para la búsqueda. Por defecto nunca se des referencia los alias.

-l tiempo limite: Especifica el tiempo máximo que se permite a una búsqueda completar su tarea. Si no se especifica la opción o se pone un valor de 0, significa que no tiene tiempo límite. Si el valor es max significa el número máximo permitido por el protocolo, un servidor puede imponer un tiempo límite máximo el cual solo el usuario root puede cambiar.

-z tamaño limite: Se limita a retener el tamaño especificado en la opción, como en la opción –l si no se especifica esta opción o se detalla con un valor de 0, significa que no hay tamaño limite, y si se especifica con el valor de max, significa el tamaño máximo permitido por el protocolo el cual solo el usuario root puede cambiar esta característica.

CONCLUSIONES

Al finalizar este capitulo se tiene una mayor idea y mayor conocimiento de cómo funcionan los comandos que se utilizan con el servidor LDAP, la manera de trabajar y de interactuar que tiene cada uno de estos comandos con el servidor, las opciones con las que cuentan cada uno de estos comandos.

También se puede entender como deben estar estructurados los archivos LDIF sobre los cuales van a trabajar cada uno de los comandos, y los propósitos que tienen estos para con el servidor y también se puede dar cuenta cuando es conveniente hacer una u otra operación con los comandos de LDAP y para qué casos es recomendable usar cada uno de los comando que se pueden utilizar con el protocolo LDAP.

CAPITULO 4: Funcionamiento del servidor LDAP

4.1 Introducción.

En este capitulo se mostrara el funcionamiento del servidor LDAP con distintos programas clientes de plataforma Windows, como estos acceden y trabajan con el servidor LDAP.

Los programas clientes que serán utilizados son aplicaciones para envió y recepción de correo electrónico, las aplicaciones que serán referidas en este capitulo son las siguientes: *Microsoft Outlook 2003, Mozilla Thunderbird 2.0.0.6* y *Pegasus Mail v4.4*.

4.2 Habilitación del servicio de replicación (*slurpd*).

Es muy importante contar con el servicio de replicación habilitado, así los programas clientes podrán comunicarse con el servidor LDAP, y con el servicio de replicación este responderá al llamado de las aplicaciones.

Para hacer posible el funcionamiento del servidor LDAP, se utilizara el nombre distintivo "cn=jose,dc=uda,dc=com" y como contraseña se utilizara "usuario".

Al contar con registros, los cuales van a ser accedidos por todos los programas clientes que utilicen ese servidor, en el momento de obtener respuesta el puerto del protocolo LDAP (389) se encontrara abierto y será posible acceder a los datos del servidor desde los programas clientes.

Desde la consola de comandos de Windows si se ejecuta el comando *netstat –na*, en la columna de dirección remota nos mostrara la dirección IP del servidor junto con el puerto que esta utilizando, con esto sabremos que esta abierta la conexión entre el cliente y el servidor.

Para habilitar el servicio de replicación se debe agregar las siguientes líneas al final de la definición de la base de datos; es decir, después de donde se define los índices.

Replogfile /var/lib/ldap/openldap-master-replog
Replica host=192.168.47.12:389 starttls=critical
Binddn=”cn=jose,dc=uda,dc=com”
Bindmethod=simple

Con estas líneas lo que hace es en la primera se especifica la ruta donde se guarda las incidencias de la replica, es decir los resultados de la interacción del cliente con el servidor.

También se especifica la IP del servidor que para el ejemplo es 192.168.47.12, igualmente se especifica el nombre distintivo y el método por el cual el cliente va a acceder al servidor, en este caso es autenticación simple.

Con esto esta listo el servidor, ahora se debe configurar los distintos clientes para que estos puedan acceder al directorio LDAP.

4.3 Funcionamiento del servidor LDAP con *Pegasus Mail v4.4.*

En el menú principal se debe ir a la parte en donde dice “*addresses”* o directorios y seleccionar la opción *“LDAP client”* o cliente LDAP y una vez ahí seleccionar la opción “*setup”, luego “new”* y se ingresa la información referente al directorio LDAP.

Una vez echo esto en los combo box se selecciona los criterios de búsqueda, ya sea por nombre, apellido, correo electrónico o teléfono, se escribe una o mas letras que indican que le campo seleccionado contenga la o las letras seleccionadas, luego se presiona la tecla *Enter* o se selecciona el botón *query* y aparecerá en pantalla las entradas que corresponden con el criterio de búsqueda.

Al seleccionar una entrada en la parte inferior de la pantalla, se mostrara toda la información referente a la misma, y si se hace doble clic aparecerá la ventana para enviar un correo nuevo y ahí aparecerá la dirección de correo del contacto seleccionado como destinatario.

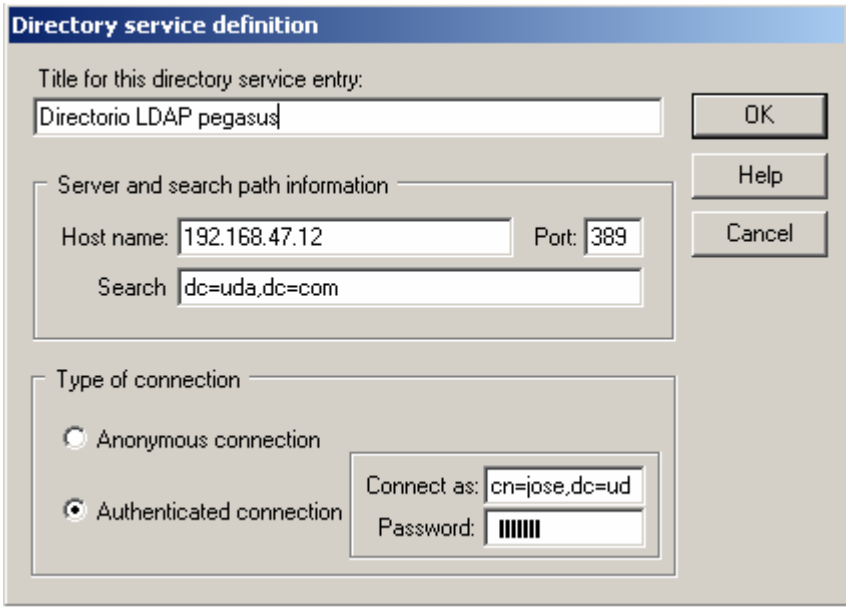

Figura 4.1: Definición de un servicio de directorio en *Pegasus Mail v4.4*

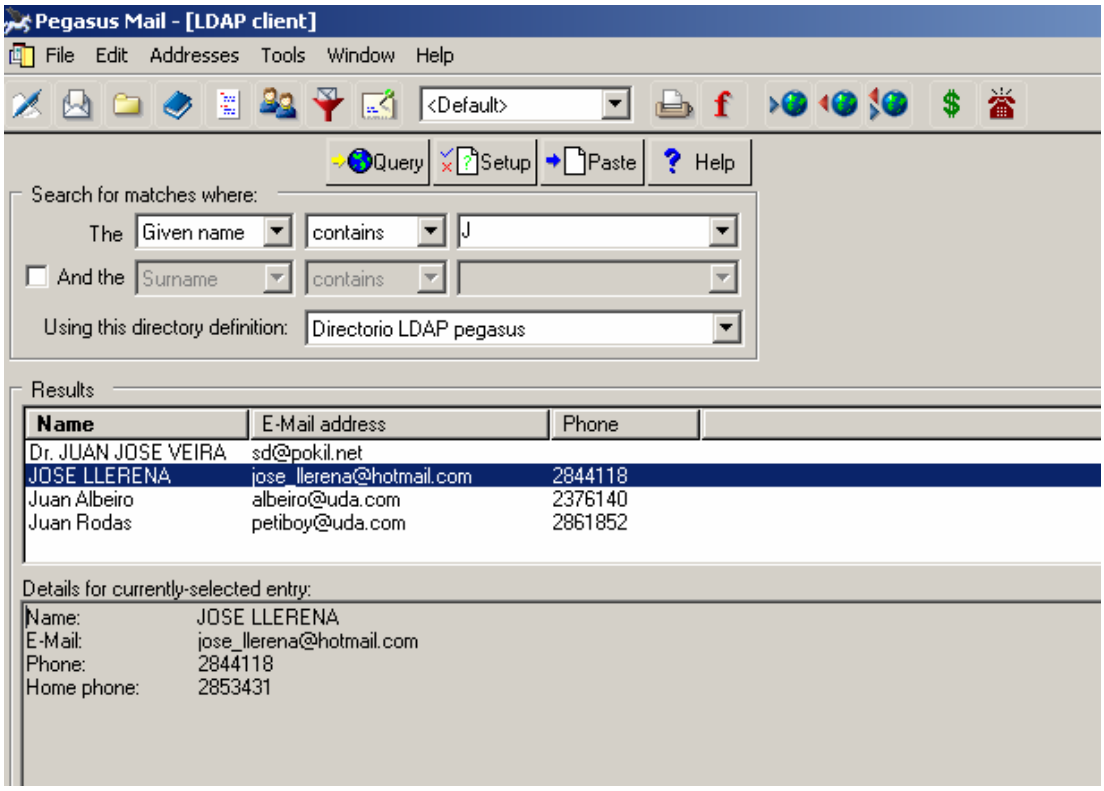

Figura 4.2: búsqueda dentro del directorio LDAP con *Pegasus Mail v4.4*

4.4 Funcionamiento del servidor LDAP con *Mozilla Thunderbird 2.0.0.6*

La configuración del directorio LDAP es tal y como se muestra en la Figura 2.18 (pagina 29), una vez configurado los datos del directorio, se procede a dar *Enter* y en la casilla de búsqueda se debe ingresar los parámetros de búsqueda ya sea una o

varias letras que corresponda con lo que queremos buscar, para realizar la búsqueda este programa verifica la información ingresada en la barra de búsqueda y compara con el nombre completo o el correo electrónico correspondiente.

Una vez realizado esto aparecerá una ventana solicitándonos la contraseña que se especifico en la configuración del servidor, una vez ingresada la contraseña correcta aparecerá las coincidencias de la búsqueda que hayamos realizado, si hay coincidencia aparecerán las entradas correspondientes caso contrario en la parte inferior izquierda del programa aparecerá un mensaje que dice "no se han encontrado coincidencias". Puede realizarse tantas consultas como se desee usando el mismo criterio.

Al hacer doble clic aparecerá la tarjeta del contacto en cuestión. También se puede arrastrar el contacto seleccionado hacia la libreta de direcciones personales y así tener la información del contacto localmente. Al tener el contacto en la libreta personal se podrá realizar cambios a la información de los contactos que se hayan copiado.

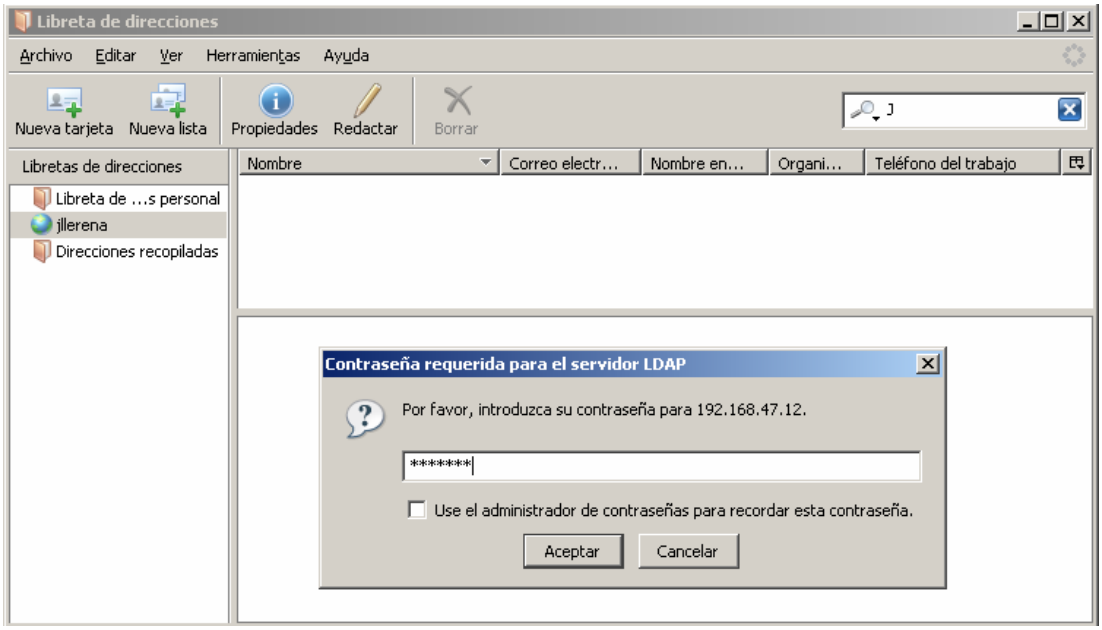

Figura 4.3: Solicitud de contraseña para acceder al directorio LDAP

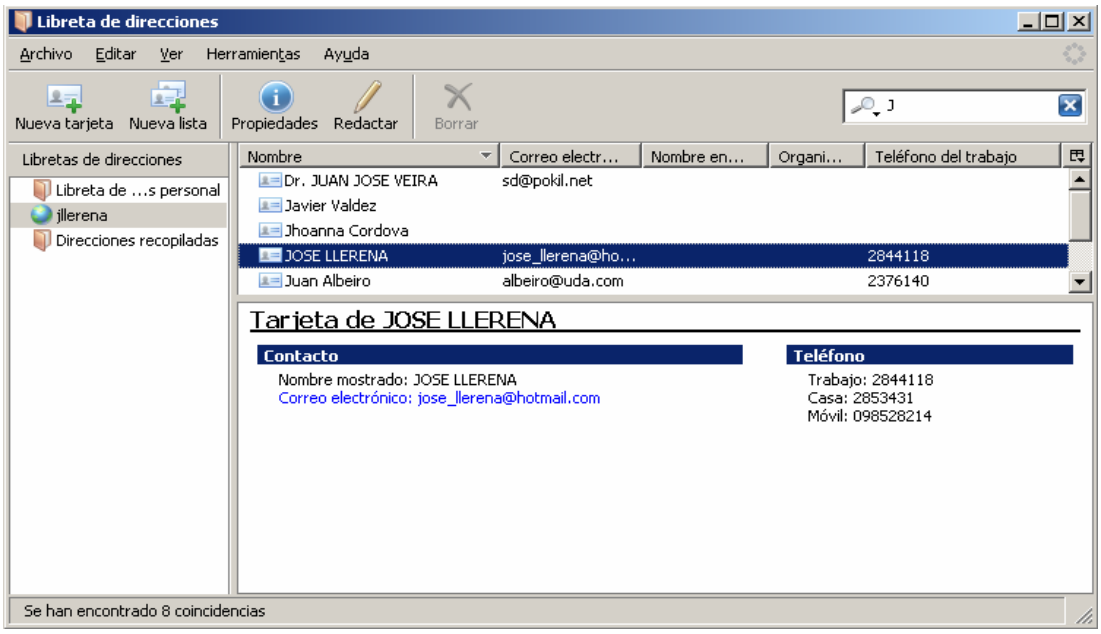

Figura 4.4: Resultado de la solicitud de búsqueda

Otra manera de acceder al directorio es en el momento de enviar un correo. En archivo → nuevo → mensaje, aparece la ventana para escribir un nuevo correo y en la parte izquierda de la ventana aparece un panel de contactos donde hay una barra de búsqueda y se puede acceder de la misma manera al directorio, si no aparece ese panel en el menú ver → panel lateral de contactos se lo activa y el panel aparecerá en el lado izquierdo de la ventana.

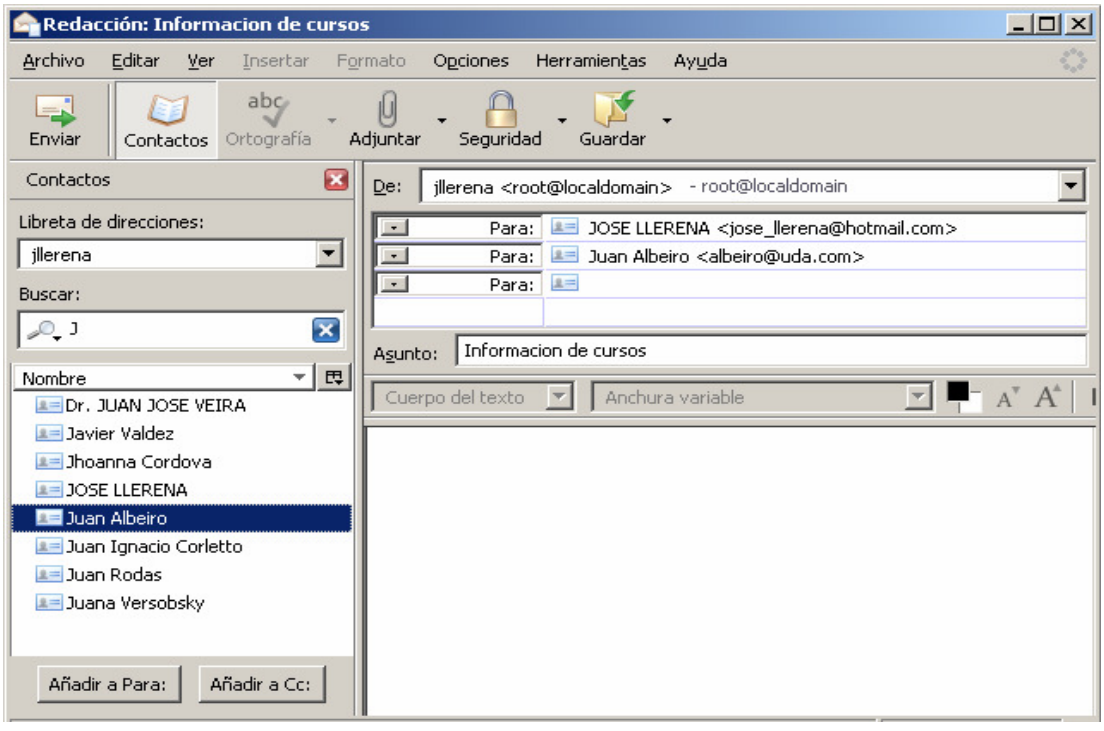

Figura 4.5: búsqueda del directorio en la ventana de envió de correo nuevo

4.5 Funcionamiento del servidor LDAP con *Microsoft Outlook 2003*

Lo primero que debe hacer es agregar el directorio LDAP, para esto en el menú principal en "herramientas", se va a la opción que dice "cuentas de correo electrónico". Una vez ahí se selecciona la opción "agregar una nueva libreta de direcciones o directorio". Luego se selecciona la opción de "servicio de directorios de Internet (LDAP)".

Después aparecerá la ventana en la que se configura la información referente al directorio LDAP, en la que se debe ingresar la información referente. Igualmente se debe hacer clic en el botón "Mas configuraciones" y aparece otra ventana que tiene dos pestañas: "Conexión" y "Buscar", en donde debe ingresarse los datos correspondientes, una vez realizado la configuración de da doble *Enter* y se tendrá el directorio listo para ser accedido.

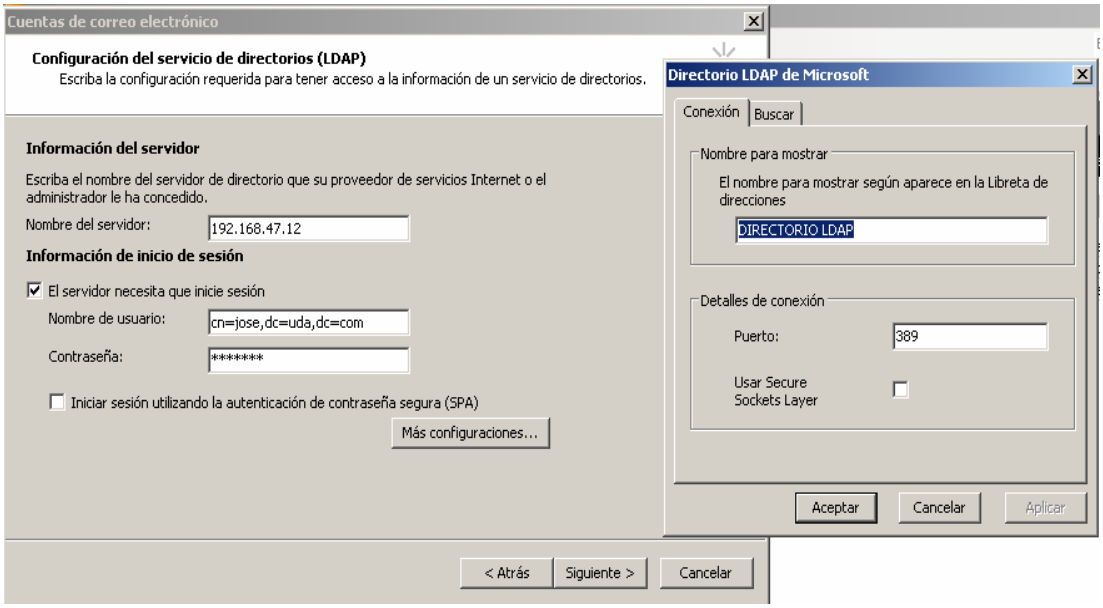

Figura 4.6: Cuadro de configuración de LDAP con *Outlook 2003*

Ahora se debe verificar que esté habilitada la barra de herramientas estándar, eso se lo hace yendo a la opción ver → barra de herramientas → estándar. Al tener habilitado la barra estándar, en esta misma se debe dar un clic en el icono de cuaderno para que nos muestre la ventana de libreta de direcciones.

En la ventana de la libreta de direcciones se debe seleccionar en el icono de cuaderno con una lupa para realizar la búsqueda deseada y en el combo box de la derecha se debe tener seleccionado el nombre del directorio (DIRECTORIO LDAP), en la ventana de búsqueda se debe seleccionar de igual manera los criterios deseados y al hacerlo, se regresara a la ventana de libreta de direcciones con los resultados de la búsqueda, si no encuentra coincidencias, se dará el mensaje de que eso ha ocurrido.

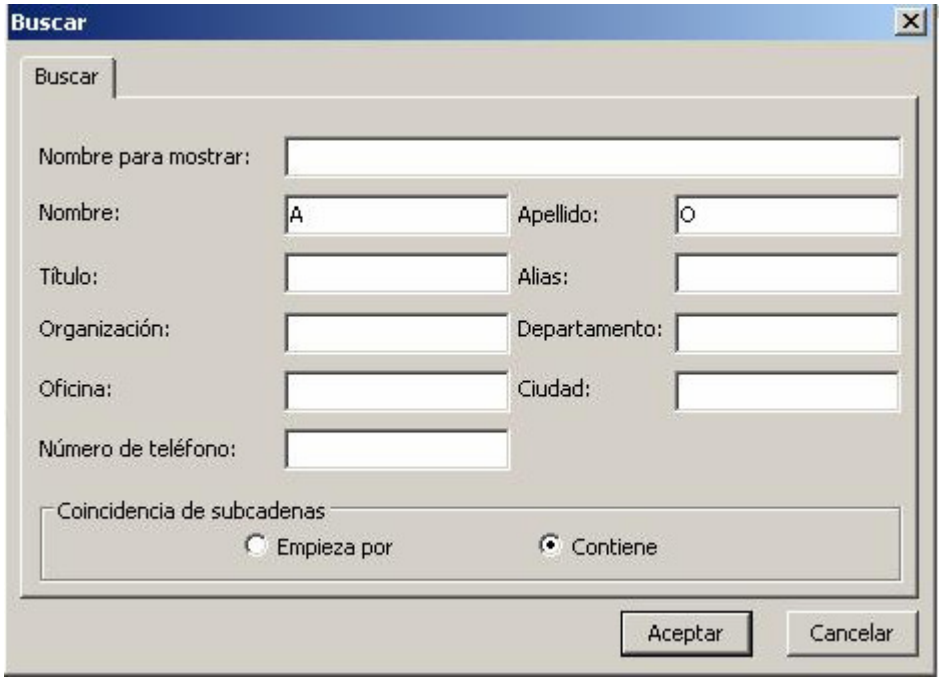

Figura 4.7: Ventana de búsqueda de entradas LDAP en *Outlook 2003*

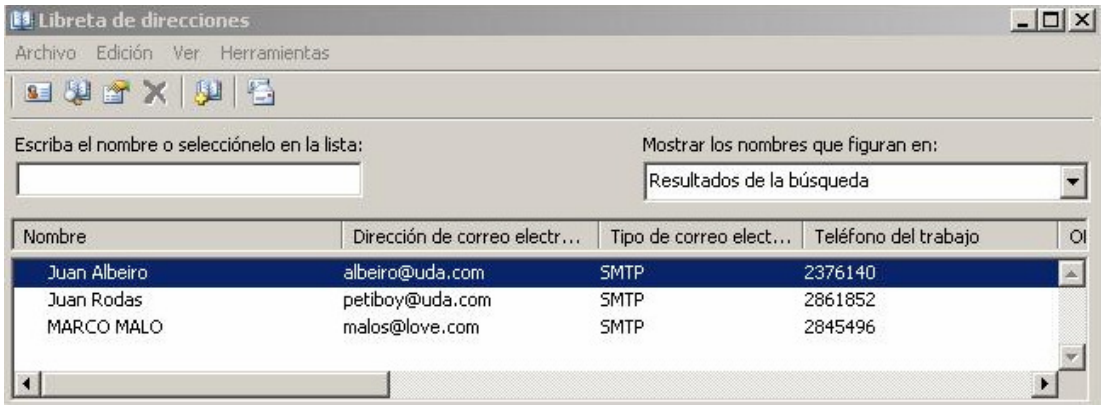

Figura 4.8: Resultado de la búsqueda del directorio LDAP en *Outlook 2003*

Después de haber realizado varias búsquedas, en la ventana de libreta de direcciones en el combo box de la derecha si se selecciona "DIRECTORIO LDAP" (el nombre al cual se lo llamo al directorio en el momento de configurar), nos mostrara los resultados de todas las búsquedas realizadas que se van almacenando ahí.

Al hacer doble clic sobre una entrada en particular nos mostrara las propiedades de este en la que nos da la opción de guardar el contacto localmente.

En la barra de herramientas estándar a la derecha del icono de cuadernos que se utilizo para acceder a la ventana de libreta de direcciones se encuentra una barra de búsqueda en la que utiliza un criterio de búsqueda en el cual si el nombre o el correo electrónico del contacto comienza con las letras especificadas en la barra de búsqueda, nos mostrara una ventana de comprobar nombres en la que nos muestra las coincidencias de búsqueda, si el resultado da un solo contacto, mostrara directamente las propiedades del mismo.

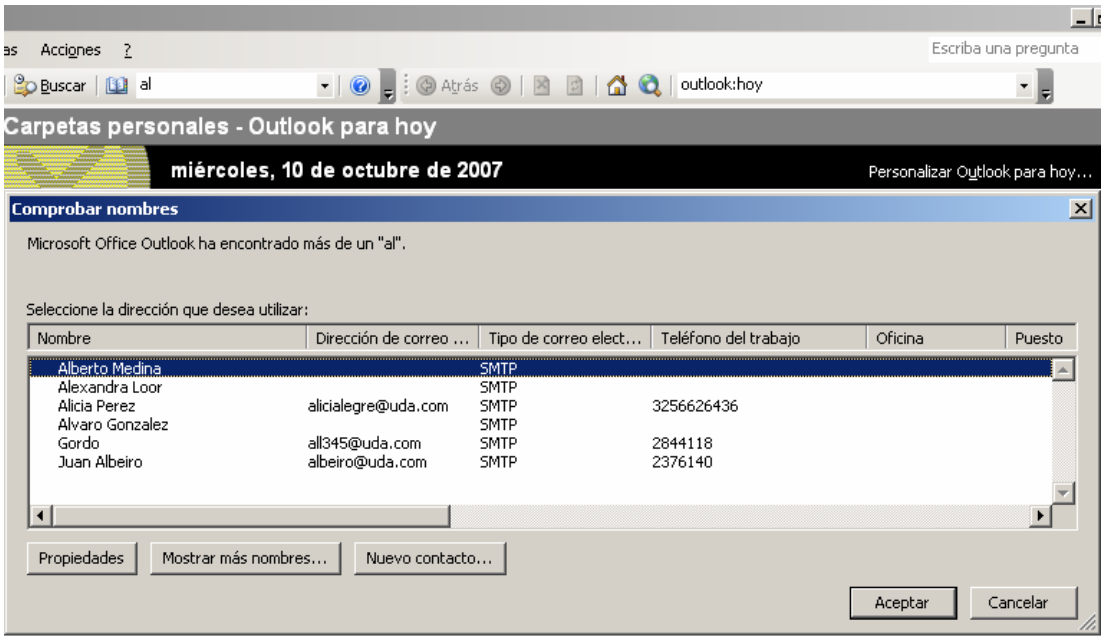

Figura 4.9: búsqueda por medio de la barra de herramientas estándar.

De igual manera es posible acceder al directorio al momento de enviar un mensaje de correo electrónico nuevo, en la barra de herramientas estándar se da clic en el botón "nuevo", una vez en esa ventana, en la barra de destinatarios se selecciona el botón que dice "Para" o "CC" que tienen además un icono de cuaderno, una vez seleccionado el botón, aparece una ventana de "seleccionar nombres" en la que nos muestra todas las entradas del directorio con las que se cuentan.

En el combo box se debe tener seleccionado el nombre del directorio LDAP, para que nos visualice los contactos del directorio LDAP, además es posible seleccionar las libretas de direcciones locales que se hayan creado en *Outlook.*

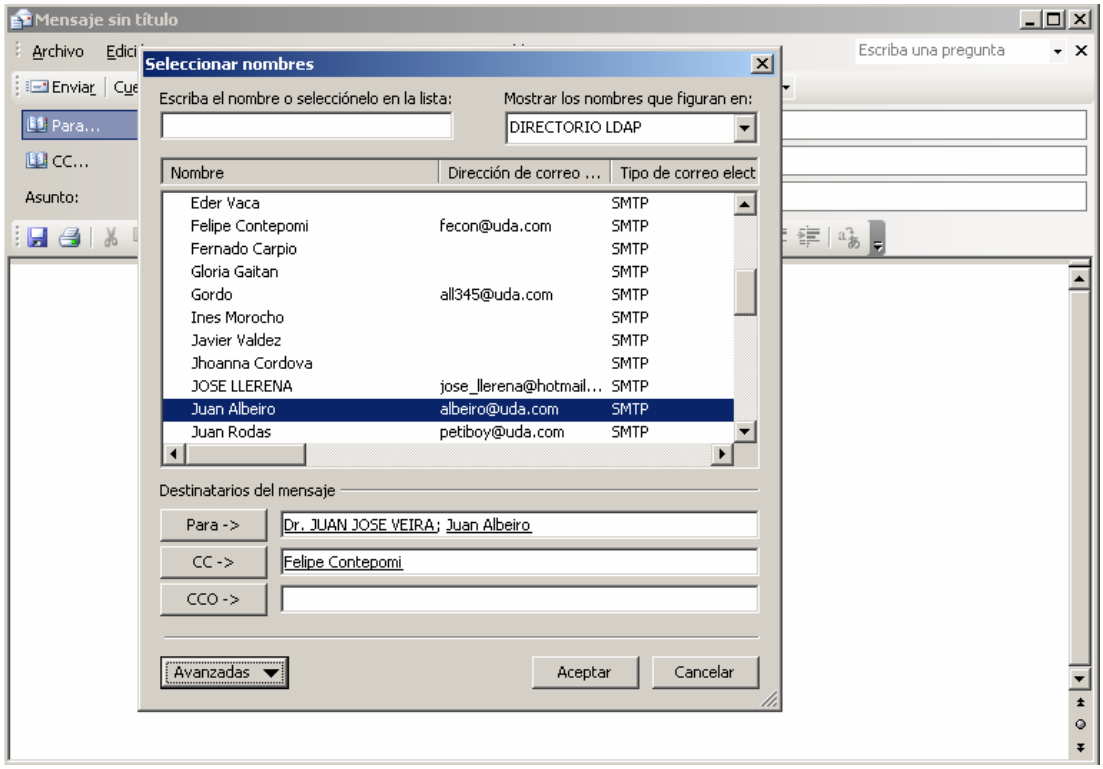

Figura 4.10: Ventana de seleccionar nombres del directorio LDAP para envió de un nuevo correo electrónico

CONCLUSIONES

Como conclusión se puede observar la manera que tiene un directorio LDAP de interactuar con programas cliente de correo electrónico de plataforma Windows y como estos acceden al directorio y la forma en la cual manejan la información almacenada en el servidor de directorios LDAP.

Finalmente se puede agregar que normalmente se utiliza el servicio de LDAP cuando se cuenta con un gran numero de registros dentro del ambiente en donde se este trabajando, cuando se trabaja con un numero pequeño de registros no es muy común el uso del servicio LDAP.

CONCLUSIONES

Los conceptos teóricos permiten conocer las definiciones más útiles e importantes en el servidor de directorios LDAP, los cuales permitirán conocer con mayor nivel de detalle y que de aquí hacia delante va a servir y ayudar para realizar los distintos tipos de configuraciones, soportes y pruebas posibles que se pueden realizar con el servidor LDAP.

Al realizar las instalaciones, pruebas, configuraciones y creaciones de directorios se pueden acceder a los directorios con diferentes programas de tipo correo, libretas de direcciones, al tener la correcta configuración se vera los datos tal y como se crearon con los comandos de LDAP.

La importancia, utilidad y practicidad de contar con un directorio personal como una agenda personal, información de artículos, de factura o de cualquier tipo ayudara a mantener organizada y ordenada la información dentro de un grupo dado, además de mantener al día esa información.

Es importante entender como funciona el directorio y como trabaja la base de datos, en la que se llega a conocer su manera de actuar y trabajar, que es lo mas recomendable hacer para cada operación de ingreso, modificado, eliminado o búsquedas, su definición define como va a trabajar la base de datos con el directorio y con el servidor LDAP .

La creación de certificados permite utilizar soporte para seguridades en capa de transporte, el cual utiliza el mismo puerto vía TCP, ayuda a que al momento de transportar datos, provea de confidencialidad y los datos mantendrán toda su integridad.

El servidor de directorios LDAP es un tema de mayor amplitud con la que se ha trabajado, en la que se puede realizar mayores configuraciones, otro tipo de soportes, en las que se pueden utilizar varios programas cliente para acceder a las distintas configuraciones que pueda tener el servidor.

El servidor LDAP puede funcionar tanto en una red domestica, como en una red grande o corporativa, dentro del mundo del Internet, el protocolo LDAP es bastante utilizado y se puede acceder a el de distintas maneras siempre que se cuente con el soporte dado y necesario.

RECOMENDACIONES

- El usuario administrador del sistema es el único que debe tener acceso al archivo de configuración del servidor, como para los distintos archivos de configuración de esquemas, contraseñas y todo lo relacionado con la configuración.
- Establecer contraseñas que sean de fácil recordatorio y mas recomendable es el utilizar combinación de letras mayúsculas y minúsculas además de números.
- Para realizar las distintas pruebas con el servidor de directorios es preferible previamente el contar con un conocimiento teórico que sirva de base para el momento práctico.
- El servidor LDAP viene por defecto con el sistema operativo Linux pero si en el caso de que no se cuente con los archivos de LDAP y se desea hacer la instalación, se recomienda revisar el punto 2.1.
- Es bueno utilizar atributos y objetos creados por uno mismo para tener mayor familiaridad con los registros, aunque esto impedirá el acceso al directorio por parte de varias aplicaciones (incluyendo las usadas en el capitulo 4) y si se llega a utilizar atributos definidos previamente, es importante entender su estructura y el significado de cada uno.
- Para usuarios principiantes es preferible usar autenticación simple, cuando se cuente con mayor experiencia se puede usar distintos métodos de autentificación.
- Para la creación de registros se debe utilizar estructura jerárquicas, al menos un objeto padre y uno que sea su hijo.
- Cuando se utilizan los distintos comandos de LDAP es necesario especificar el nombre distinguido (DN) tal y como se especifica en el archivo de formato LDIF.
- Es recomendable que regularmente se realicen respaldos de la información de los directorios.
- De igual manera es muy importante mantener el directorio actualizado constantemente para evitar inconsistencia de información.

GLOSARIO

Access: Traducción del ingles para **"**acceso".

Argfile: El nombre del archivo que tendrá las opciones de la línea de comandos del servidor si este se inicia sin la opción de depuración.

BDB: Siglas que significan Berkeley Data Base.

Cookie: Dato enviado de un servidor web al navegador del cliente que se guarda localmente en la maquina del usuario. Contiene información que identifican al usuario.

CP: Comando que permite copiar uno o varios archivos de un directorio a otro.

DC: Siglas que significan domain component o componente de dominio en español

DcObject: Nombre de un objeto que tiene como atributo dc.

Desc: Atributo que quiere decir descripción. Parte de la definición de un atributo en la que va la descripción de ese atributo entre comillas.

Directory: Traducción del ingles para directorio.

Dp: Atributo utilizado para abreviar departamento.

Em: Atributo utilizado para abreviar empresa.

Equality: Identificador de atributo que significa igualdad de correspondencia.

FTP: Siglas para File Transfer Protocol o protocolo de transferencia de archivos.

GidNumber: Índice que hace referencia al numero de ID de un grupo dado.

Givenname: Atributo usado para el nombre.

InetOrgPerson: Objeto que contiene los atributos de sn y cn (surname o apellido y common name o nombre completo respectivamente).

LDAP: Siglas que significan Lightweight Directory Access Protocol o protocolo de acceso a directorio ligero.

LDIF: Siglas de LDAP interchange format o formato de intercambio LDAP, es el formato de los archivos sobre los cuales LDAP actúa.

Lightweight: Traducción del ingles de peso ligero.

Login: Clave de acceso que se asigna a un usuario para que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de una red junto con la dirección electrónica de la computadora que utiliza.

Make: Utilidad o comando que permite hacer distintas operaciones como recompilados, dependencias, pruebas e instalaciones.
Nc: Atributo que hace referencia al nombre complete de una persona.

NIS: Siglas de Network Information Service o Servicio de Información de Red, es un servicio utilizado para gestionar bases de datos distribuidas dentro de un ambiente de red.

NisMapEntry: Índice utilizado en la configuración del servidor para hacer referencia a entrada de NIS.
NisMapName: Índice utilizado en la configuración del servidor para hacer referencia al nombre del NIS.
Nm: Atributo utilizado para abreviar nombre.
NSS: Siglas usadas para Name Service Switch o cambio de servicio de nombre, permite a LDAP actuar como servicio de nombre.
ObjectClass: patrón que hace referencia al la clase de objeto en cuestión.
Obsolete: Identificador de un atributo en la que indica si esta o no obsoleto.
OID: Identificador de objeto único.
Openldap: Paquete donde están los distintos archivos de LDAP.
OpenSSL: Es un grupo de herramientas criptográficas que implementan protocolos de red como SSL, SSL y estándares sobre criptografía relacionada que son requeridas.
Ordering: Identificador de atributo de regla de correspondencia si está permitida la ordenación; ausente si no está permitida.
PAM: Siglas de Pluggable Authentication Module o modo de autenticación enchufable.
Pidfile: Archivo referente al ID del proceso del servidor *slapd*.
Protocol: Traducción del ingles de protocolo.
RDN: Siglas utilizadas para *relative distinguished name.*
Realm: Es un dominio.
RA: Siglas utilizadas para Registration **A**uthority o Autoridad de Registro.

RSA: Algoritmo criptográfico de clave pública el cual está patentado por los autores que lo crean.

Schema Es una plantilla que contiene la definición de los valores y datos de los posibles atributos que se pueden introducir en un árbol LDAP. Así las entradas que son permitidas en un árbol LDAP son aquellas que cumplen una definición de alguno de los esquemas que se incluyen en la configuración del servidor LDAP.

Script: Es un grupo líneas de ordenes que constituyen un programa.

Shell: Programa por el cual un usuario se comunica con el sistema operativo.

Slapd: El nombre del archive de configuración del servidor LDAP, también es usado como un comando.
Slurpd: Dominio que se encarga de hacer replicación con la ayuda de *slapd*.
Sn: Atributo que significa Surname en español se refiere a apellido.

SSL: Siglas utilizadas para Secure Socket Layer. Que permite la transmisión encriptada, en el cual sólo el servidor y el cliente podrán entender lo enviado.
Substring: Identificador de atributo referente a la regla de correspondencia si es que está permitida la correspondencia de sub-string, ausente si no lo está.
SUP: Tipo de atributo superior del que se deriva el atributo definido.
Syslog: Syslog es un servicio de registro de datos que es frecuentemente usado en entornos Linux y Unix. Lo que hace Syslog es que el registro de sucesos e información es enteramente manejado por un servidor dedicado llamado 'Servidor Syslog'.
TLS: Siglas para Transport Layer Security o seguridad de capa de transporte.
TLSCertificateFile: Archivo de certificación de la capa de seguridad de transporte.
TLSCACertificateFile: Archivo de autorización de certificado de la capa de seguridad de transporte.
TLSCertificateKeyFile: Archivo donde se ubica la llave de la certificación de la seguridad de capa de transporte.
UidNumber: Numero de identificador único.
URI: Siglas para Uniform Rescue Identifier.
X.509: Es un estándar de redes de ordenadores sobre servicios de directorio, son como bases de datos de direcciones electrónicas. Estándar desarrollado en conjunto con la ISO.

BIBLIOGRAFIA

Libros:

Suse Linux Professional 9.1 User Guide. Edition 2004

Suse Linux Professional 9.1 Administration Guide. Edition 2004

Artículos de Internet:

www.linuxparatodos.com. Linux para todos. [consulta 09 de julio del 2007].

www.ecualug.org. Grupo de usuarios de LINUX. [consulta 09 de julio del 2007].

www.bulma.net. Usuarios de Linux de Balears. [consulta 09 de Julio del 2007].

http://www.openldap.org/. OpenLdap. [consulta 10 de Julio del 2007].

http://www.rage.net/ldap/. Linux Directory Services. [consulta 11 de julio del 2007].

http://www.tldp.org/HOWTO/LDAP-HOWTO/. Ldap Linux HOWTO. [consulta 11 de Julio del 2007].

es.tldp.org/Tutoriales/doc-open**ldap**-samba-cups-python/htmls/open**ldap**-que-es.html. Que es LDAP?. [consulta 12 de julio del 2007].

es.wikipedia.org/wiki/**LDAP.** Wikipedia La enciclopedia libre. [consulta 12 de Julio del 2007].

www.**ldap**man.org/articles/sp_intro.html. An introduction to Ldap. [consulta 12 de julio del 2007].

www.osmosislatina.com/soporte/**ldap**.htm. Ldap. [consulta 12 de julio del 2007].

en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol. Ldap Wikipedia The free encyclopedia. [consulta 12 de julio del 2007].

www.umich.edu. University of Michigan. [consulta 26 de Julio del 2007].

www.glosario.panacom.com. Glosario Informática e Internet. [consulta 9 de Agosto del 2007].

www.web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ldap.html Demonios y utilidades OpenLdap. [consulta 17 de Agosto del 2007].

ANEXOS

Anexo 1: Diseño de Monografía.