ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

"ANÁLISIS DE LAS IMPLEMENTACIONES DEL PROTOCOLO LDAP. CASO PRÁCTICO: IMPLANTACIÓN DE UN SISTEMA DE AUTENTICACIÓN APLICADO A LOS LABORATORIOS DE LA EIS"

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

DAVID ANÍBAL OLEAS BRAVO

RIOBAMBA ECUADOR

2013

AGRADECIMIENTO

A Dios y al Grupo 24 horas de Alcohólicos Anónimos Riobamba, por haberme dado la oportunidad de integrarme a la sociedad y brindarme una vida útil y feliz, a mi madre por el amor, paciencia y tolerancia en todos estos años de estudio, a mis hermanas Mónica, Aída y Margarita por confiar en mí y haber sustentado toda mi carrera y la mayor parte de mi vida, por eso les estoy eternamente agradecido, y como no, a todos mis amigos por el apoyo moral, respeto y afecto que me tienen. Gracias por haberme hecho alcanzar un sueño.

DEDICATORIA

A Dios.

Por permitirme culminar esta etapa de mi vida y haberme dado la salud mental para lograr mis objetivos, además de su infinita bondad y amor.

A mi hermana Mónica.

Por ser un ejemplo de esfuerzo y trabajo y estar en los momentos que más te necesitó la familia.

A mi hijo Ronald Jair.

Por ser un motivo latente de superación y amor, por tocar mi alma y ser parte de mi vida.

NOMBRE	FIRMA	FECHA
Ing. Iván Menes		
DECANO	**….....**	**.....**
Ing. Raúl Rosero		
DIRECTOR DE LA		
ESCUELA	**….....**	**.....**
Ing. Danilo Pástor		
DIRECTOR DE TESIS	**….....**	**.....**
Ing. Patricio Moreno		
MIEMBRO DEL TRIBUNAL	**.....**	**.....**
Tlgo. Carlos Rodríguez		
DIRECTOR DPTO	**.....**	**.....**
DOCUMENTACIÓN		
NOTA DE LA TESIS	**.....**	

RESPONSABILIDAD DEL AUTOR

Yo, David Aníbal Oleas Bravo, soy responsable de las ideas y doctrinas y resultados expuestos en esta Tesis y el patrimonio de la misma pertenece a la Escuela Superior Politécnica de Chimborazo.

_____

David Aníbal Oleas Bravo

INDECE DE ABREVIATURAS

A

ACL Access Control List

AIX Advanced Interactive eXecutive

AOL America Online (an internet service)

API Interfaz de programación de Aplicaciones

B

BSD Berkeley Software Distribution

C

CDDL Common Development and Distribution License

D

DAP Directory Access Protocol

DBMS Database Management System

DIT Data Information Tree

DIXIE Directory Assistance Service

DNS Domain Name Server

DSE Directory Service Entry

DSML Directory Service Markup Language

F

FTP Protocol Transfer file

G

GNU GNU No es UNIX

I

IBM International Business Machines Corporation

IETF Internet Engineering Task Force

ISP Internet Service Provide

ITU International Telecommunications Union

J

JDK Java Development Kit

JRE Java Runtime Environment

L

LDAP Lightweight Directory Access Protocol

LDBP Lightweight Directory Browsing Protocol

O

OSI Open Systems Interconnection

R

RADIUS Remote Authentication Dial-In User Server

RDN Relative Distinguished Name

RFC Request For Comments

S

SLP Service Location Protocol

SPML Service Provisioning Markup Language

SSL Secure Socket Layer

T

TLS Transport Layer Security

X

XED XML Enabled Directory

XML Extensible Markup Language

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo de investigación de tesis previo a la obtención del título de Ingeniería en Sistemas Informáticos, trata sobre el “ANALISIS DE LAS IMPLEMENTACIONES DEL PROTOCOLO LDAP. CASO PRACTICO: IMPLANTACION DE UN SISTEMA DE AUTENTICACION APLICADO A LOS LABORATORIOS DE LA EIS”.

Es un análisis investigativo completo sobre las diferentes implementaciones del protocolo LDAP, tiene como finalidad obtener la implementación más óptima para realizar autenticaciones de usuarios y poder controlar la información de forma centralizada.

Como precedente, de lo que estamos tratando es de un Controlador de Dominio, que cumple con la función de administrar la información de una organización o empresa de una manera correcta, almacenando todos los datos de la organización en Directorios en forma jerárquica y organizada. Una de las utilidades que se puede sacar de este tipo de implementaciones es la autenticación de los usuarios, permitiendo gestionar el ingreso de los mismos.

El presente trabajo contiene los siguientes capítulos:

En el capítulo 1 se presenta el planteamiento de la investigación, antecedentes, hipótesis, métodos y técnicas, es todo el marco referencial para el desarrollo de la tesis.

El capitulo 2 muestra el Marco Teórico en general, los conceptos, arquitectura y funcionamiento del protocolo LDAP.

En el capítulo 3 se realiza la presentación de las implementaciones del protocolo LDAP, donde por medio de la investigación y encuestas realizadas se elijen las más populares para proceder al análisis comparativo y poder definir la ganadora entre ellas.

El capítulo 4 consiste en la implementación de forma real, configurando un servidor de autenticación e ingresando datos reales para poner a prueba el proyecto efectuado.

1. CAPÍTULO I

MARCO REFERENCIAL

1.1. ANTECEDENTES

1.1.1. PLANTEAMIENTO DEL PROBLEMA.

1.1.1.1. DESCRIPCIÓN DEL OBJETO DE ESTUDIO.

El Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos. [1]

El problema de la autorización a menudo, es idéntico a la de autenticación; muchos protocolos de seguridad han adoptado estándares y regulaciones obligatorias. Sin embargo, el uso más exacto describe la autenticación como el proceso de verificar la identidad de una persona, mientras la autorización es el proceso de verificación que una persona conocida tiene la autoridad para realizar una cierta operación. La autenticación por lo tanto, debe preceder la autorización. [3]

Cuando no se aplica un protocolo de acceso a datos dentro de una red en general no se puede gestionar la información de los usuarios que han solicitado el uso de algún servicio, tampoco habrá un control de acceso para cierto determinado grupo de clientes o personas.

La Escuela Superior Politécnica de Chimborazo cuenta con una tecnología de punta y con una excelente organización informática, pero carece el control de usuarios dentro de los laboratorios.

En el departamento técnico de la Escuela de Ingeniería en Sistemas de la Escuela Superior Politécnica de Chimborazo, no existe un sistema de autenticación que gestione la información de los usuarios y se optimicen recursos dentro de esta dependencia, la única forma que los técnicos controlan el ingreso de los usuarios es a nivel de registro, formularios impresos en papel, en donde muchas veces los usuarios no se registran y no se lleva el control de quien uso dicha máquina.

En la actualidad el ingreso a cada máquina se lo realiza solo a nivel de cuentas de usuario y autenticación propia de cada sistema operativo llamadas (Administrador y Sistemas), en donde cualquier persona puede hacer uso de estos recursos, incluso sin ser miembro de esta institución.

1.1.2. SITUACIÓN ACTUAL DEL OBJETO DE ESTUDIO.

LDAP son las siglas de Lightweight Directory Access Protocol (en español *Protocolo Ligero de Acceso a Directorios*) que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado

una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos u organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).

Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red. [9]

Por lo tanto es muy importante saber elegir dónde es conveniente usarlo. No será conveniente como base de datos para sitios que realicen constantes modificaciones de datos.

1.1.3. ANÁLISIS DEL OBJETO DE ESTUDIO.

Usos Empresariales

Dadas las características de LDAP sus usos más comunes son:

- **Directorios de información**. Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) o cualquier tipo de páginas amarillas.
- **Sistemas de autenticación/autorización centralizada**. Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos. Por ejemplo:
    - **Active Directory Server de Microsoft,** para gestionar todas las cuentas de acceso a una red corporativa y mantener centralizada la gestión del acceso a los recursos.
    - **Sistemas de autenticación para páginas Web,** algunos de los gestores de contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.
    - **Sistemas de control de entradas a edificios, oficinas.**
- **Sistemas de correo electrónico.** Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.
- **Sistemas de alojamiento de páginas web y FTP,** con el repositorio de datos de usuario compartido.
- **Grandes sistemas de autenticación basados en RADIUS,** para el control de accesos de los usuarios a una red de conexión o ISP.
- **Servidores de certificados públicos y llaves de seguridad**

- **Autenticación única ó "single sign-on"** para la personalización de aplicaciones.
- **Perfiles de usuarios centralizados,** para permitir itinerancia ó "roaming"
- **Libretas de direcciones compartidas**.

Servidores LDAP disponibles en el mercado

Existen diversas implementaciones y aplicaciones reales del protocolo LDAP:

Active Directory

Active Directory es el nombre utilizado por Microsoft (desde Windows 2000) como almacén centralizado de información de uno de sus dominios de administración.

Un Servicio de Directorio es un depósito estructurado de la información de los diversos objetos que contiene el Active Directory, en este caso podrían ser impresoras, usuarios, equipos, etc.

Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAP versión 3, lo cual permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc.

Novell Directory Services

También conocido como **eDirectory** es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Básicamente está compuesto por una base de datos jerárquica y orientada a objetos,

que representa cada servidor, computadora, impresora, servicio, personas, etc. entre los cuales se crean permisos para el control de acceso, por medio de herencia. La ventaja de esta implementación es que corre en diversas plataformas, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo.

iPlanet - Sun ONE Directory Server

Basado en la antigua implementación de Netscape, iPlanet se desarrolló cuando AOL adquirió Netscape Communications Corporation y luego conjuntamente con Sun Microsystems comercializaron software para servidores, entre ellos el iPlanet Directory Server, su implementación de LDAP... Actualmente se denomina Sun ONE Directory Server.

OpenLDAP

Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP.

Tiene su propia licencia, la OpenLDAP Public License. Al ser un protocolo independiente de la plataforma, varias distribuciones GNU/Linux y BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS.

Red Hat Directory Server

Directory Server es un servidor basado en LDAP que centraliza la configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas así como información de control de acceso dentro de un sistema operativo independiente de la plataforma.

Forma un repositorio central para la infraestructura de manejo de identidad, simplifica el manejo de usuarios, eliminando la redundancia de datos y automatizando su mantenimiento.

Apache Directory Server

Apache Directory Server (ApacheDS), es un servidor de directorio escrito completamente en Java por Alex Karasulu y disponible bajo la licencia de Apache Software, es compatible con LDAPv3 certificado por el Open Group, soporta otros protocolos de red tal como Kerberos y NTP, además provee Procedimientos Almacenados, triggers y vistas; características que están presente en las Base de Datos Relacionales pero que no estaban presentes en el mundo LDAP.

Open DS

Basado en los estándares LDAPv3 y DSMLv2, OpenDS surgió como un proyecto interno de SUN, aunque posteriormente se puso a disposición de la comunidad. Está desarrollado en JAVA y precisa de un entorno de ejecución (Java Runtime Environment) para funcionar. Es multiplataforma. [4]

1.1.4. DELIMITACIÓN

El presente estudio se encontrará enfocado en un análisis comparativo de las diferentes implementaciones del protocolo LDAP, para determinar la mejor opción que permita implantar un sistema de autenticación controlado desde un servidor en los laboratorios de la Escuela de Ingeniería en Sistemas.

La arquitectura que se empleará para el protocolo LDAP es cliente servidor, por esta razón en el presente proyecto se analiza e implementa una autenticación de cuentas de usuario, en la cual se tendrá que configurar un servidor LDAP.

Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.).

El aplicar la autenticación con la mejor implementación LDAP es brindar el control y gestión de los usuarios que requieran hacer uso de las máquinas del laboratorio de redes de la Escuela de Ingeniería en sistemas, lugar donde se llevará a cabo la implementación de este proyecto.

1.1.5. FORMULACIÓN DEL PROBLEMA

¿Cuál es la mejor implementación del protocolo LDAP para el control de un sistema de autenticación en un entorno de red?

1.1.6. SISTEMATIZACIÓN

- ¿Qué es un Directorio Activo?
- ¿Qué es LDAP?
- ¿Cuáles son las características de un servidor LDAP?
- ¿Cuáles son las ventajas de aplicar un servidor LDAP?
- ¿Cuál es la Administración de LDAP?
- ¿Cómo se encuentra estructurada la Arquitectura básica de un Servidor LDAP?

- ¿Cuáles son los servidores que se pueden implementar con el protocolo LDAP?
- ¿Cuál es la mejor implementación del protocolo LDAP para un sistema de autenticación?

1.1.7. JUSTIFICACIÓN DEL PROYECTO DE TESIS.

Justificación Teórica.

LDAP *(Protocolo Ligero de Acceso a Directorios)* es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

El beneficio de configurar LDAP es manejar la información, en este caso de los usuarios de una manera, jerárquica y organizada para poder efectuar la autenticación de los usuarios que requieran el uso de una computadora dentro de un laboratorio. La información de los datos de autenticación se validará de una forma segura para los usuarios brindando a la institución la facilidad de poder gestionarla información, optimizar recursos y llevar en control automatizado de dicha información.

Justificación Práctica.

Como se ha visto en resumen LDAP es una base de datos optimizada para entornos donde se realizan muchas lecturas de datos y pocas modificaciones o borrados.

Existen diferentes implementaciones para poder configurar un servidor LDAP, esto dependerá de la plataforma en la que deseemos implementarlo como por ejemplo

Novell Directory Services que es una implementación de Novell, iPlanet Sun ONE Directory Server basado en la antigua implementación de Netscape y para Linux OpenLDAP y otras implementaciones más, de las cuales se analizan todas las herramientas y en base a un estudio comparativo entre las más adecuadas se implementará la que mejor beneficio nos brinde.

Cada usuario se identifica por un nombre de usuario y los atributos asignados son la contraseña, los permisos de acceso, los grupos de trabajo a los que pertenece, la fecha de caducidad de la contraseña.

Este sistema de autenticación recibirá una consulta cada vez que el usuario acceda a la red y una más cada vez que acceda a los recursos del grupo de trabajo (directorios compartidos, impresoras…) para comprobar los permisos del usuario. Frente a estos cientos de consultas solo unas pocas veces se cambia la contraseña de un usuario o se le incluye en un nuevo grupo de trabajo.

En los laboratorios de la EIS es el lugar donde se llevará a cabo la implementación del servidor de autenticación, como la infraestructura con la que cuenta es en red entonces cada vez que un usuario necesite hacer uso de las computadoras se mostrará una pantalla de autenticación, la cual una vez ingresado los datos estos serán validados en el servidor LDAP.

1.1.8. OBJETIVOS

1.1.9. OBJETIVO GENERAL

Analizar las implementaciones del protocolo LDAP para implantar un sistema de autenticación aplicado a los laboratorios de la EIS.

1.1.10. OBJETIVOS ESPECÍFICOS:

- Estudiar la arquitectura del protocolo LDAP.
- Analizar y comparar las implementaciones del protocolo LDAP, y seleccionar la más adecuada de acuerdo a parámetros y métricas de evaluación.
- Implementar un sistema de autenticación LDAP para los laboratorios de la Escuela de Ingeniería en Sistemas.

1.1.11. HIPÓTESIS.

El análisis de las implementaciones del protocolo LDAP permitirá escoger la más adecuada para el desarrollo de un sistema de autenticación en los laboratorios de la Escuela de Ingeniería en Sistemas.

1.1.12. MÉTODOS Y TÉCNICAS

El método utilizado como guía para la presente investigación es el método científico que avalará nuestra investigación sobre la autenticación con LDAP, y a su vez contempla los siguientes puntos que involucran el desarrollo de esta tesis:

- El planteamiento del problema motivo del presente trabajo.
- El apoyo del proceso previo a la formulación de la Hipótesis.
- El proceso de recopilación de la información necesaria.
- Análisis e interpretación de Resultados.
- El proceso de Comprobación de la Hipótesis, etc.

También se utilizará como complemento del presente trabajo al método Analítico – Sintético, como lo dice su nombre, es el análisis que se realizará de los aspectos delimitados de la presente investigación que permitirá conocer, comprender y estudiar sobre el servidor LDAP en partes y del todo investigado en sus diferentes componentes para la implementación propuesto por el autor. Además el mismo, es aplicado en la sistematización de la bibliografía IENTA.

2. CAPÍTULO II

MARCO TEORICO

2.1. INTRODUCCIÓN A LDAP

LDAP ("Lightweight Directory Acces Protocol", en español Protocolo Ligero de Acceso a Directorios) es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

Se usó inicialmente como un Front-end o interfaz final para x.500, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

¿Qué es un directorio?

Un directorio es una base de datos, pero en general contiene información más descriptiva y más basada en atributos.

La información contenida en un directorio normalmente se lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos, Las actualizaciones en un directorio son usualmente cambios sencillos de todo o nada, si es que permiten algo.

Los directorios están para proporcionar una respuesta rápida a operaciones de búsqueda o consulta.

Pueden tener capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y fiabilidad, y a la vez reducir tiempo de respuesta. Cuando se duplica la información de un directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización.

Hay muchas formas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados. Algunos servicios de directorios son locales, proporcionando servicios a un contexto restringido. Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

¿Un directorio LDAP es una base de datos?

El sistema gestor de una base de datos (Database Management System ó DBMS) de Sybase, Oracle, Informix ó Microsoft es usado para procesar peticiones (queries) ó actualizaciones a una base de datos relacional. Estas bases de datos pueden recibir cientos o miles de órdenes de inserción, modificación o borrado por segundo.

Un servidor LDAP es usado para procesar peticiones (queries) a un directorio LDAP. Pero LDAP procesa las órdenes de borrado y actualización de un modo muy lento. En otras palabras, 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. [15]

2.2. HISTORIA

Las compañías de telecomunicaciones introdujeron el concepto de servicios de directorio a Tecnologías de Información y Redes de Computadoras, así su comprensión de los requerimientos de directorios era bien desarrollado después de 70 años de producir y manejar directorios de teléfonos. La culminación de este esfuerzo fue la especificación X.500, un conjunto de protocolos producido por la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) en la década de 1980.

Los servicios de directorio X.500 fueron accedidos tradicionalmente vía DAP (Directory Access Protocol), que requería la pila de protocolos OSI (Open Systems Interconnection). LDAP fue originalmente dirigido a ser un protocolo alternativo y ligero para acceder a servicios de directorio X.500 a través de la pila de protocolos más simple (y ahora más difundido) TCP/IP. Este modelo de acceso a directorio fue imitado de los protocolos DIXIE Directory Assistance Service.

Servidores de directorio LDAP independientes pronto fueron implementados, así como los servidores de directorio que soportaban DAP y LDAP. El último se hizo popular en empresas debido a que eliminaba cualquier necesidad de desplegar una red OSI. Ahora, los protocolos de directorio X.500 incluyendo DAP pueden ser usados directamente sobre TCP/IP.

El protocolo fue creado originalmente por Tim Howes (University of Michigan), Steve Kille (Isode Limited), y Wengyik Yeong (Performance Systems International) hacia 1993. Un desarrollo más completo ha sido hecho por la Internet Engineering Task Force.

En las primeras etapas de ingeniería de LDAP, éste era conocido como *Lightweight Directory Browsing Protocol*, o *LDBP*. Posteriormente fue renombrado dado que el

ámbito del protocolo había sido expandido para incluir no sólo navegación en el directorio y funciones de búsqueda, sino también funciones de actualización de directorio.

LDAP ha influenciado protocolos posteriores de Internet, incluyendo versiones posteriores de X.500, XML Enabled Directory (XED), Directory Service Markup Language (DSML), Service Provisioning Markup Language (SPML), y Service Location Protocol (SLP). [10]

LDAP aparece con el estándar de los directorios de servicios, originalmente para gestionar directorios telefónicos.

La primera versión fue desarrollada por la Universidad de Michigan. Hasta 1995 no se publicaron los RFC (Request For Comments) de la versión LDAPv2.

Los RFC para la versión LDAPv3 fueron publicados en 1997. La versión 3 incluía características como las listas de acceso (control access lists) y replicación de directorios.

LDAP RFCs

Los RFCs asociados con LDAP son:

- RFC1777 - Lightweight Directory Access Protocol. (Obsoletes RFC1487)
- RFC1778 - The String Representation of Standard Attribute Syntaxes
- RFC1779 - A String Representation of Distinguished Names (Obsoletes RFC1485)
- RFC1823 - The LDAP Application Program Interface

- RFC1960 - A String Representation of LDAP Search Filters (Obsoletes RFC1558)
- RFC 2251 - Lightweight Directory Access Protocol (v3)
- RFC 2252 - LDAPv3 Attribute Syntax Definitions
- RFC 2253 - UTF-8 String Representation of Distinguished Names
- RFC 2254 - The String Representation of LDAP Search Filters
- RFC 2255 - The LDAP URL Format
- RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3
- RFC2829 Authentication Methods for LDAP.
- RFC2830 - Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security.

RFCs Relacionados

- RFC1274 - The COSINE and Internet X.500 Schema
- RFC1279 - X.500 and Domains
- RFC1308 - Executive Introduction to Directory Services Using the X.500 Protocol
- RFC1309 - Technical Overview of Directory Services Using the X.500 Protocol
- RFC1617 - Naming and Structuring Guidelines for X.500 Directory Pilots (Obsoletes RFC1384)
- RFC1684 - Introduction to White Pages services based on X.500
- RFC2079 - Definition of an X.500 Attribute Type and an Object Class to Hold Uniform [5]

2.3. CARACTERÍSTICAS DE LDAP

Las características propias del protocolo LDAP son:

Escalabilidad

Los directorios LDAP, particularmente cuando una base de datos relacional hace una copia de seguridad de ellos, como en IBM Secure Way Directory, son muy escalables. El rendimiento de los directorios de gran tamaño con millones de entradas es excelente.

Debido a la base estándar común, otro factor de escalabilidad es la posibilidad de configurar de manera simple hardware y software de mayores prestaciones. LDAP no se basa en un sistema operativo específico y es independiente del proveedor.

Disponibilidad

LDAP soporta la réplica y división de espacios de nombres. La réplica permite a varios servidores LDAP almacenar el contenido del mismo directorio. Esto permite a los clientes disponer de estos servidores adicionales cuando uno presenta anomalías.

La división permite almacenar las secciones de todo el directorio en diferentes ubicaciones de servidores distintos. Esto no sólo aumenta la disponibilidad (ni una sola anomalía) si no que simplifica la gestión distribuida.

Seguridad

LDAP soporta características de seguridad que impiden el acceso no autorizado a datos. Los protocolos de comunicación segura, como SSL y procedimientos de

autenticación, junto con las políticas de listas de control de accesos (ACL) para entradas de datos, garantizan el máximo nivel de seguridad.

Gestionabilidad

Las versiones actuales de LDAP, como IBM SecureWay Directory, proporcionan una interfaz gráfica de usuario tanto para la administración de sistemas como para la administración de datos de directorio. Su esquema ampliable dinámicamente le permite ampliar el esquema de directorios sin interrumpir el servicio.

Estandarización

El protocolo LDAP --junto con la mayoría de prestaciones de cliente/servidor relacionadas, las interfaces de programación de aplicaciones (API) y las definiciones de datos-- están definidos por estándares oficiales o los RFC (solicitud de comentarios) correspondientes.

Por ejemplo, Lightweight Directory Access Protocol (v3), RFC 2251, define el protocolo LDAP básico. En borradores de Internet hay definidas otras características, ampliamente aceptadas e implementadas. Gran parte de este trabajo lo llevan a cabo IETF (Internet Engineering Task Force) y DMTF (Distributed Management Task Force). [17]

2.4. ESTUDIO DE LA ARQUTECTURA DEL PROTOCOLO LDAP

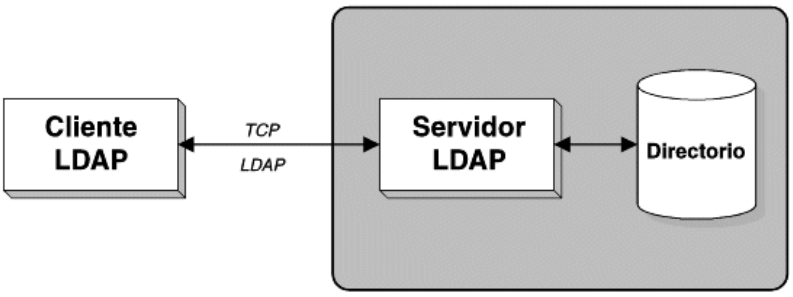


Figura II 1 Servidor LDAP Autónomo

Fuente: http://publib.boulder.ibm.com/tividd/td/ITAME/GC23-4684-00/es_ES/HTML/adminmst11.htm

El protocolo LDAP define el método para acceder a datos en el servidor a nivel cliente pero no la manera en la que se almacena la información.

El protocolo LDAP actualmente se encuentra en su 3era versión y el IETF (Grupo de Trabajo de Ingeniería de Internet) lo ha estandarizado. Por lo tanto, existe una RFC (petición de comentarios) para cada versión de LDAP que constituye un documento de referencia:

- RFC 1777 para LDAP v.2
- RFC 2251 para LDAP v.3

LDAP le brinda al usuario métodos que le permiten:

- conectarse
- desconectarse
- buscar información
- comparar información
- insertar entradas
- cambiar entradas

- eliminar entradas

Asimismo, el protocolo LDAP (en versión 3) ofrece mecanismos de cifrado (SSL, etc.) y autenticación para permitir el acceso seguro a la información almacenada en la base.

2.4.1. Estructura de árbol de la información (DIT)

LDAP presenta la información bajo la forma de una estructura jerárquica de árbol denominada **DIT** (*Árbol de información de directorio*), en la cual la información, denominada **entradas** (o incluso *DSE, Directory Service Entry*), es representada por bifurcaciones.

Una bifurcación ubicada en la raíz de una bifurcación se denomina *entrada raíz*.

Cada entrada en el directorio LDAP corresponde a un objeto abstracto o real (por ejemplo, una persona, un objeto material, parámetros, etc.).

Cada entrada está conformada por un conjunto de pares clave/valor denominados **atributos**.

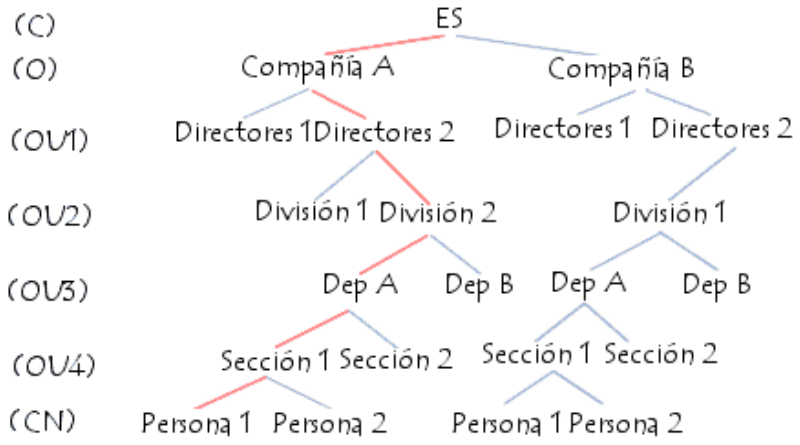


Figura II 2 Árbol Jerárquico

Fuente: http://es.kioskea.net/contents/internet/ldap.php3

2.4.2. Atributos de entrada

Cada entrada está compuesta por un conjunto de atributos (pares clave/valor) que permite caracterizar el objeto que la entrada define. Existen dos tipos de atributos:

- **Atributos normales**: éstos son los atributos comunes (apellido, nombre, etc.) que distinguen al objeto.
- **Atributos operativos**: éstos son atributos a los que sólo el servidor puede acceder para manipular los datos del directorio (fechas de modificación, etc.).

Una entrada se indexa mediante un **nombre completo** (**DN**) que permite identificar de manera única un elemento de la estructura de árbol.

Un DN se constituye tomando el nombre del elemento denominado *Nombre distintivo relativo* (*RDN*, es decir, la ruta de la entrada en relación con sus entradas superiores) y agregándole el nombre entero de la entrada principal.

Se trata de utilizar una serie de pares clave/valor para poder localizar una entrada de manera única. A continuación encontrará una serie de claves generalmente utilizadas:

- **uid** (*id de usuario*), ésta es una identificación única obligatoria;
- **cn** (*nombre común*), éste es el nombre de la persona;
- **givenname**, éste es el nombre de pila de la persona;
- **sn** (*apellido*), éste es el apellido de la persona.
- (*organización*), ésta es la compañía de la persona.
- **u** (*unidad organizacional*), éste es el departamento de la compañía para la que trabaja la persona.
- **mail**, ésta es la dirección de correo electrónico de la persona (por supuesto).

Por lo tanto, un *nombre completo* tendrá la siguiente forma:

uid=doleas, cn=david, givenname=banner

Le *Nombre Distintivo Relativo es* "*uid=doleas*".

Así, el conjunto de definiciones de objetos y atributos que un servidor LDAP puede administrar se denomina **esquema**. Esto permite, por ejemplo, definir si un atributo puede poseer uno o varios valores. Además, un atributo llamado *objectclass* permite definir si los atributos son obligatorios u opcionales. [13]

3. CAPITULO III

ANALISIS COMPARATIVO DE LAS IMPLEMENTACIONES LDAP

3.1. Determinación de las Implementaciones a comparar

En la actualidad existen varias implementaciones del Protocolo LDAP, para lo cual se ha realizado una investigación previa, como artículos publicados en el Internet que certifiquen cuál de ellas son las más populares o las más utilizadas.

- Partimos como referencia del portal educativo de wikipedia "http://es.wikipedia.org/wiki/LDAP", en donde nos lista algunas de las implementaciones según el criterio de esta página. [13]
    - Active Directory
    - Novell Directory Services
    - iPlanet – Sun ONE Directory Server
    - OpenLDAP
    - Red Hat Directory Server
    - Apache Directory Server
    - OpenDS
- En la página de Apache Directory Server, sitio actualizado http://directory.apache.org/apacheds/1.0/apacheds-v10-features.html

han realizado un análisis comparativo de algunas Implementaciones que considera importantes tanto en forma general como técnica. [2]

- OpenLDAP
- ApacheDS
- FedoraDS
- OpenDS

- En el sitio informativo El Pensamiento Blender, su dirección "http://thoughtblender.info/2008/11/04/comparison-of-directory-ldap-servers/", exponen por que utilizar solo dos implementaciones de toda la lista, haciendo un pre análisis de acuerdo a ciertos requerimientos planteados, para luego realizar pruebas automatizadas de las siguientes implementaciones. [6]
  - OpenDS
  - OpenLDAP
- Se realizó una encuesta por medio de la red social G+ operada por google a compañeros estudiantes, docentes y desarrolladores existentes en el sitio, "https://plus.google.com/u/0/111234914617087348938/posts", los resultados arrojados fueron los siguientes:

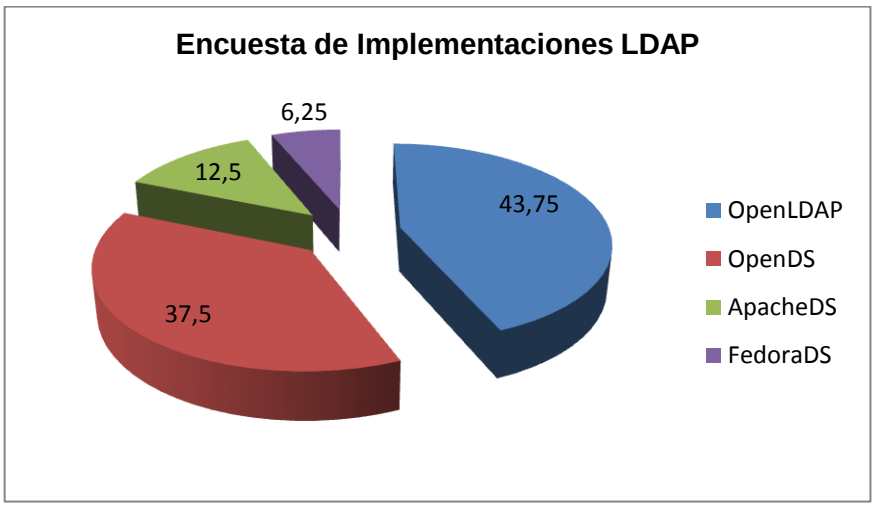


Figura III 1 Resultados de la Encuesta

Prosiguiendo con el análisis comparativo de las Implementaciones del protocolo LDAP, previo al estudio anterior se determinaron OpenLDAP y OpenDS por las siguientes razones.

- Las dos implementaciones tienen mucha aceptación en el medio, de acuerdo a las publicaciones de los sitios web.
- Tienen una excelente documentación en línea y también cuenta con su propia página de información y descarga, debidamente respaldada por cada organización.
- Los resultados de la encuesta realizada por medio de google+ brindo como resultado dos implementaciones, que son las más reconocidas para el medio. (Ver anexo 4)
- Poseen una factibilidad adecuada, ya que cuentan con diferentes herramientas administrativas para su manejo.
- Mediante Decreto Ejecutivo No. 1014 emitido el 10 de Abril de 2008, se dispone el uso de Software Libre en los sistemas y equipamientos informáticos de la Administración Pública de Ecuador. Estas dos implementaciones cumplen con esta disposición.

3.2. Análisis de las Implementaciones seleccionadas

A continuación se analizará cada una de las herramientas definidas anteriormente.

3.2.1. OpenLDAP

OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP.

Está liberada bajo su propia licencia OpenLDAP Public License. LDAP es un protocolo de comunicación independiente de la plataforma.

Muchas distribuciones GNU/Linux incluyen el software OpenLDAP para el soporte LDAP. Este software también corre en plataformas BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows (NT y derivados, incluyendo 2000, XP, Vista), y z/OS. [12]

Los orígenes del protocolo LDAP tal y como lo conocemos hoy en día hay que buscarlos en la década de 1980, cuando la Unión Internacional de Telecomunicaciones (UIT) definió el standard x.500. Dentro de sus especificaciones, además de los conceptos de escalabilidad y estructura jerárquica, se describían los servicios de directorio mediante diversos protocolos:

- Acceso a directorio (DAP).
- Sistema de directorio.
- Ocultación de información de directorio.
- Gestión de enlaces operativos de directorio.

Dichos protocolos se basaban en el modelo OSI de la pila de siete niveles de protocolos. Adicionalmente, en los años 90, un proyecto de la Universidad de Michigan propuso implementar una versión alternativa de DAP más liviana sobre la

familia de protocolos TCP/IP, mucho más simple que el modelo OSI. Esta nueva implementación se llamó LDBP (Lightweight Directory Browsing Protocol) ya que su función se limitaba a las funciones de navegación y búsqueda dentro del directorio. Posteriormente, a medida que se fueron incluyendo operaciones de escritura y gestión de la información, tomó la denominación de LDAP.

Actualmente el protocolo LDAP ha reemplazado por completo a su predecesor, en parte gracias a la gran difusión que tiene la familia de protocolos TCP/IP, dotándole de mayor simplicidad de comprensión e implementación. Ha alcanzado la madurez y reforzado su capacidad de expansión gracias a desarrollos sólidos como OpenLDAP, una alternativa en software libre surgida del proyecto original. [7]

3.2.1.1. Funcionalidad

OpenLDAP incluye un número de características importantes.

- Soporte LDAPv3 — OpenLDAP soporta la Capa de autenticación y seguridad (SASL), la Seguridad de la capa de transporte (TLS) y la Capa de conexión segura (SSL), entre otras mejoras. Muchos de los cambios en el protocolo desde LDAPv2 han sido diseñados para hacer LDAP más seguro.
- Soporte IPv6 — OpenLDAP soporta la próxima generación del protocolo de Internet versión 6.
- LDAP sobre IPC — OpenLDAP se puede comunicar dentro de un sistema usando comunicación interproceso (IPC). Esto mejora la seguridad al eliminar la necesidad de comunicarse a través de la red.
- API de C actualizada — Mejora la forma en que los programadores se conectan para usar servidores de directorio LDAP.

- Soporte LDIFv1 — Provee compatibilidad completa con el formato de intercambio de datos, Data Interchange Format (LDIF) versión 1.
- Servidor Stand-Alone mejorado — Incluye un sistema de control de acceso actualizado, conjunto de hilos, herramientas mejoradas y mucho más. [14]

3.2.2. OpenDS

OpenDS es una implementación de código abierto de servicios de directorio , escrito en Java , y se desarrolló como parte del proyecto OpenDS. Software OpenDS implementa una amplia gama de Lightweight Directory Access Protocol (LDAP) y las normas conexas, incluido el pleno cumplimiento de LDAPv3 sino también el apoyo de servicios de directorio Markup Language (DSMLv2) . También ofrece varias réplicas principales, el control de acceso, y muchas extensiones.

OpenDS software se distribuye bajo desarrollo de Sun Microsystems común y Distribución (CDDL) Licencia. LDAP y DSML son independientes de la plataforma protocolos. El software se desarrolla y funciona en cualquier sistema con soporte Java lenguaje de programación, incluyendo distribuciones de Linux y UNIX, Microsoft Windows, Mac OS X, y otros. La documentación para OpenDS se presenta como un Wiki .

El trabajo de OpenDS comenzó como un proyecto de Sun en interno alrededor de febrero de 2005. OpenDS fue al principio desarrollado principalmente por Neil A. Wilson. Neil fue acompañado por un pequeño equipo de ingenieros del equipo del Servidor del Directorio de SUN. El código estaba abierto-sourced en el junio de 2006.

Sun aumentó el número de reveladores que trabajan en la tecnología de OpenDS después abierto-sourcing el código. Los reveladores que estaban fuera de SUN

también se afiliaron al nuevo proyecto de código abierto. Los miembros de la comunidad como Boni.org, Penrose y JBoss comenzaron a usar OpenDS en sus proyectos. A principios de 2008 el proyecto de OpenDS tenía más de 20 donantes regulares.

El software OpenDS se construye [http://www.opends.org/daily-builds/latest] diariamente. Cada uno construye pasa por pruebas de la unidad automatizadas. Los ingenieros de calidad supervisan el código fuente, con regularidad la recogida construye para dirigir pruebas adicionales, a fin de promover construir. Promovido añade qué tensión adicional y las campañas de prueba del sistema se dirigen se puede hacer jalones. Los jalones que se someten adelante, pruebas más exhaustivas se pueden hacer liberaciones de la versión principales. [8]

3.2.2.1. Funcionalidad

OpenDS incluye las siguientes características:

- Una herramienta gráfica de la instalación de 6 pasos que permite tener un servidor configurado, en servicio en menos de 3 minutos.
- Un panel de estado gráfico.
- Una línea de comando rica herramienta para realizar todas las tareas administrativas en línea ambas recíprocamente o con guión.
- Políticas anticipadas de la seguridad y de la contraseña.
- Capacidades de reserva y del restablecimiento anticipadas.
- Un servlet de la entrada de DSML.
- OpenDS también hace disponible una documentación de usuario completa. [16]

3.3. Determinación de parámetros de comparación

Para la comparación de las Implementaciones del protocolo LDAP, se tiene que considerar algunos aspectos, entre los cuales como parámetros tenemos la instalación y administración, la autenticación, la seguridad y el rendimiento, con sus respectivos índices para determinar la mejor Implementación.

- **Instalación y Administración**
    - Tiempo de Instalación
    - Grado de Complejidad de Configuración
    - Nivel de Control de Acceso
    - Grado de Factibilidad en la Administración
- **Autenticación**
    - Tiempo en establecer Sesión
    - Cantidad de Paquetes de Entrada/Salida
    - Cantidad de Algoritmos de Cifrado
    - Compatibilidad con Métodos de Cifrado
- **Seguridad**
    - Cantidad de Protocolos
    - Cantidad de Sockets
    - Cantidad de Algoritmos Hashing
    - Soporte de Respaldo de Datos
- **Rendimiento**
    - Consumo de Procesos
    - Cantidad de Memoria
    - Nivel de Carga de CPU
    - Utilización de Disco Duro

3.3.1. Indicador 1: Instalación y Administración

El indicador de Instalación y administración proporciona métricas referentes a la instalación y administración, así como los tiempos que aplica cada una de ellas, también factibilidad y el ambiente operativo que proporciona la implementación.

Tabla III I Descriptora del indicador 1 Instalación y Administración

Indicador 1	**Instalación y Administración**	**Descripción**
[índice 1.1]	Tiempo de Instalación	Es el tiempo que tarda en instalar la Implementación.
[índice 1.2]	Grado de Complejidad de Configuración	Describe el grado de complejidad que toma en configurar cada parámetro en definirse en la Implementación.
[índice 1.3]	Nivel de Control de Acceso	Este índice evaluará si la implementación posee un ambiente gráfico.
[índice 1.4]	Grado de Factibilidad en la Administración	Este índice evalúa la facilidad de manipulación que tiene la interfaz administrativa.

3.3.2. Indicador 2: Autenticación

Aquí se describe la Autenticación que posee cada implementación, haciendo énfasis en el tiempo para iniciar una sesión, los paquetes que se envían y la cantidad de algoritmos que ofrece cada implementación analizada.

Tabla III II Descripción Indicador 2 Autenticación

Indicador 2	Autenticación	Descripción
[índice 2.1]	Tiempo en establecer Sesión	Es el tiempo que tarda en autentificarse un usuario.
[índice 2.2]	Cantidad de Paquetes de Entrada/Salida	Describe la cantidad de paquetes que recibe el servidor tanto de entrada como el envío a la salida.
[índice 2.3]	Cantidad de Algoritmos de Cifrado	Este índice evaluará el número de algoritmos de cifrado que posee cada implementación.
[índice 2.4]	Compatibilidad con Métodos de Cifrado	Determina con que métodos de autenticación es compatible o se puede aplicar en cada implementación.

3.3.3. Indicador 3: Seguridad

El indicador de Seguridad nos indica la cantidad de protocolos, la longitud de claves y el soporte con que cuenta cada implementación para respaldar la información.

Tabla III III Descripción del Indicador 3 Seguridad

Indicador 3	Seguridad	Descripción
[índice 3.1]	Cantidad de Protocolos	Permitirá evaluar el número de protocolos que tiene cada Implementación para transmisión de la información.
[índice 3.2]	Cantidad de Sockets	Permitirá visualizar todos los puertos que estén abiertos en el momento que este en ejecución el servidor.
[índice 3.3]	Cantidad de Algoritmos Hashing	Aquí describe cuantos algoritmos hashing ofrece la implementación, y que cual se ejecuta por defecto en el momento de la instalación.
[índice 3.4]	Soporte de Respaldo de Datos	Se evaluará el soporte que tiene cada implementación para respaldar la información.

3.3.4. Indicador 4: Rendimiento

Este indicador describe la funcionalidad con respecto al rendimiento que tienen las implementaciones estudiadas, tomando en cuenta la capacidad, consumo y tiempo de respuesta del servidor.

Tabla III IV Descripción Indicador 5 Rendimiento

Indicador 4	Rendimiento	Descripción
[índice 4.1]	Consumo de Procesos	Evaluará el consumo de recursos por las operaciones que realicen los usuarios.
[índice 4.2]	Cantidad de Memoria	Describe el uso de memoria que ocupa el computador por conexión de usuario.
[índice 4.3]	Nivel de Carga de CPU	Se evalúa el uso del procesador por las conexiones establecidas de usuario.
[índice 4.4]	Utilización de Disco Duro	Este índice tiene como objetivo medir el tamaño utilizado en Disco Duro

3.4. Descripción del Entorno de Pruebas

Para desarrollar el análisis comparativo de las implementaciones del protocolo LDAP, OpenLDAP y OpenDS en los respectivos módulos de prueba se ejecutará bajo el siguiente entorno de hardware y software:

3.4.3. Entorno de Pruebas Hardware

Las siguientes características son tomadas de la distribución realizada a la estación de trabajo de la maquina virtual VMWARE 7.

- **Características del Servidor**
  - Procesador Intel(R) Core(TM)2 Duo CPU E7400 @ 2.800GHz 2.79GHz.
  - Memoria RAM 1 GB
  - Disco Duro 20 GB
  - Tarjeta de red Ethernet 100 Mb/s
- **Características del Cliente**
  - Procesador Intel(R) Core(TM)2 Duo CPU E7400 @ 2.800GHz 2.79GHz.
  - Memoria RAM 512 MB
  - Disco Duro 10 GB
  - Tarjeta de red Ethernet 100 Mb/s

3.4.4. Entorno de Pruebas Software

- Sistema Operativo CentOS 5.6
- Kernel - 2.6.18-238.1.1.el5

3.5. Determinación de los Módulos de Pruebas

Los módulos de prueba son escenarios porque ayudarán a verificar y obtener datos para determinar que Implementación es la mejor en cuanto a la configuración, administración, seguridad y rendimiento.

Los módulos que se desarrollarán serán implementados en el sistema operativo de software libre CentOS 5.6, que es la plataforma en la que se desarrollaron cada una de las implementaciones.

En cada Implementación se probará los mismos escenarios y se obtendrá los resultados mediante comandos o algún software especializado para calcular el rendimiento de hardware y software, así como los tiempos de respuesta.
Para las Implementaciones de LDAP, se tendrá 4 módulos que son:

- Módulo 1: Instalación y Administración de las implementaciones del protocolo LDAP, OpenLDAP y OpenDS.
- Módulo 2: Autenticación al establecer sesión, determinando los algoritmos de cifrado que soportan las implementaciones OpenLDAP y OpenDS.
- Módulo 3: Protocolos utilizados por las herramientas de administración de las implementaciones OpenLDAP y OpenDS.
- Módulo 4: Consumo de recursos de las implementaciones del protocolo LDAP tanto en OpenLDAP como en OpenDS.

A continuación se explicará cada uno de los módulos para su posterior desarrollo e implementación.

3.5.1. Módulo 1: Instalación y Administración de las implementaciones del protocolo LDAP, OpenLDAP y OpenDS.

Este módulo de pruebas desarrollará la instalación de las implementaciones de OpenLDAP y OpenDS, así como la gestión administrativa que ofrece cada una de las mencionadas implementaciones, tomando como base el entorno Hardware y Software definidos anteriormente con la respectiva configuración.

Idioma del Teclado: Inglés US

Configuración Personalizada:

- Aplicaciones Java
- Servidor DNS
- Servidor de Red

Cortafuegos: Deshabilitado

SELinux: Deshabilitado

Bajo este entorno se desarrollará la evaluación del parámetro de Instalación y Administración con sus respectivos indicadores:

- Tiempo de Instalación
- Grado de Complejidad de Configuración
- Nivel de Control de Acceso
- Grado de Factibilidad en la Administración.

Esto se aplicará a cada una de las Implementaciones del Protocolo LDAP, OpenLDAP y OpenDS

3.5.2. Módulo 2: Autenticación al establecer sesión, determinando los algoritmos de cifrado que soportan las implementaciones OpenLDAP y OpenDS.

Este módulo pretende evaluar la autenticación que realiza un cliente para tener acceso al directorio que ha sido definido en el servidor LDAP.

Con el desarrollo de este módulo se analizará el parámetro de Autenticación descrito anteriormente en la determinación de parámetros de comparación y que se basará en los siguientes indicadores.

- Tiempo en establecer Sesión
- Cantidad de Paquetes de Entrada/salida
- Cantidad de Algoritmos de Cifrado
- Compatibilidad con Métodos de Cifrado

3.5.3. Módulo 3: Seguridad utilizada por las herramientas de administración de las implementaciones OpenLDAP y OpenDS.

Este módulo aspira evaluar la seguridad que ofrecen cada una de las implementaciones del protocolo LDAP, OpenLDAP y OpenDS, determinando la cantidad de protocolos y sockets, así como el análisis de la clave que puede soportar cada implementación.

La ejecución del presente modulo de prueba se aplicará a cada uno de los indicadores del parámetro de seguridad, descritos anteriormente como son:

- Cantidad de Protocolos
- Cantidad de Sockets en Ejecución

- Cantidad de Algoritmos Hashing
- Soporte de Respaldo de Datos

3.5.4. Módulo 4: Consumo de recursos de las implementaciones del protocolo LDAP tanto en OpenLDAP como en OpenDS.

Este último módulo de prueba analiza el rendimiento del servidor donde se encuentra configurada la implementación del protocolo LDAP, podría ser OpenLDAP u OpenDS, para esto haremos uso de comandos o herramientas que nos permitan evaluar los indicadores expuestos anteriormente en el parámetro de Rendimiento, como son:

- Tiempo de Respuesta
- Consumo de procesos
- Cantidad de Memoria%
- Nivel de Carga de CPU%

3.6. Desarrollo de los Módulos de Prueba

3.6.1. Módulo 1: Instalación y Administración de las implementaciones del protocolo LDAP en OpenLDAP y OpenDS.

3.6.1.1. Instalación y Administración implementada sobre OpenLDAP

La Instalación de la implementación OpenLDAP y OpenDS se encuentran anexadas (ver anexo 1) al final de este documento, a continuación se desarrollarán los siguientes indicadores con respecto a la Instalación y Administración de la implementación OpenLDAP.

Tiempo de Instalación

El tiempo de Instalación de la implementación OpenLDAP es de 25m10.852s, para obtener este resultado se ejecutó en una terminal independiente de la instalación el comando **time cat**, una vez ejecutado corre el tiempo y en el momento de parar la ejecución del comando este arroja el tiempo en minutos horas segundos y milisegundos. El porcentaje de este tiempo es del 65.96%. (Ver anexo 3)

Grado de Complejidad de Configuración

EL grado de complejidad de configuración de la implementación OpenLDAP, es regular porque se tiene que modificar los archivos de configuración y los esquemas, que son un conjunto de propiedades de los elementos del árbol del directorio LDAP. Se ha tomado como referencia el número de procesos realizados, este valor es igual a 15 con un porcentaje del 71,42%. (Ver anexo 3)

Nivel de Control de Acceso

El indicador de Nivel de Control de Acceso no aplica para la implementación de OpenLDAP, debido que para gestionar las cuentas de usuario se requiere la instalación de una herramienta adicional. (Ver anexo 3)

Grado de Factibilidad en la Administración

La Factibilidad en la Administración es medianamente fácil, debido a que no cuenta con una interfaz de administración gráfica, pero se puede llevar a cabo la administración mediante línea de comandos ejecutados en una terminal.

3.6.1.2. Modulo 1 Instalación y Administración Implementada sobre OpenDS

La instalación de la implementación del protocolo LDAP, OpenDS se encuentra anexada al final de este documento, a continuación se desarrollaran los siguientes indicadores pertenecientes al parámetro de Instalación y Administración.

Tiempo de Instalación

El tiempo de Instalación de la implementación OpenDS es de 12m59.557s, al igual que en la implementación anterior para obtener este resultado se ejecutó en una terminal independiente de la instalación el comando **time cat**, una vez ejecutado corre el tiempo y en el momento de parar la ejecución del comando este arroja el tiempo en minutos horas segundos y milisegundos. Este tiempo ha sido transformado a segundos para obtener un porcentaje del 34.04% (Ver Anexo 3)

Grado de Complejidad de Configuración

Para el grado de complejidad de configuración de la implementación OpenDS, esta se presenta fácil, ya que sumado los pasos de configuración dan un valor de 6, debido que al momento de instalar la implementación la mayoría de estos se realizan automáticamente y si requiere personalizar el esquema, propiedades o atributos se lo puede hacer por medio de la interfaz gráfica. Representado en un valor porcentual es el 28.57% (Ver Anexo 3)

Nivel de Control de Acceso

La Implementación de OpenDS cuenta con un nivel de control de Acceso, debido que al momento de la instalación se ejecuta una interfaz de administración propia. (Ver Anexo 3)

Grado de Factibilidad en la Administración

En la Factibilidad en la Administración de esta implementación se puede decir que es fácil de usar, debido a que cuenta con una interfaz de administración gráfica amigable e intuitiva para él usuario. (Ver Anexo 3)

3.6.2. Módulo 2: Autenticación al establecer sesión, determinando los algoritmos de cifrado que soportan las implementaciones OpenLDAP y OpenDS.

3.6.2.1. Módulo 2 Implementado sobre OpenLDAP.

Tiempo en establecer Sesión

El tiempo en establecer sesión hacia el servidor OpenLDAP, será obtenido con la herramienta de análisis de tráfico y protocolos Wireshark. Este tiempo se define como la latencia, y es la suma de los tiempos: Retardo del Nodo, Transmisión de Datos (Velocidad de Transmisión de la tarjeta en Mbps), y Tiempo de Propagación. El tiempo en establecer sesión es de 0.009401488 segundos o 9.401488 milisegundos. (Ver Anexo 3)

Cantidad de Paquetes de Entrada/Salida

El análisis de la cantidad de paquetes transmitidos por el cliente al servidor implementado con OpenLDAP es capturado por la herramienta de análisis de protocolos Wireshark, la cual al ser ejecutada visualiza los diferentes protocolos de comunicación que existen en mi red. Nos ubicamos en el protocolo LDAP bindresponse, que es la respuesta que emite mi servidor a la petición de autenticación

del cliente. Dentro de este protocolo, observamos las características de la capa 1, donde muestra la longitud de la trama, en este caso es de 80 bytes. Expresado en porcentaje da un valor del 50%. (Ver Anexo 3)

Cantidad de Algoritmos de Cifrado

La cantidad de Algoritmos de cifrado que presta el servidor configurado con la implementación OpenLDAP, con respecto a la encriptación de la contraseña son los siguientes: (Ver Anexo 3)

1. Kerberos
2. LDAP - TLS
3. Tarjeta Inteligente
4. SMB
5. Winbind

Para establecer un valor más legible se sumó la cantidad de algoritmos de cifrado de las dos implementaciones y se obtuvo un porcentaje del 16.66%. (Ver Anexo 3)

Compatibilidad con Métodos de Cifrado

La compatibilidad con los métodos de cifrado que presta la implementación en OpenLDAP son dos, NSS y PAM lo cual permite que los datos se envíen de forma segura luego de una adecuada configuración. (Ver Anexo 3)

3.6.2.2. Módulo 2 implementado sobre OpenDS

Tiempo en establecer Sesión

El tiempo en establecer sesión hacia el servidor OpenDS, será obtenido con la herramienta de análisis de tráfico y protocolos Wireshark. Este tiempo se define como la latencia, y es la suma de los tiempos, Retardo del Nodo, Transmisión de Datos (Velocidad de Transmisión de la tarjeta en Mbps), y Tiempo de Propagación. El tiempo en establecer sesión es de 0.001029444 segundos o 1.029444 milisegundos. (Ver Anexo 3)

Cantidad de paquetes de Entrada/Salida

El análisis de la cantidad de paquetes transmitidos por el cliente al servidor implementado con OpenDS es capturado por la herramienta de análisis de protocolos Wireshark, la cual al ser ejecutada visualiza los diferentes protocolos de comunicación que existen en mi red. Nos ubicamos en el protocolo LDAP bindresponse, que es la respuesta que emite mi servidor a la petición de autenticación del cliente. Dentro de este protocolo, observamos las características de la capa 1, donde muestra la longitud de la trama, en este caso es de 80 bytes. Expresado en porcentaje da un valor del 50%. (Ver Anexo 3)

Cantidad de Algoritmos de Cifrado

La cantidad de Algoritmos de cifrado que presta el servidor configurado con la implementación OpenDS, respecto a la encriptación del nombre de usuario y la contraseña son los siguientes:

1. ds-cfg-start-tls-extended-operation-handler

Este valor es encontrado en el panel del control como clase de objeto estructural.

La cantidad a sido transformada porcentualmente en 83.33%. (Ver Anexo 3)

Compatibilidad con Métodos de Cifrado

No aplica compatibilidad con otros métodos de cifrado, ya que viene estructurada en un solo conjunto con su interfaz gráfica y esquemas definidos dentro de ella.

3.6.3. Módulo 3: Seguridad utilizada por las herramientas de administración de las implementaciones OpenLDAP y OpenDS.

3.6.3.1. Implementado sobre OpenLDAP

Cantidad de Protocolos

La cantidad de protocolos que usa el servidor en la implementación de OpenLDAP son 7, los mismos que se obtienen ejecutando el comando **netstat –s** en una terminal.

1. Ip
2. Icmp
3. IcmpMsg
4. Udp
5. Tcp
6. TcpExt
7. IpExt

La cantidad de protocolos tiene un valor en porcentaje del 50%. (Ver Anexo 3)

Cantidad de Sockets

En la implementación OpenLDAP, una vez conectados los clientes, desde nuestro servidor en una terminal ejecutamos el comando **lsof –i | wc -l**, que lista la información de los archivos abiertos por los procesos, y con el atributo **–i**, indica los puertos que se están ejecutando en ese momento. Como resultado este comando con ayuda de un **| pipeline** y el atributo **wc -l** lista **65** conexiones abiertas.

El valor obtenido de la cantidad de sockets da un porcentaje del 51.18%. (Ver Anexo3)

Cantidad de Algoritmos Hashing

La cantidad de algoritmos de hashing de la contraseña que tiene la implementación de OpenLDAP, son las siguientes:

1. DESCRYPT
2. BIGCRYPT
3. MD5
4. SHA256
5. SHA512

Por defecto OpenLDAP tiene configurado el hashing de contraseñas MD5, pero si deseamos cambiar por otro, esto lo podemos hacer ejecutando en una terminal el comando authconfig-gtk o en el menú principal elegimos Sistema – Administración – Autenticación – Opciones. La cantidad de algoritmos hashing porcentualmente tiene un valor del 50%. (Ver Anexo 3)

Soporte de Respaldo de Datos

OpenLDAP si tiene un buen soporte de respaldo de datos, el archivo que genera está en formato LDIF, que quiere decir “formato de intercambio de datos ldap”, utilizando el comando **slapcat**. Este respaldo se lo puede hacer solo en frío, esto quiere decir que es necesario detener el servicio de LDAP para proseguir con el respaldo de datos.
Todo este proceso se lo realiza en base a comandos, como está indicado anteriormente o puede apoyarse en el soporte de alguna interfaz administrativa.
(Ver Anexo 3)

3.6.3.2. Implementado sobre OpenDS

Cantidad de Protocolos

La cantidad de protocolos que usa el servidor en la implementación de OpenLDAP son 7, los mismos que se obtienen ejecutando el comando **netstat –s** en una terminal.

1. Ip
2. Icmp
3. IcmpMsg
4. Udp
5. Tcp
6. TcpExt
7. IpExt

La cantidad de protocolos tiene un valor en porcentaje del 50%. (Ver Anexo 3)

Cantidad de Sockets en Ejecución

En la implementación OpenDS, una vez conectados los clientes, desde nuestro servidor en una terminal ejecutamos el comando **lsof –i | wc -l**, que lista la información de los archivos abiertos por los procesos, y con el atributo **–i**, indica los puertos que se están ejecutando en ese momento. Como resultado este comando con ayuda de un **| pipeline** y el atributo **wc -l** lista **62** conexiones abiertas.

El cálculo del porcentaje de este valor dio como resultado el 48.41%. (Ver Anexo 3)

Cantidad de Algoritmos Hashing de la Contraseña

La interfaz gráfica que tiene OpenDS permite incluir clases de objeto a nuestros registros el cual tiene 5 algoritmos hashing que yo puedo utilizar para proteger mis contraseñas y que no se muestren en texto plano.

1. MD5
2. SHA1
3. SHA256
4. SHA384
5. SHA512

Expresando en porcentaje da como resultado el 50%. (Ver Anexo 3)

Soporte de Respaldo de datos

La implementación de OpenDS tiene la posibilidad de respaldar los datos desde la interfaz administrativa, ejecutando desde el menú **Datos del Directorio** – **Realizar copia de seguridad** y si se desea se pueden cifrar los datos, y se lo puede hacer en caliente sin necesidad de detener el servidor. (Ver Anexo 3)

3.6.4. Módulo 4: Consumo de recursos de las implementaciones del protocolo LDAP tanto en OpenLDAP como en OpenDS.

3.6.4.1. Implementado sobre OpenLDAP

Consumo de Procesos

El consumo de procesos que tiene el servidor OpenLDAP, es analizado con el comando **ps aux | wc -l**, el cual va a ser ejecutado dentro de una terminal. Este a la vez nos arrojará un valor numérico de **151** procesos.

Obtenido el valor en porcentaje da como resultado el 49.47% (Ver Anexo 3)

Cantidad de Memoria

Este indicador referente a la cantidad de memoria es analizado desde una terminal de comandos en el servidor OpenLDAP, ejecutando el comando **free**, el cual nos muestra la cantidad de memoria total asignada, el usado y el disponible, todo esto expresado en kilobytes, los valores son los siguientes:

Total: 1034708

Used: 606928

Free: 427780

El porcentaje del la cantidad de memoria utilizada es del **58.65%.** (Ver anexo 3)

Nivel de Carga de CPU

El nivel de carga que tiene el CPU se lo puede mostrar de manera porcentual, utilizando el comando **top** siempre y cuando se lo ejecute desde una terminal de

comandos, en la tercera línea se encuentra los porcentajes utilizados de CPU(s), el valor mostrado dependerá de los procesos que se ejecuten en ese momento, de ahí solo con la conexión de usuarios su porcentaje oscila del 14%sy, (las siglas sy provienen de system y quiere decir el nivel de carga utilizado por el sistema).
(Ver anexo 3)

Utilización de Disco Duro

La utilización de disco duro en la implementación de OpenLDAP, lo podemos analizar ejecutando desde una terminal el comando ejecutando **df –h,** lo cual mostrará como resultado el 32% del uso del disco. (Ver anexo 3)

3.6.4.2. Implementado sobre OpenDS

Consumo de Procesos

El consumo de procesos que tiene el servidor OpenDS, es analizado con el comando **ps aux | wc -l**, el cual va a ser ejecutado dentro de una terminal. Este a la vez nos arrojará un valor numérico de **143** procesos.
El consumo de procesos en porcentaje da un valor del 50.53%. (Ver anexo 3)

Cantidad de Memoria

Este indicador referente a la cantidad de memoria es analizado desde una terminal de comandos en el servidor OpenDS, ejecutando el comando **free**, el cual nos muestra la cantidad de memoria total asignada, el usado y el disponible, todo esto expresado en kilobytes, los valores son los siguientes:

Total: 1628040

Used: 1112636

Free: 347560

El porcentaje obtenido de la cantidad de memoria es igual al 68.34%. (Ver Anexo 3)

Nivel de Carga de CPU

El nivel de carga que tiene el CPU se lo puede mostrar de manera porcentual, utilizando el comando **top** siempre y cuando se lo ejecute desde una terminal de comandos, en la tercera línea se encuentra los porcentajes utilizados de CPU(s), el valor mostrado dependerá de los procesos que se ejecuten en ese momento, de ahí solo con la conexión de usuarios su porcentaje oscila del 17%sy, (las siglas sy provienen de system y quiere decir el nivel de carga utilizado por el sistema).
(Ver Anexo 3)

Utilización de Disco Duro

La utilización de disco duro en la implementación de OpenDS, se puede analizar ejecutando desde una terminal el comando el mandato **df –h,** lo cual mostrará como resultado directo el 41% del uso del disco. (Ver Anexo 3)

3.7. Criterios de Evaluación

Para evaluar los indicadores anteriormente definidos en cada uno de los módulos correspondientes se empleará la siguiente matriz de valorización con los valores cuantitativos y cualitativos.

3.7.1. Matriz de Valorización

Tabla III V Valorización Módulos

Valor Cuantitativo	**0**	**1**	**2**	**3**	**4**	**5**
Valor Cualitativo	**N/A**	**Malo**	**Regular**	**Bueno**	**Muy Bueno**	**Excelente**
		Muy Difícil	Difícil	Medianamente Fácil	Fácil	Muy Fácil
	NO					SI
		Desisegundo	Centisegundo	Milisegundo	Microsegundo	Nanosegundo
Porcentaje (%)		100 - 81	80 - 61	60 - 41	40 - 21	20 - 1

3.7.2. N/A

El valor cualitativo N/A se asignará cuando el requerimiento del indicador no aplica para alguna de las implementaciones analizadas. El equivalente al valor cuantitativo será igual a 0.

3.7.3. Malo

Esta calificación cualitativa se asignará cuando la implementación cumpla de forma pésima las características del indicador, o no efectúe el requisito del mismo. También está definido como el valor cualitativo de Muy Difícil y un porcentaje del 100% al 81%. El equivalente en el valor cuantitativo será igual a 1.

3.7.4. Regular

Este valor cualitativo se asignará a las implementaciones que cumplan de forma deficiente con el objetivo del indicador correspondiente. Seguido está definido con el valor cualitativo de Difícil y un rango del 61% al 80% de su porcentaje. El equivalente en el valor cuantitativo será igual a 2.

3.7.5. Bueno

La calificación cualitativa se le asignará a las implementaciones que cumplan parcialmente con el objetivo del indicador. Este valor puede estar definido con el valor cualitativo de Medianamente Fácil o con un porcentaje medio del 41% al 60% El equivalente en el valor cuantitativo será igual a 3.

3.7.6. Muy Bueno

El valor cualitativo Muy bueno se asignará a las implementaciones que cumpla con la mayor parte de los requerimientos del indicador. Como también puede tener el valor cualitativo de Fácil o un grado porcentual del 21% al 40% por ciento. El equivalente en el valor cuantitativo será igual a 4.

3.7.7. Excelente

Esta calificación se asignará a las implementaciones que cumplan a cabalidad con el objetivo del indicador. Se puede representar con el valor cualitativo de Muy Fácil o un porcentaje del 1% al 20% de acuerdo a lo que requiera el indicador. El equivalente en el valor cuantitativo será igual a 5.

3.8. Evaluación de Indicadores de los Módulos del Análisis Comparativo de las Implementaciones del Protocolo LDAP, OpenLDAP y OpenDS.

3.8.1. Evaluación de los Indicadores del Módulo 1: Instalación y Administración de las implementaciones del protocolo LDAP, OpenLDAP y OpenDS.

En la siguiente tabla se muestra la calificación de se asignó a los indicadores del parámetro 1 de las implementaciones del protocolo LDAP.

Tabla III VI Análisis Comparativo del Módulo 1

INDICADORES	**IMPLEMENTACIONES**	
	OpenLDAP	**OpenDS**
Tiempo de Instalación	Regular	Muy Bueno
Grado de Complejidad de Configuración	Regular	Muy Bueno
Nivel de Control de Acceso	N/A	Excelente
Grado de Factibilidad en la Administración	Bueno	Muy Bueno

Se pudo observar en lo referente al indicador del Tiempo de Instalación, que entre las dos implementaciones, la diferencia de tiempo es mínima, por la complejidad que cada una tiene en su configuración. Por esta razón se categorizó en porcentajes.

El indicador de Grado de Complejidad de Configuración, muestra una diferencia significativa entre OpenLDAP y OpenDS, ya que la primera denota mayor dificultad en la configuración.

El indicador que define el Nivel de Control Acceso se ve representado solo en OpenDS con el valor cualitativo más alto ya que esta cuenta con una interfaz grafica para la administración.

El indicador del Grado de Factibilidad en la Administración, expresado cualitativamente para OpenLDAP es Medianamente Fácil ya que su configuración es en base a línea de comandos mientras que en OpenDS se torna Fácil debido a que posee una interfaz gráfica.

En la siguiente tabla se asigna los valores cuantitativos, de acuerdo a la calificación definida en los indicadores de cada una de las implementaciones del protocolo LDAP:

Tabla III VII Valores Cuantitativos del Módulo 1

INDICADORES	**IMPLEMENTACIONES**	
	OpenLDAP	**OpenDS**
Tiempo de Instalación	2	4
Grado de Complejidad de Configuración	2	4
Nivel de Control de Acceso	0	5
Grado de Factibilidad en la Administración	3	4
Total	7	17

Análisis Comparativo del Módulo 1: Instalación y Administración de las implementaciones del protocolo LDAP en OpenLDAP y OpenDS. Se puede observar claramente que OpenDS es superior a gran escala frente a OpenLDAP de acuerdo al total de sus valores cuantitativos.

A continuación se ven reflejados los datos obtenidos en un gráfico estadístico.

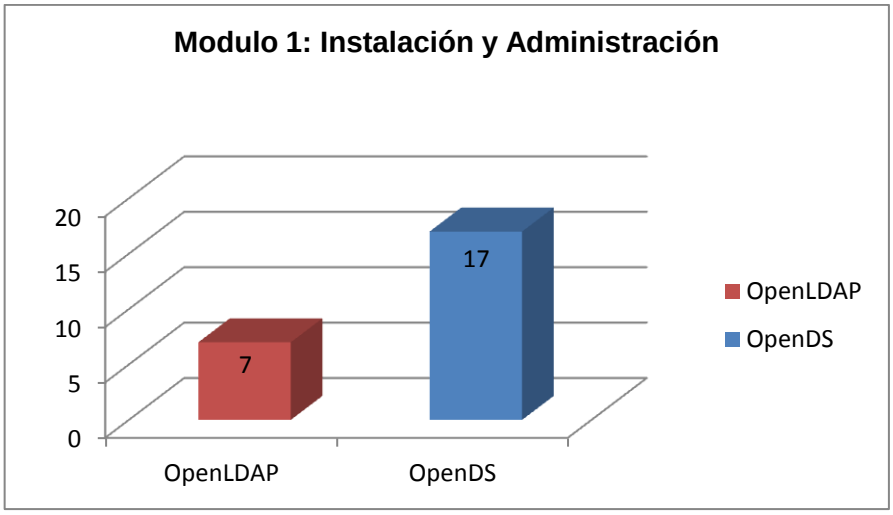


Figura III 2 Gráfico Estadístico del Análisis Comparativo del Módulo 1

3.8.2. Evaluación de los Indicadores del Módulo 2: Autenticación al establecer sesión, determinando los algoritmos de cifrado que soportan las implementaciones OpenLDAP y OpenDS.

En la siguiente tabla se expresa el análisis comparativo del módulo 2 de forma cualitativa aplicada a las implementaciones del protocolo LDAP.

Tabla III VIII Valores Cualitativos del Módulo 2

INDICADORES	IMPLEMENTACIONES	
	OpenLDAP	**OpenDS**
Tiempo en establecer Sesión	Bueno	Bueno
Cantidad de Paquetes de Entrada/Salida	Bueno	Bueno
Cantidad de Algoritmos de Cifrado	Excelente	Malo
Cantidad de Métodos de Cifrado Compatibles	Excelente	N/A

El indicador del Tiempo en establecer Sesión da como resultado valores en milisegundos aproximadamente, esto quiere decir que las dos implementaciones poseen un inicio de sesión instantáneo, por eso se categorizó un rango de tiempos para poder expresar que tan rápida es su autenticación.

El análisis comparativo del módulo 2 aplicado al indicador de Cantidad de Paquetes de Entrada/Salida da como resultado una igualdad, y se ha valorizado cualitativamente como bueno ya que el paquete transmitido es liviano.

Los métodos de cifrado obtenidos de OpenLDAP son expuestos por el entorno de escritorio GNOME de CentOS5.6. En OpenDS se obtuvo del Panel de Control, por esta razón se le ha dado un porcentaje del 50% a cada una y un valor cualitativo de Buena.

Analizando el último indicador del módulo 2 su valor es parcial ya que solo en una de las implementaciones son aplicables los métodos de autenticación.

En la siguiente tabla se expresa el análisis comparativo del módulo 2 de forma cuantitativa aplicado a las implementaciones del protocolo LDAP.

Tabla III IX Valores Cuantitativos del Módulo 2

INDICADORES	IMPLEMENTACIONES	
	OpenLDAP	**OpenDS**
Tiempo en establecer Sesión	3	3
Cantidad de Paquetes de Entrada/Salida	3	3
Cantidad de Algoritmos de Cifrado	5	1
Compatibilidad con Métodos de Cifrado	5	0
Total	16	7

Análisis Comparativo del Módulo 2: Autenticación al establecer sesión, determinando los algoritmos de cifrado que soportan las implementaciones OpenLDAP y OpenDS. Se puede observar claramente que OpenLDAP es más fuerte en la autenticación que OpenDS de acuerdo al total de sus valores cuantitativos expresados en la tabla anterior.

Por consiguiente se muestran los valores en un gráfico estadístico.

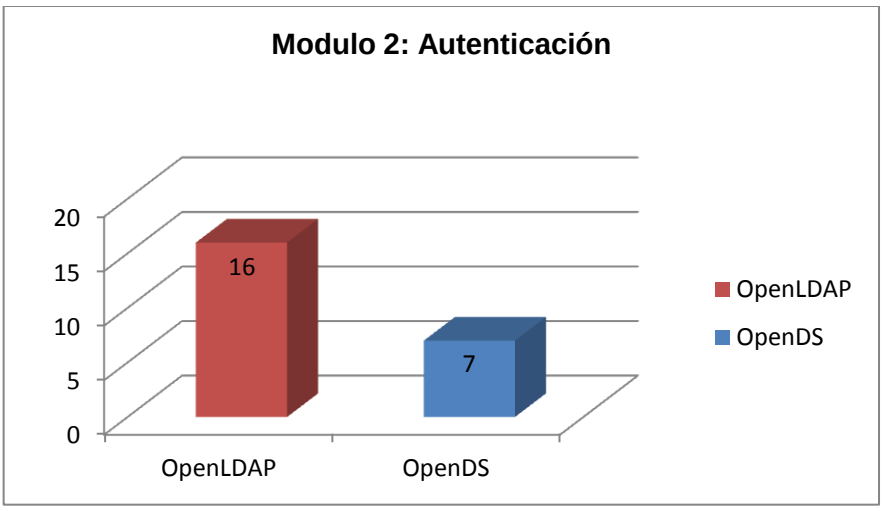


Figura III 3 Grafico Estadístico del Análisis Comparativo del Módulo 2

3.8.3. Evaluación de los Indicadores del Módulo 3: Seguridad utilizada por las herramientas de administración de las implementaciones OpenLDAP y OpenDS.

En la siguiente tabla se expresa el análisis comparativo del módulo 3 de forma cualitativa aplicada a las implementaciones del protocolo LDAP.

Tabla III X Valores Cualitativos del Módulo 3

INDICADORES	**IMPLEMENTACIONES**	
	OpenLDAP	**OpenDS**
Cantidad de Protocolos	Bueno	Bueno
Cantidad de Sockets	Bueno	Bueno
Cantidad de Algoritmos Hashing	Bueno	Bueno
Soporte de Respaldo de Datos	Excelente	Excelente

En el indicador de Cantidad de protocolos del análisis comparativo del módulo 3, las dos implementaciones del protocolo LDAP muestran una similitud en su valor cualitativo, y se ha definido como bueno por que utiliza los protocolos necesarios dentro de la configuración de un servidor LDAP.

En el análisis comparativo del indicador de la Cantidad de Sockets, la variación es mínima, dentro del mismo rango por eso se ha definido a las dos implementaciones con un valor cualitativo bueno por la comunicación que tienen con el cliente.

La Cantidad de Algoritmos Hashing descrito en el indicador 3 muestra una similitud entre las implementaciones ya que tiene el mismo número de algoritmos definida en cada implementación.

En el análisis comparativo del Soporte de Respaldo de Datos, se obtuvo el valor cualitativo de Excelente en las dos implementaciones, porque si han cumplido a cabalidad con el índice establecido.

En la siguiente tabla se expresa el análisis comparativo del módulo 3 de forma cuantitativa aplicada a las implementaciones del protocolo LDAP.

Tabla III XI Valores Cuantitativos del Módulo 3

INDICADORES	**IMPLEMENTACIONES**	
	OpenLDAP	**OpenDS**
Cantidad de Protocolos	3	3
Cantidad de Sockets	3	3
Cantidad de Algoritmos Hashing	3	3
Soporte de Respaldo de Datos	5	5
Toltal	14	14

Análisis Comparativo del Módulo 3: Seguridad utilizada por las herramientas de administración de las implementaciones OpenLDAP y OpenDS. Se puede observar claramente que la seguridad no difiere entre OpenLDAP y OpenDS de acuerdo al total de sus valores cuantitativos.

A continuación se expresa los valores en un gráfico estadístico.

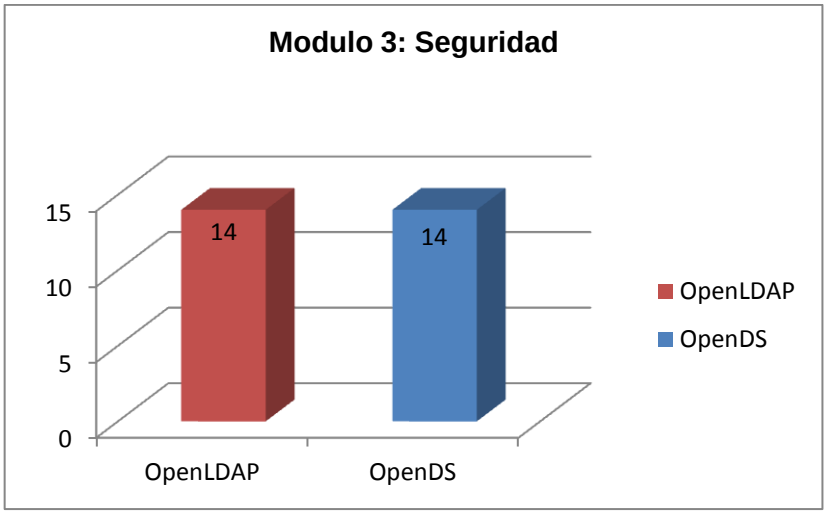


Figura III 4 Gráfico Estadístico del Análisis Comparativo del Módulo 3

3.8.4. Evaluación de los Indicadores del Módulo 4: Consumo de recursos de las implementaciones del protocolo LDAP tanto en OpenLDAP como en OpenDS.

En la siguiente tabla se expresa el análisis comparativo del módulo 4 de forma cualitativa aplicada a las implementaciones del protocolo LDAP.

Tabla III XII Valores Cualitativos del Módulo 4

INDICADORES	IMPLEMENTACIONES	
	OpenLDAP	**OpenDS**
Consumo de Procesos	Bueno	Bueno
Cantidad de Memoria	Bueno	Regular
Nivel de Carga del CPU	Excelente	Excelente
Utilización de Disco Duro	Muy Bueno	Bueno

En el indicador de Consumo de Procesos en el análisis comparativo del módulo 4, se ha ubicado un valor cualitativo bueno a las dos implementaciones a pesar de que hay una variación y es mejor OpenLDAP por tener menos procesos ejecutándose, en su valor porcentual pertenece al mismo rango.

En el análisis comparativo del indicador de Cantidad de Memoria del módulo 4, se puedo notar la diferencia en los porcentajes que arrojó cada implementación, por ende se ha valorizado cualitativamente entre bueno a OpenLDAP y regular a OpenDS que es la implementación que más alto porcentaje de memoria a consumido.

En el indicador de Nivel de Carga de CPU en el análisis comparativo del módulo 4 dio una igualdad de valores ya que el porcentaje de consumo de CPU de cada servidor se ubicó en el mismo rango, se ha representado el valor cualitativo de excelente, a pesar que OpenLDAP consume menos nivel de carga que OpenDS.

El análisis del último indicador del módulo 4, que es la Utilización de Disco Duro, también tiene una diferencia poco significativa, valorizada entre muy bueno y bueno dependiendo del consumo de tamaño en disco duro, en este caso OpenDS ocupó mayor capacidad en disco.

En la siguiente tabla se expresa el análisis comparativo del módulo 4 de forma cuantitativa aplicada a las implementaciones del protocolo LDAP.

Tabla III XIII Valores Cuantitativos del Módulo 4

INDICADORES	IMPLEMENTACIONES	
	OpenLDAP	OpenDS
Consumo de Procesos	3	3
Cantidad de Memoria	3	2
Nivel de Carga del CPU	5	5
Utilización de Disco Duro	4	3
Total	15	13

Análisis Comparativo del Módulo 4: Consumo de recursos de las implementaciones del protocolo LDAP tanto en OpenLDAP como en OpenDS. Se puede observar que rotundamente el rendimiento es mejor en OpenLDAP que OpenDS de acuerdo al total de sus valores cuantitativos.

A continuación se expresa los valores en un gráfico estadístico.

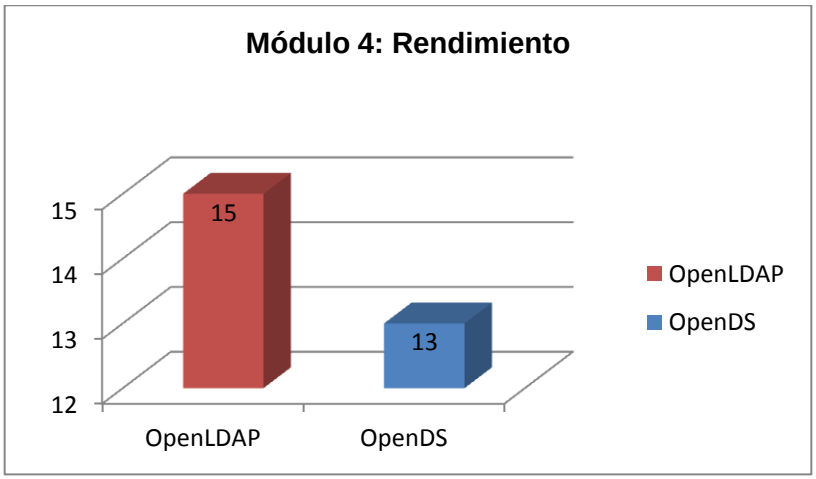


Figura III 5 Grafico Estadístico del Análisis Comparativo del Módulo 4

3.9. Matriz de Valorización: Análisis Comparativo de los indicadores de los Módulos de Prueba de las Implementaciones del Protocolo LDAP, OpenLDAP y OpenDS.

Luego del experimento en el comportamiento de cada una de las implementaciones del protocolo LDAP, OpenLDAP y OpenDS en los módulos de prueba desarrollado anteriormente, se pudo cualificar y cuantificar cada indicador que conforman los 4 parámetros definidos en el análisis comparativo. A continuación se presenta la matriz de valorización con todos los indicadores.

Tabla III XIV Matriz de Valorización de las Implementaciones de OpenLDAP y OpenDS

INDICADORES	**INDICES**	**IMPLEMENTACIONES**	
		OpenLDAP	OpenDS
Instalación y Administración	Tiempo de Instalación	2	4
	Grado de Complejidad de Configuración	2	4
	Nivel de Control de Acceso	0	5
	Grado de Factibilidad en la Administración	3	4
Autenticación	Tiempo en establecer Sesión	3	3
	Cantidad de Paquetes de Entrada/Salida	3	3
	Cantidad de Algoritmos de Cifrado	5	1
	Compatibilidad con Métodos de Cifrado	5	0
Seguridad	Cantidad de Protocolos	3	3
	Cantidad de Sockets	3	3
	Cantidad de Algoritmos Hashing	3	3
	Soporte de Respaldo de Datos	5	5
Rendimiento	Consumo de Procesos	3	3
	Cantidad de Memoria	3	2
	Nivel de Carga de CPU	5	5
	Utilización de Disco Duro	4	3
Total		**52**	**51**

Haciendo uso de la estadística analítica representaremos gráficamente el total de los valores cuantitativos de los indicadores del análisis comparativo de las Implementaciones del protocolo LDAP, OpenLDAP y OpenDS.

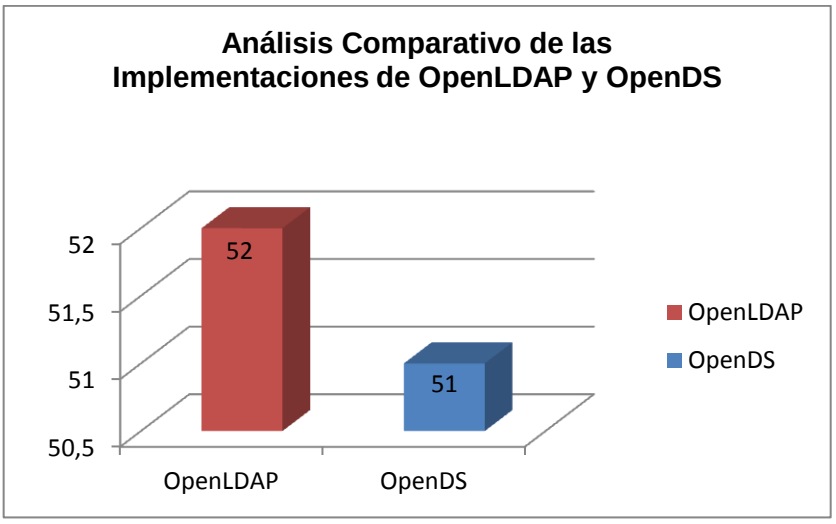


Figura III 6 Gráfico Estadístico del Análisis Comparativo de OpenLDAP y OpenDS

3.10. Comprobación de Hipótesis y Resultados

3.10.1. Hipótesis

El análisis de las implementaciones del protocolo LDAP permitirá escoger la más adecuada para el desarrollo de un sistema de autenticación en los laboratorios de la Escuela de Ingeniería en Sistemas.

3.10.2. Análisis Comparativo en porcentajes de las Implementaciones del Protocolo LDAP, OpenLDAP y OpenDS.

Gráfico de resultados del Análisis Comparativo de las Implementaciones del Protocolo LDAP, OpenLDAP y OpenDS expresado en porcentajes.

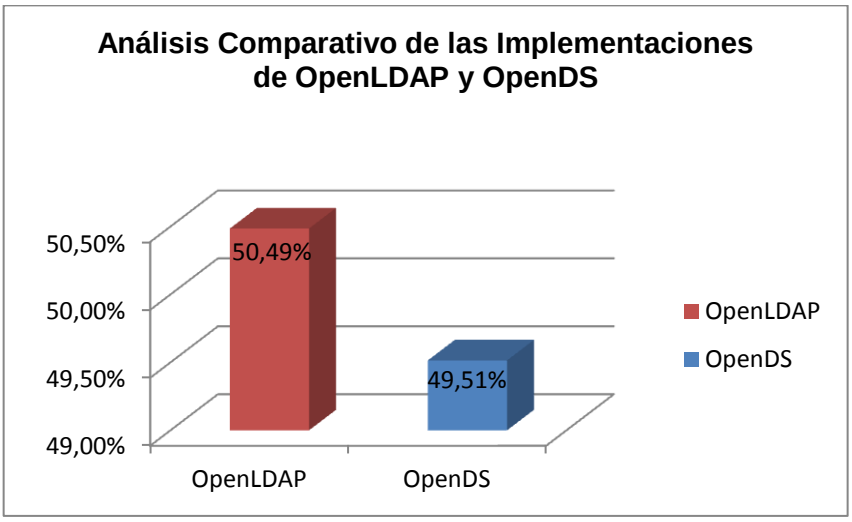


Figura III 7 Gráfico Estadístico del Análisis Comparativo en Porcentajes de OpenLDAP y OpenDS

3.10.3. Resultados Obtenidos

- En los resultados obtenidos, se puede observar que la implementación de OpenLDAP obtiene el resultado más alto con un porcentaje del 50.49%, debido a características de factibilidad, usabilidad, eficiencia y rendimiento. La siguiente implementación OpenDS, tiene un porcentaje del 49.51%.
- Después del análisis comparativo del parámetro de Instalación y Administración se puedo verificar que la herramienta con mejores características es OpenDS, debido a su corto tiempo de instalación y por presentar una herramienta administrativa. Por el contrario OpenLDAP se complica un poco en este parámetro porque no tiene una interfaz administrativa y su gestión se la realiza en base a código en una terminal de comandos, y también el tiempo de instalación de la implementación no es el adecuado.
- En la Autenticación las dos implementaciones son muy proporcionales en los valores cuantitativos ya que el tiempo en iniciar sesión del cliente es bastante

aceptable, y el número de algoritmos de cifrado es el mismo. Aquí se observó una variación total en los métodos de autenticación ya que se puede aplicar en OpenLDAP y no en OpenDS.

- La Seguridad que ofrecen las dos implementaciones, OpenLDAP y OpenDS es muy buena ya que maneja la misma cantidad de protocolos en cambio los números de sockets para la comunicación varían, ya que OpenLDAP tiene mayor cantidad. En el soporte para el respaldo de datos en OpenDS es mejor por tiene la facilidad de hacer los respaldos sin necesidad de detener el servicio LDAP.
- En lo que se refiere al rendimiento de los servidores, se puede deducir que OpenLDAP consume menos servicios de memoria, CPU y almacenamiento de Disco en relación a OpenDS, esto se debe en gran parte a que OpenLDAP no cuenta con una interfaz administrativa por defecto en el momento de su instalación.

3.10.4. Conclusión de la Comprobación de la Hipótesis

Después de realizar el análisis comparativo de las implementaciones del protocolo LDAP: OpenLDAP y OpenDS, por observación directa se concluye que la herramienta más idónea y con mejores características de acuerdo a los resultados obtenidos por los indicadores planteados es OpenLDAP con un 50.49%, debido a que ofrece una buena autenticación y los datos del usuario pueden estar más seguros, así como ofrece un mejor rendimiento en sus servicios.

4. CAPITULO IV

IMPLANTACION DE UN SISTEMA DE AUTENTICACION OPENLDAP

Para la implementación de un sistema de autenticación aplicado en la Escuela Superior Politécnica de Chimborazo, a los laboratorios de la Escuela de Ingeniería en Sistemas, se ha configurado una máquina de escritorio como un servidor de servicio de directorio, utilizando la implementación OpenLDAP.

4.1. Características Generales

4.1.1. Características Hardware

- Fabricante del Sistema: INTEL.
- Modelo del Sistema: ECG3510M.
- Tipo de Sistemas: Equipo basado en X86.
- Procesador: Intel(R) Core(TM)2 Duo CPU E7400 @ 2.80GHz 2793 Mhz, 2 procesadores.
- Versión y fecha de BIOS: Intel Corp. ECG3510M.0106.2008.0730.1746, 30/07/2008.

- Memoria física instalada (RAM): 4,00 GB
- Memoria física total: 3,24 GB
- Capacidad en Disco Duro: 150 GB

4.1.2. Características Software

- Sistema Operativo CentOS5.6
- Kernel - 2.6.18-238.1.1.el5

4.2. Configuración de OpenLDAP como un Servidor de Autenticación

La Instalación del sistema operativo de software libre CentOS5.6 puede encontrarla, al final de este documento (Anexos 1). A continuación se procede con los pasos de instalación y preparación del Servidor de Autenticación OpenLDAP.

Para realizar la configuración de OpenLDAP se debe ingresar al sistema como súper usuario (root).

4.2.1. Aplicaciones necesarias para el equipamiento lógico

- openldap
- openldap-servers
- openldap-clients
- authconfig
- authconfig-gtk (Opcional)
- bind
- bind-chroot
- bind-utils
- caching-nameserver

- samba
- samba-client
- samba-common

4.3. Procedimiento de Configuración de OpenLDAP

4.3.1. Instalación a través del comando yum

La instalación se realizó a través del comando yum, lo único que se necesita es tener salida a internet para realizar la instalación de todos los paquetes de OpenLDAP.

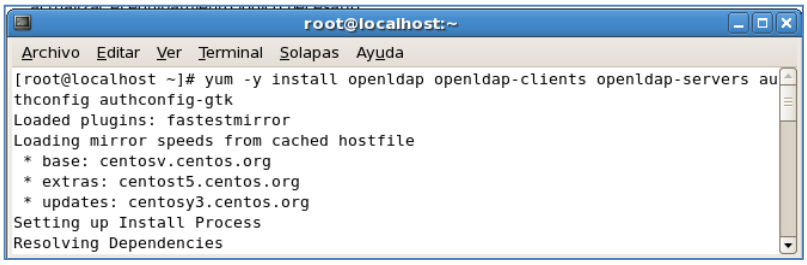


Figura IV. 1 Instalación de OpenLDAP

4.3.2. Desactivar la Protección del Sistema

Para que SELinux permita al servicio ldap funcionar normalmente, haciendo que se pierda toda la protección que brinda esta implementación, se utilizó el siguiente mandato en una terminal de comandos:

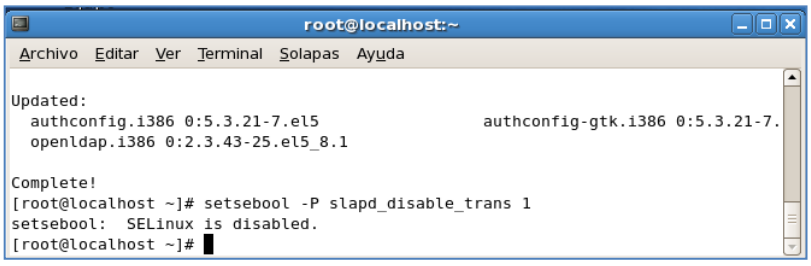


Figura IV. 2 Desactivar el SELinux

4.3.3. Creación de Directorios

Para tener organizada la información de ldap se crea un directorio específico con permisos de acceso exclusivamente al usuario y grupo ldap.

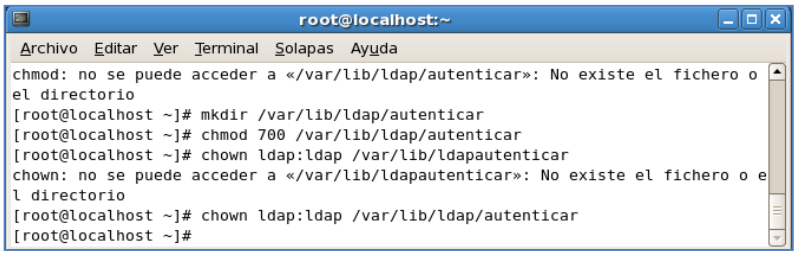


Figura IV. 3: Creación del Directorio autenticar

Además se requiere copiar el fichero DB_CONFIG.example dentro del directorio autenticar que se creó anteriormente con el nombre DB_CONFIG como muestra la figura. Este archivo es la configuración para la base de datos de ldap.

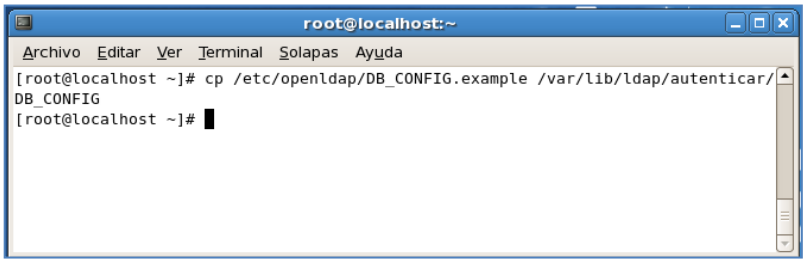


Figura IV. 4: Copiar la base de datos en el directorio autenticar

4.3.4. Generación de la clave de acceso para LDAP

Es necesario crear la clave de acceso que se asignará en LDAP para el usuario Administrador, utilizando el comando slappasswd.

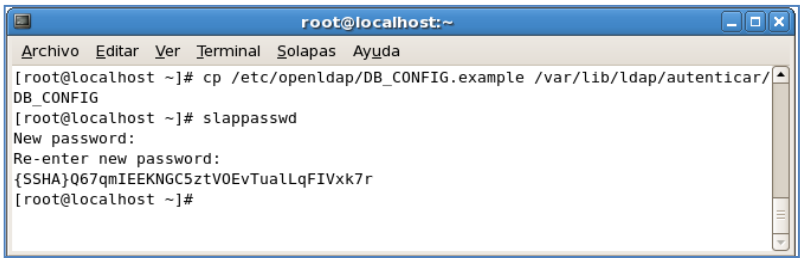


Figura IV. 5: Generar clave del administrador LDAP

Se recomienda por precaución copiar y respaldar este criptograma en un editor de texto, porque se la asignará en un fichero más adelante, y se definirá como clave de acceso para el usuario administrador.

4.3.5. Configuración del fichero slapd.conf

Para configurar el fichero /etc/openldap/slapd.conf se ha utilizado el editor de texto vi como nos muestra la siguiente figura.

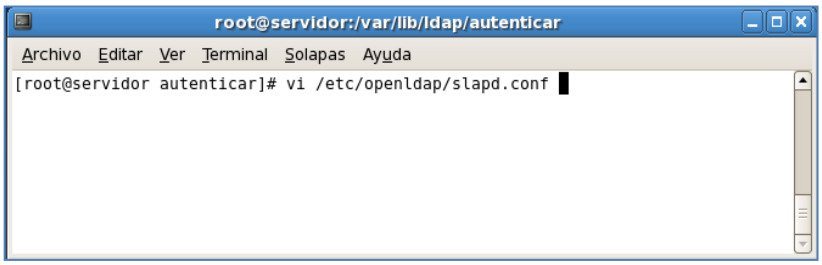


Figura IV. 6: Ingresar al fichero de configuración slapd.conf

Una vez ejecutado el editor de texto se accederá a configurar el fichero slapd.conf, y se verifica que estén presentes los esquemas mínimos requeridos.

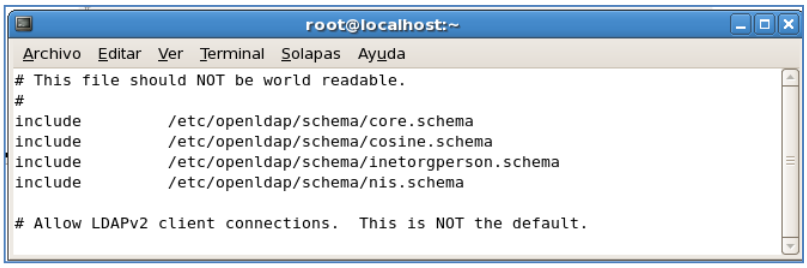


Figura IV. 7: Verificación de esquemas de configuración

Una vez cumplido lo anterior se prosigue revisando dentro del documento y se efectúan los siguientes cambios como muestra la pantalla:

Figura IV. 8: Edición del fichero slapd.conf

Aquí el dominio común que se utilizó para LDAP es dc=sistemas, dc=edu, que está ubicado en el campo suffix que significa sufijo, y si se desea se puede cambiar el nombre del administrador cn=Manager. Como puede observar en el campo rootpw va ubicada la calve del usuario administrador que se copió anteriormente, y el directorio donde va a estar ubicado es el que creamos inicialmente en /var/lib/ldap/autenticar.

Nota: Para empezar hacer cambios en el fichero, el editor de texto vi lo permite presionando la tecla **a** o **i** y para poder guardar la configuración presione ESC, luego dos puntos**: wq** y listo se han guardaron los cambios.

4.3.6. Levantamos el Servicio ldap

Una vez configurado correctamente lo anterior el siguiente paso es levantar el servicio ldap como muestra la figura, además con el siguiente comando chkconfig el servicio se iniciará automáticamente.

Figura IV. 9: Inicio del Servicio ldap

4.3.7. Migración de las cuentas existentes en el Sistema

Primero debe editar el fichero /usr/share/openldap/migration/migrate_common.ph

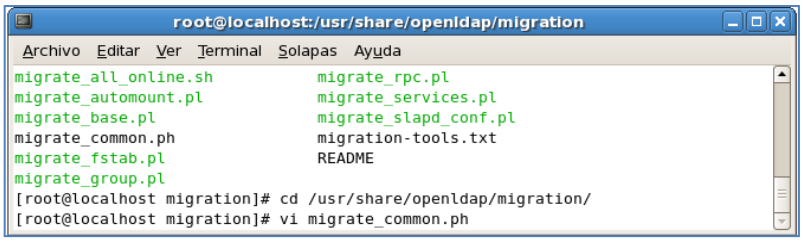


Figura IV. 10: Ingreso al fichero que configura la migración de datos

Y una vez dentro del fichero modificamos los siguientes valores, el dominio DNS por defecto y el componente de dominio.

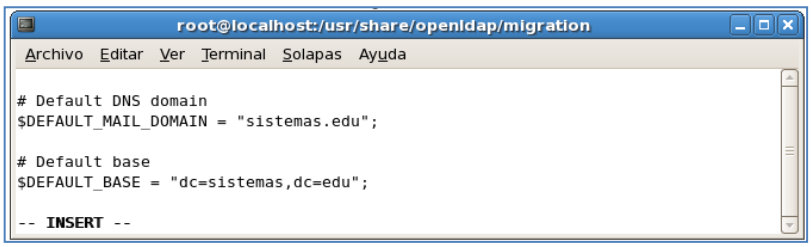


Figura IV.20: Edición del fichero de la migración de datos

A continuación hay que crear el objeto que a su vez contendrá el resto de los datos en el directorio. Genere un fichero base.ldif del siguiente modo:

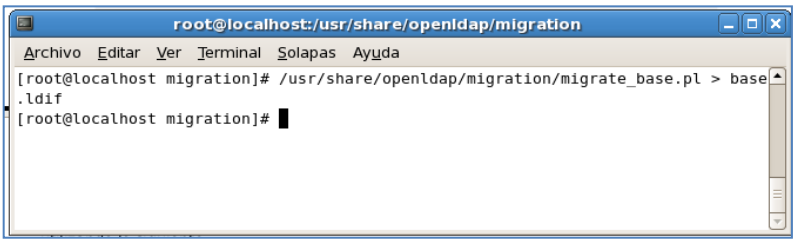


Figura IV. 11 Editar el fichero base.ldif donde se migran los datos

Se utiliza el comando **ldapadd** para insertar los datos necesarios en el fichero **base.ldif**. Para saber que hace cada opción se recomienda revisar la interfaz de los manuales del sistema **man**. A continuación se describen algunas de ellas.

-x autenticación simple

-W solicitar clave de acceso

-D nombre distinguido (dn) a utilizar

-h servidor LDAP a acceder

-f fichero a utilizar

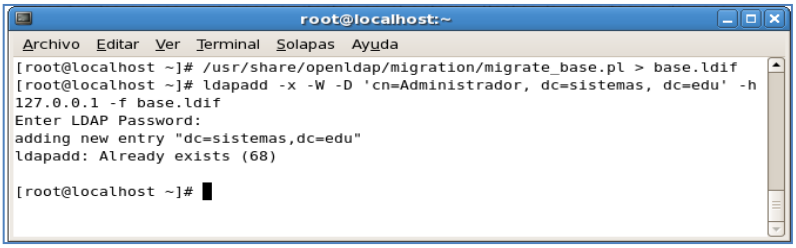


Figura IV. 12 Poblar el fichero con la información de LDAP

Una vez ejecutado lo anterior, se procedió a poblar el directorio con datos, importando los grupos y usuarios que existen en el sistema. Lo primero será crear los ficheros group.ldif y passwd.ldif.

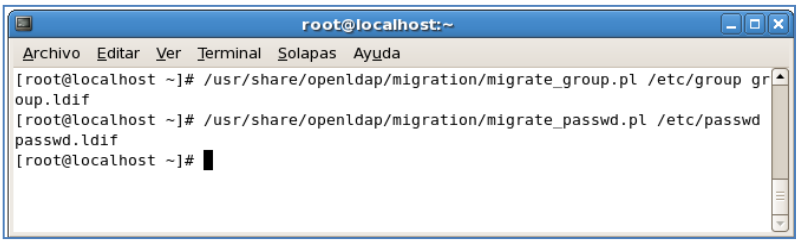


Figura IV. 13 Creación de ficheros para grupos y usuarios ldif

Ya creados los ficheros anteriores continúe añadiendo la información de los grupos y cuentas del sistema, incluido las claves de acceso

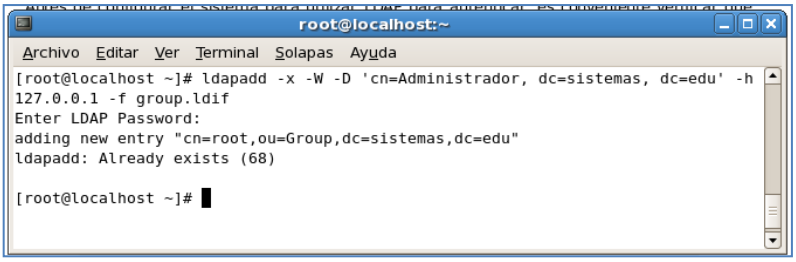


Figura IV. 14 Migrar los grupos y cuentas del sistema

Para añadir los datos del sistema una vez que se ha ejecutado el mandato, solicita el password, que es la clave que fue asignada al administrador LDAP anteriormente de allí nos permitirá migrar los datos. El mensaje que sale luego de haber ingresado la clave, que no les preocupe es a causa de que ya ha sido migrado anteriormente.

4.3.8. Comprobaciones del funcionamiento del Servidor

Antes de proseguir con el resto de la configuración de la autenticación ldap es conveniente verificar que todo funcione correctamente

La siguiente línea ejecutada dentro de la terminal de comandos, muestra que directorios hay disponibles en el servidor local.

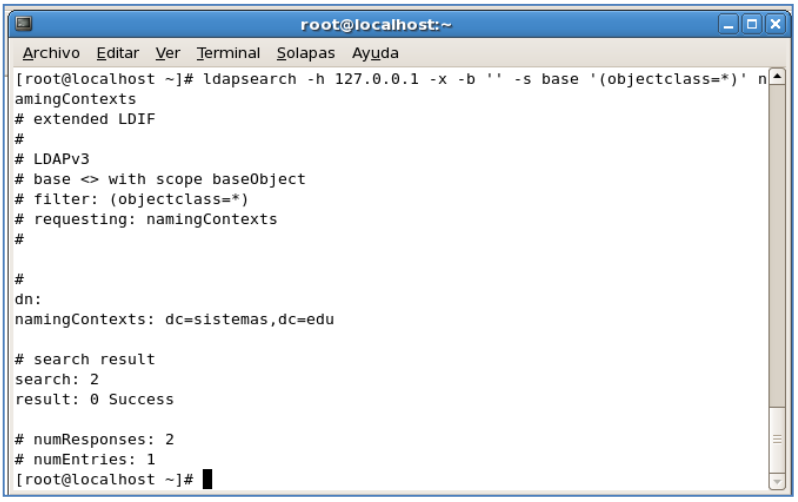


Figura IV. 15 Búsqueda de los sistemas bases disponibles LDAP

El siguiente mandato nos devuelve toda la información que existe dentro de todo el directorio (dc=sistemas, dc=edu)

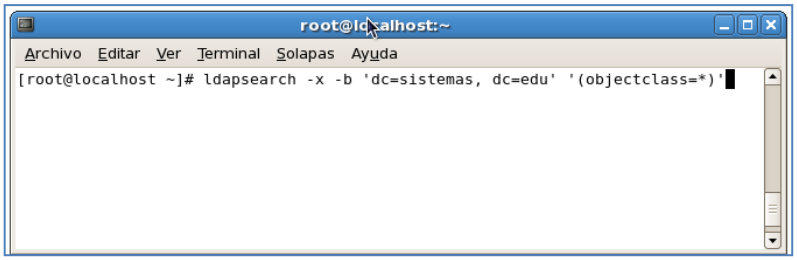


Figura IV. 16 Código de búsqueda de un directorio base

Una vez ejecutado el mandato anterior les devolverá algo como esto, incluida la información de todos los usuarios que fueron migrados anteriormente.

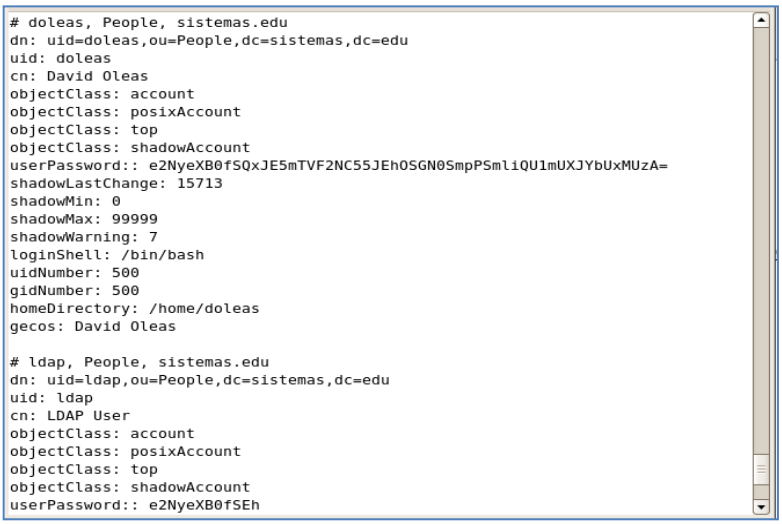


Figura IV. 17 Información de la base de datos ldap

Podrían también ver información personalizada de cada usuario, ejecutando el siguiente mandato en la terminal.

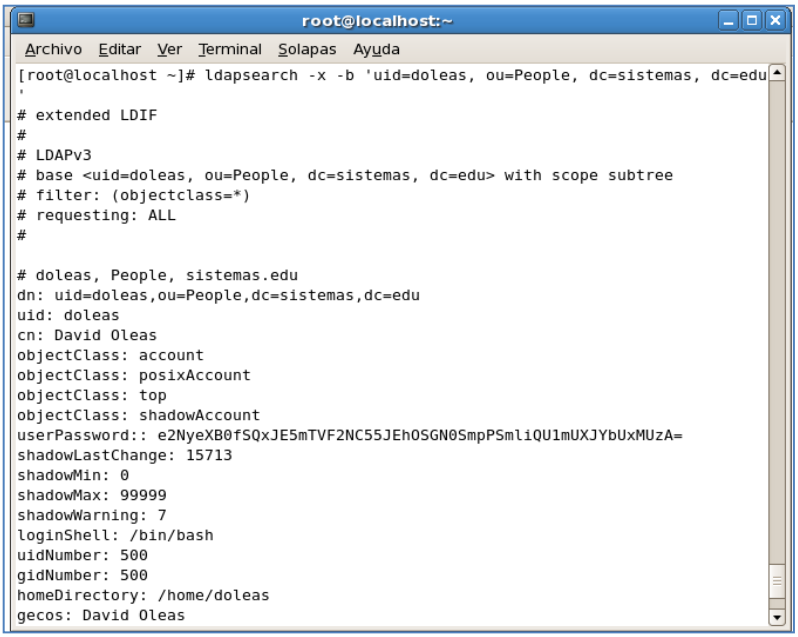


Figura IV. 18 Búsqueda personalizada de un usuario

4.4. Procedimiento de Configuración de DNS

La función que cumplirá DNS es almacenar la información necesaria para los nombres de dominio, resolviendo direcciones IP.

4.4.1. Instalación a través del comando yum

La instalación se lo realizó a través del comando yum, lo único que se necesita es tener salida a internet para realizar la instalación de todos los paquetes DNS.

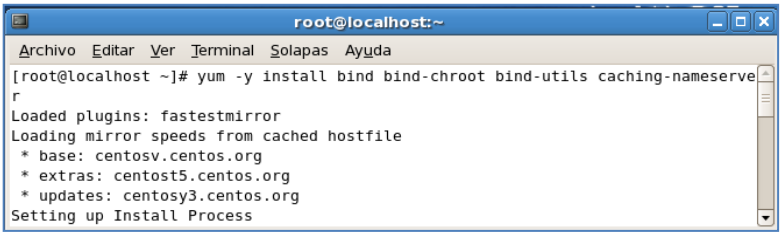


Figura IV. 19 Instalación de DNS y sus dependencias

Aquí muestra el total de paquetes descargados y el tamaño de cada uno de ellos.

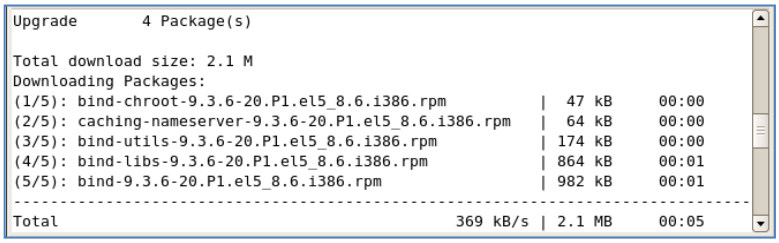


Figura IV. 20 Dependencias DNS instaladas

4.4.2. Creación mínima del archivo de Control named

Una vez instalado se procede a la configuración del fichero /var/named/chroot/etc/named.conf, que es la que permitirá utilizar el servicio, declarando las zonas que se utilizan en el servidor DNS. La configuración se realiza solo como un servidor maestro DNS.

Ejecutamos el siguiente mandato como muestra la figura a continuación:

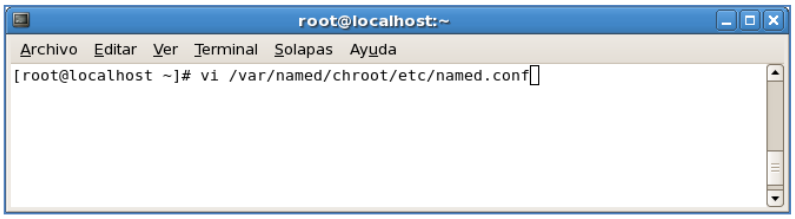


Figura IV. 21 Creación de ficheros que contendrá las zonas

Lo primero que se puede observar dentro de la estructura jerárquica definida en options {…} es la dirección del directorio que vamos a configurar.

Zone "sistemas.edu"

En esta zona está definido el dominio DNS "sistemas.edu", esta zona es conocida como de reenvío del dominio.

Zone "104.30.172.in-addr.arpa"

Aquí se encuentra definido de forma inversa de la dirección IP del servidor sistemas.edu el cuarto octeto se encuentra definido en el archivo de configuración named.172.30.104

Zone "localhost"

Esta zona le pertenece al localhost, se crea un fichero para resolver el nombre del localhost del sistema.

Zone "0.0.127.in-addr.arpa"

En esta zona se encuentra definido de forma inversa el localhost de la maquina, que es la dirección 127.0.0.1

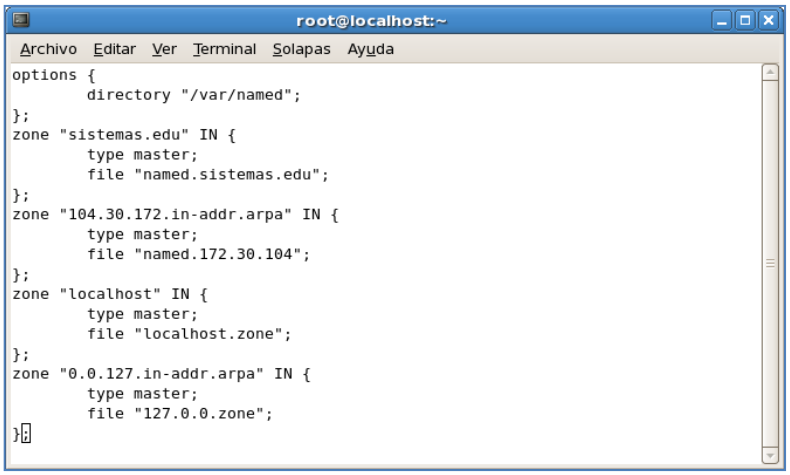


Figura IV. 22 Definición de zonas de un servidor maestro

4.4.3. Configuración de las Zonas de Autoridad

Como se definió anteriormente en la **zone "sistemas.edu"**, se crea el fichero **named.sistemas.edu**, y se puebla el fichero con la siguiente información.

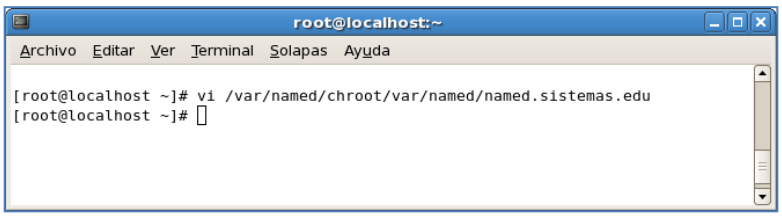


Figura IV. 23 Creación del fichero que envía el dominio a los clientes

En la parte inferior del fichero se puede observar el nombre de las máquinas y las direcciones IP que tiene cada una de ellas, incluida la del servidor.

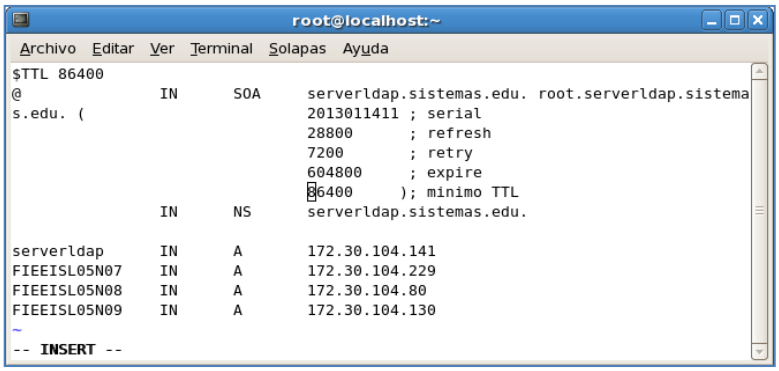


Figura IV. 24 Edición de datos al fichero que envira el dominio a clientes

Como ya estaba definido anteriormente en la **zone "104.30.172.in-addr.arpa"** se crea el fichero **named.172.30.104**, y poblamos el directorio con la siguiente información.

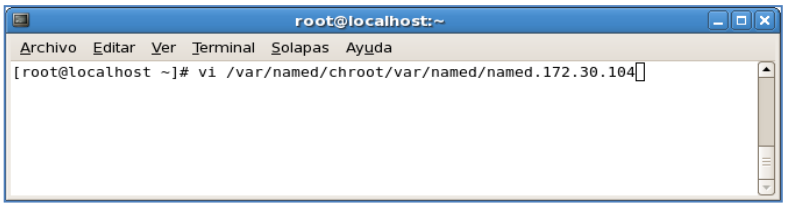


Figura IV. 25 Creación del fichero que resolverá la inversa de clientes

Como resuelve de forma inversa, en la parte inferior del fichero parte desde el último octeto de la dirección IP, para luego con el registro apuntador PTR resolver las direcciones IPV4 hacia el nombre de los anfitriones, incluido el nombre del servidor.

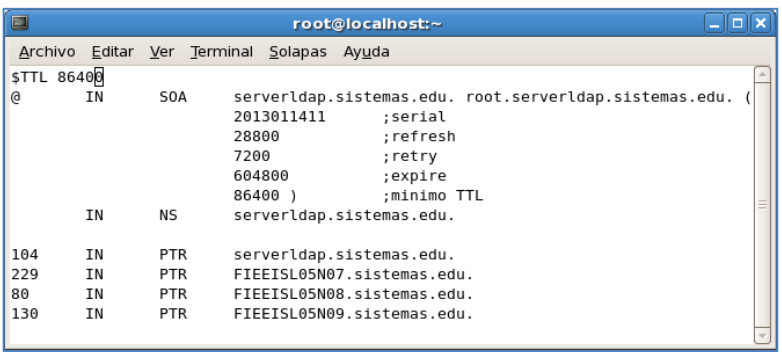


Figura IV. 26 Edición del fichero que resolverá la inversa de clientes

Como ya se definió anteriormente en la **zone "localhost"** se crea el fichero **localhost.zone**, y luego se procede a poblar el directorio de la siguiente forma:

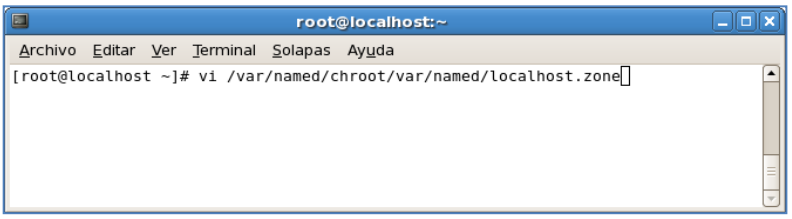


Figura IV. 27 Creación del fichero que resolverá el nombre del localhost

Al final del fichero se puede apreciar el reenvío del Dominio "**A"** al localhost de la máquina 127.0.0.1

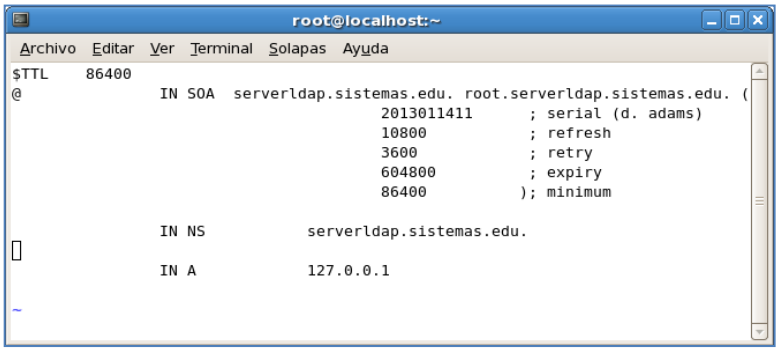


Figura IV. 28 Edición del fichero que resolverá la inversa de clientes

Como ya se ha definido anteriormente en la **zone ""0.0.127.in-addr.arpa"** se crea el fichero **127.0.0.zone**, y poblamos el directorio con la siguiente información.

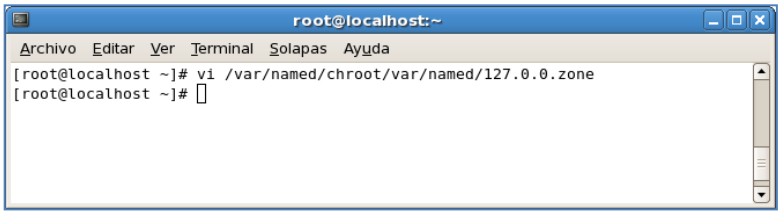


Figura IV. 29 Creación del fichero que resolverá la inversa del localhost

Aquí resuelve de forma inversa, y se aprecia al final del fichero, que parte desde el último octeto de la IP 127.0.0.1, para luego con el registro apuntador PTR resolver la dirección IPV4 hacia el nombre del localhost.

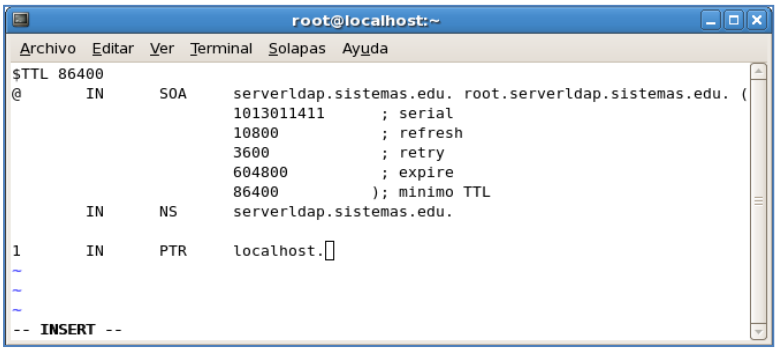


Figura IV. 30 Edición del fichero que resolverá la inversa del localhost

4.4.4. Configuración de los archivos del Sistema

Se procede a editar el hosts del sistema con la dirección y el nombre de la máquina del servidor.

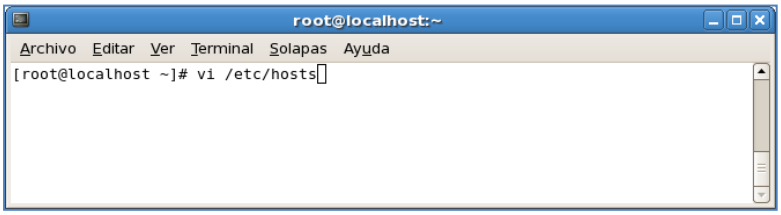


Figura IV. 31 Acceso al fichero hosts

Se ubica de la misma forma como está definido el localhost, primero la dirección IP del servidor y seguido el nombre del host de la máquina unido al dominio DNS, como muestra la figura.

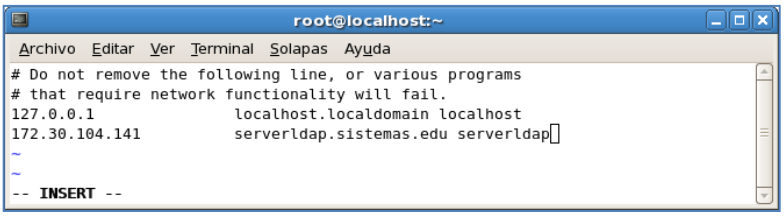


Figura IV. 32 Edición del fichero host para agregar el hostname

Edite el fichero /etc/sysconfig/network que contiene el nombre completo del hostname de la máquina.

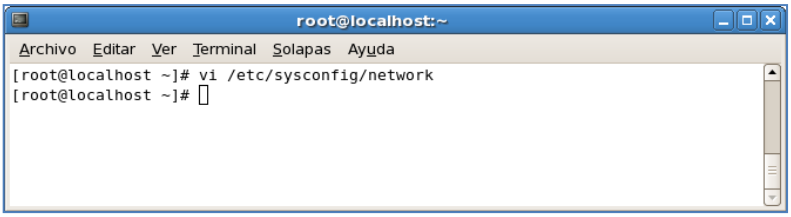


Figura IV. 33 Edición del fichero de red network

Se comenta el HOSTNAME del localhost y habilitamos el HOST del sistema que se ha definido anteriormente.

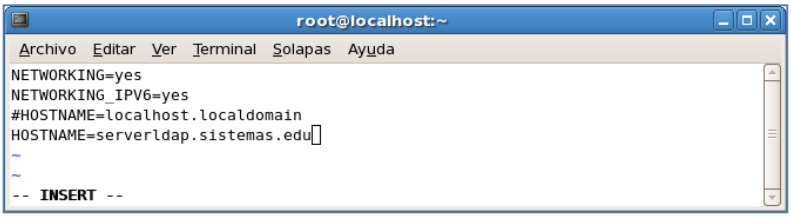


Figura IV. 34 Definir el hostname en el fichero de red network

Se edita el fichero /etc/resolv.conf, en el cual se añade el domino sistemas.edu y el nameserver que es la dirección IP del Servidor.

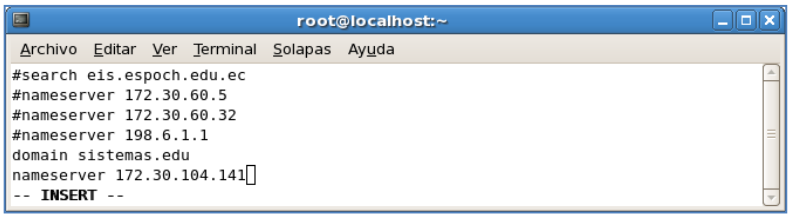


Figura IV. 35 Edición del fichero resolv.conf

Se reinicia el servicio named, como muestra la figura se ha levantado correctamente.

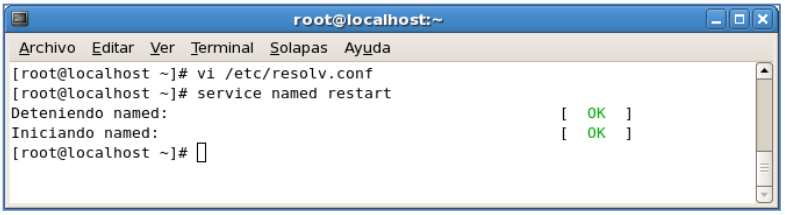


Figura IV. 36 Iniciando el servicio DNS

4.5. Procedimiento de Configuración de NFS

Está configuración cumple con la función de facilitar al servidor OpenLDAP la manera de poder replicar el directorio /home donde se encuentran almacenados los usuarios del sistema y que utiliza la base de datos de LDAP.

4.5.1. Configuración de ficheros

Editamos el fichero /etc/exports

Figura IV. 37 Edición del fichero exports para nfs

Una vez dentro del fichero montamos el /home de usuarios, asignándole la dirección IP, la máscara de subred y los permisos que va a tener el home en este caso de lectura y escritura.

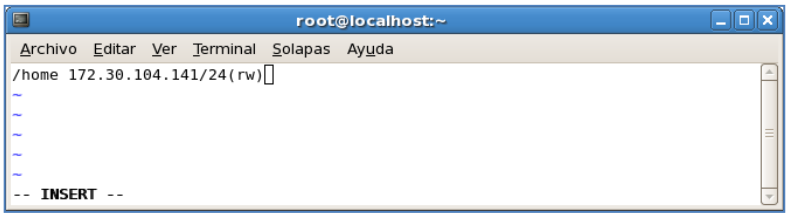


Figura IV. 38 Direccionamiento del home en nfs

Iniciamos el servicio de nfs, y como se aprecia en la figura la configuración tuvo éxito.

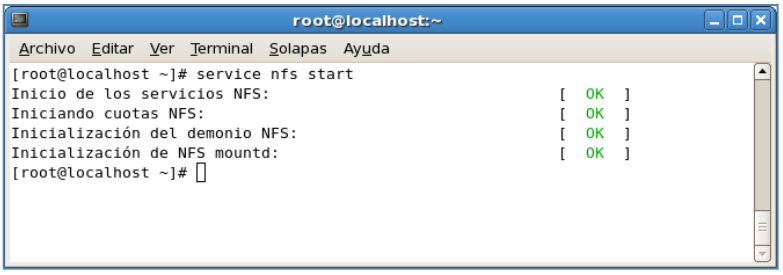


Figura IV. 39 Iniciando el servicio nfs

4.6. Procedimiento para Configurar Clientes Linux

La configuración de clientes Linux es sencilla, porque trabajan en la misma plataforma con el servidor.

Se tiene que configurar el fichero /etc/ldap.conf, asignando la misma dirección del host definida en el servidor LDAP y el parámetro base del dominio.

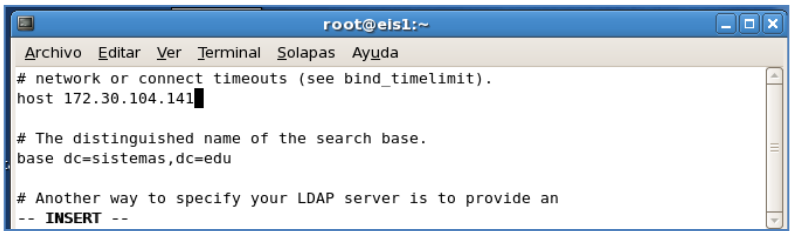


Figura IV. 40 Configuración del fichero ldap.conf

4.6.1. Configuración Authconfig

Se asigna en la terminal de comandos el mandato authconfig-tui. Habilite la utilización de LDAP y marque la Autenticación LDAP, clic en siguiente.

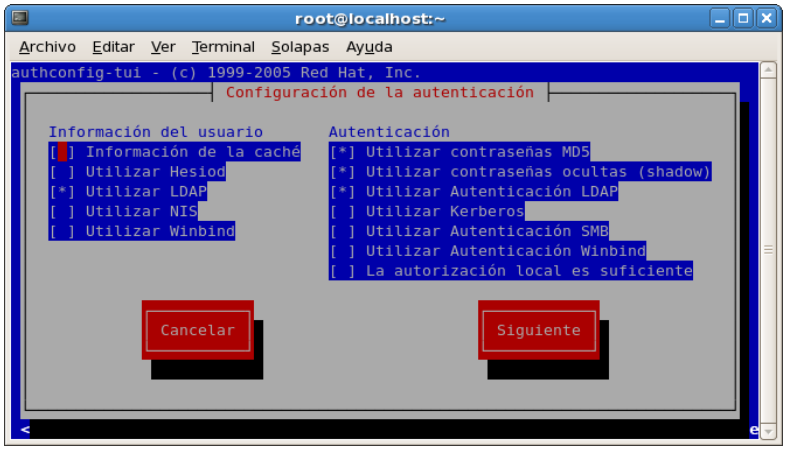


Figura IV. 41 Configuración de autenticación modo grafico

Se revisa si la dirección LDAP coincide con la del servidor OpenLDAP.

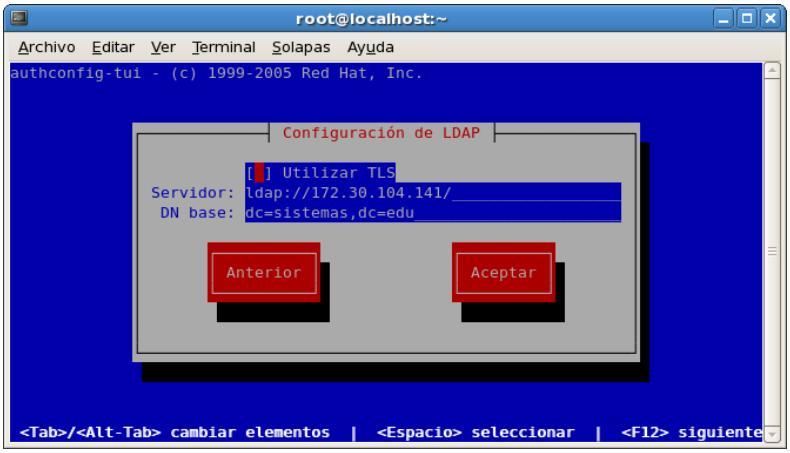


Figura IV. 42 Configuración LDAP modo gráfico

4.7. Procedimiento de Configuración de Samba

Es necesario configurar samba para unir al dominio sistemas.edu máquinas Windows, ya que smb es un protocolo que sirve como remplazo total para plataformas Microsoft.

4.7.1. Instalación de Samba a través de yum

Con el siguiente mandato ejecutado en una terminal de comandos automáticamente corre la instalación.

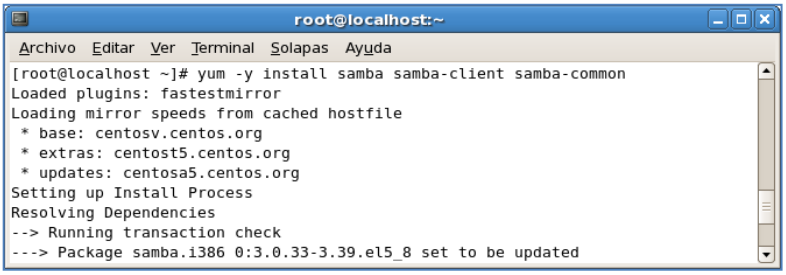


Figura IV. 43 Instalación de SAMBA

4.7.2. Configuración de Ficheros LDAP

Se debe copiar el archivo de esquema de samba al directorio de OpenLDAP que se configuró anteriormente.

Figura IV. 44 Copiando el esquema de samba en LDAP

Hay que editar el fichero de configuración de OpenLDAP /etc/openldap/slapd.conf y agregamos una línea más para que soporte el esquema de samba.

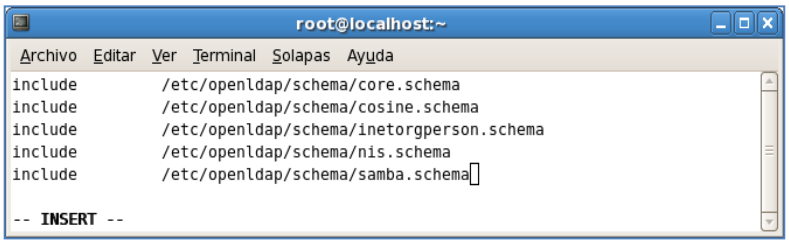


Figura IV. 45 Añadiendo esquema samba en ldap.conf

Siguiendo con el mismo archivo de configuración slapd.conf, de debe definir los objetos de samba en los índices para el sistema de búsqueda.

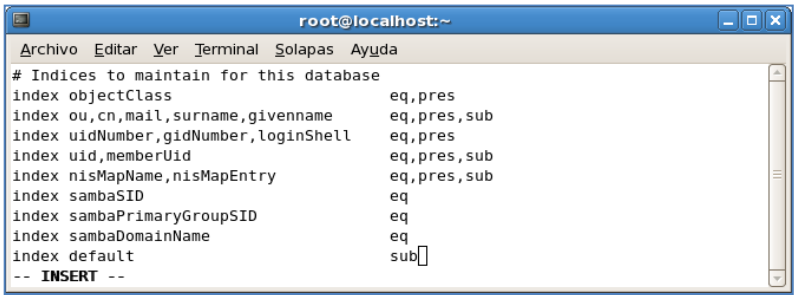


Figura IV. 46 Añadiendo los índices samba en slapd.conf

Editamos el fichero ldap.conf, para definir los parámetros globales del cliente.

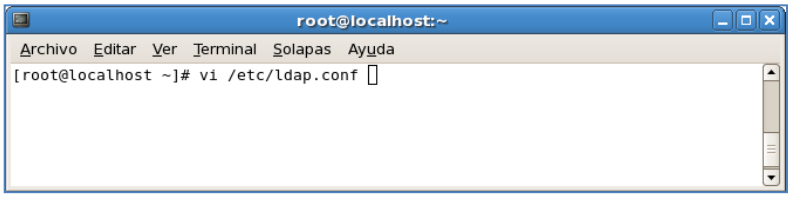


Figura IV. 47 Edición del fichero ldap.conf para definir parámetros globales

Se puede dejar la dirección del localhost definido en el host, en este caso se cambió por la dirección IP del servidor. El sistema base es el mismo que se configuró para LDAP.

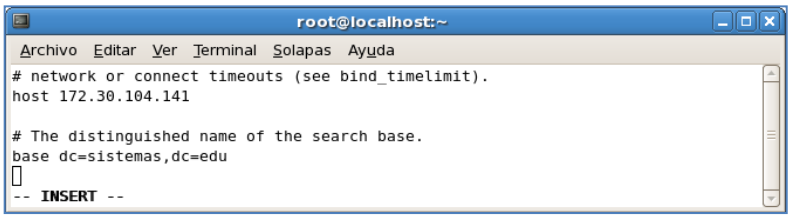


Figura IV. 48 Definición del host y sistemas base ldap

Se reinicia el servicio LDAP y con el comando chkconfig, se reiniciará el servicio automáticamente cada vez que se inicie la máquina.

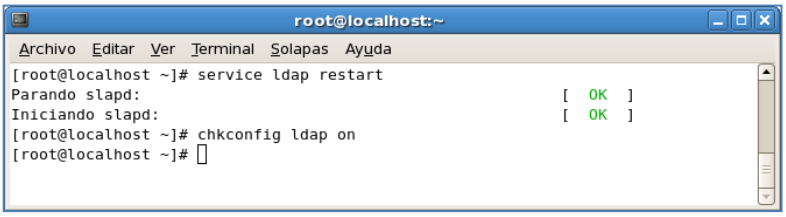


Figura IV. 49 Inicio del servicio ldap

4.7.3. Samba e Integración LDAP

Ahora se configura el fichero smb.conf

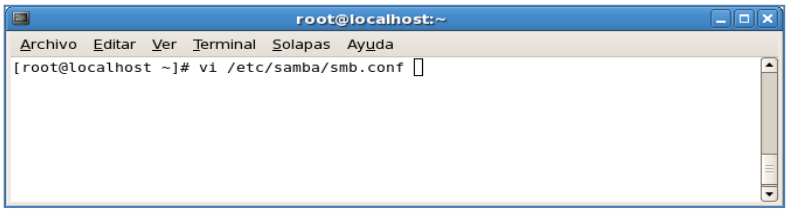


Figura IV. 50 Edición del fichero smb.conf del controlador samba

El archivo quedará poblado de la siguiente manera, asignando el dominio de LDAP, el nombre de nuestro servidor samba y el nombre del netbios. Se debe asignar la

dirección IP de nuestro servidor y la máscara, y que redes va a permitir asignar el dominio.

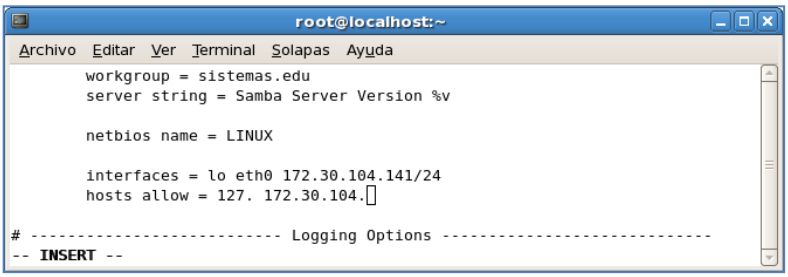


Figura IV. 51 Definición del dominio del fichero smb.conf

En la parte inferior del fichero agregamos los parámetros de LDAP, con la misma información definida anteriormente en el fichero slapd.conf de OpenLDAP.

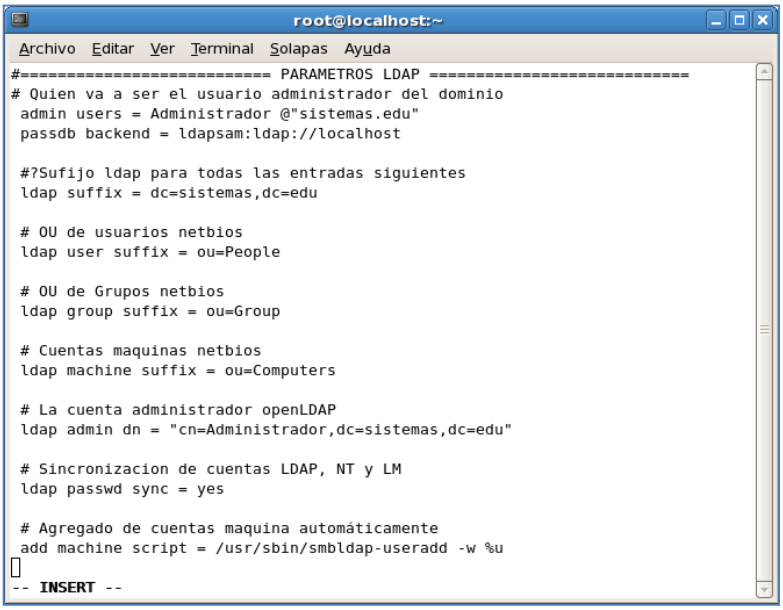


Figura IV. 52 Creación de parámetros LDAP en sbm.conf

Terminado la configuración anterior se procede a reiniciar el servicio samba y como se puede observar se ha levantado con éxito.

Figura IV. 53 Inicio del servicio samba

Se procede a instalar rpmforge, que es un repositorio de paquetes de software y que me va a permitir, la instalación de las herramientas samba para LDAP.

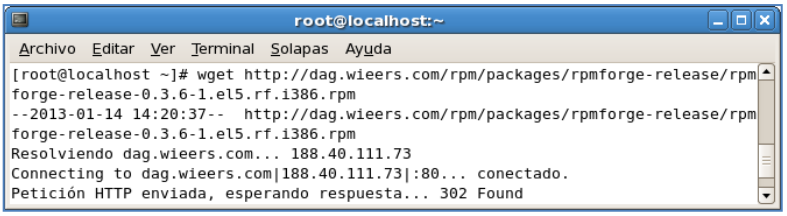


Figura IV. 54 Obtener de las dependencias samba para ldap en rpm

Edite el fichero rpmforge.repo en la siguiente dirección.

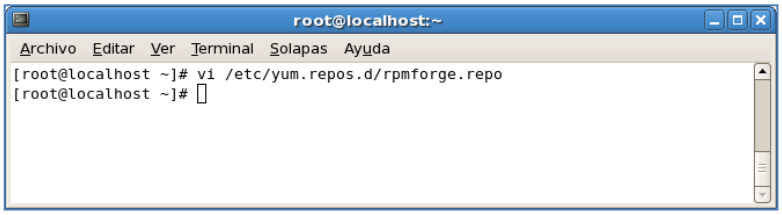


Figura IV. 55 Edición del fichero rpmforge

Una vez dentro del fichero, percátese de que enabled este deshabilitado con el valor de cero asignado.

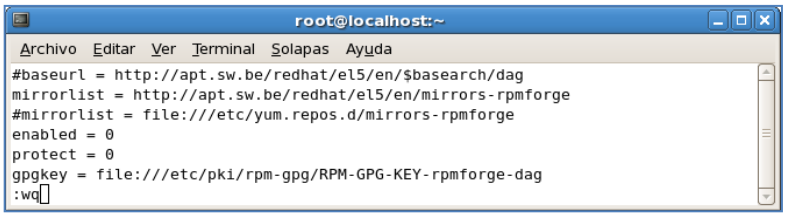


Figura IV. 56 Deshabilitar el rpm para poder instalar dependencias samba

Ahora ya es posible instalar **smb-tools**

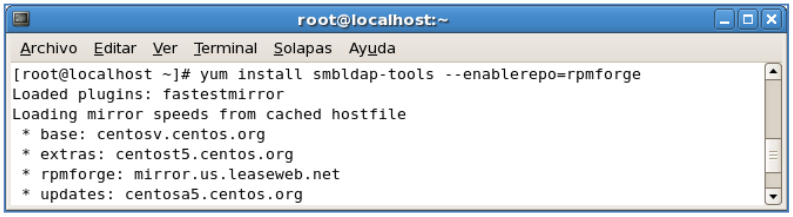


Figura IV. 57 Instalación de dependencias samba

Se observa todas las dependencias instaladas bajo el comando yum.

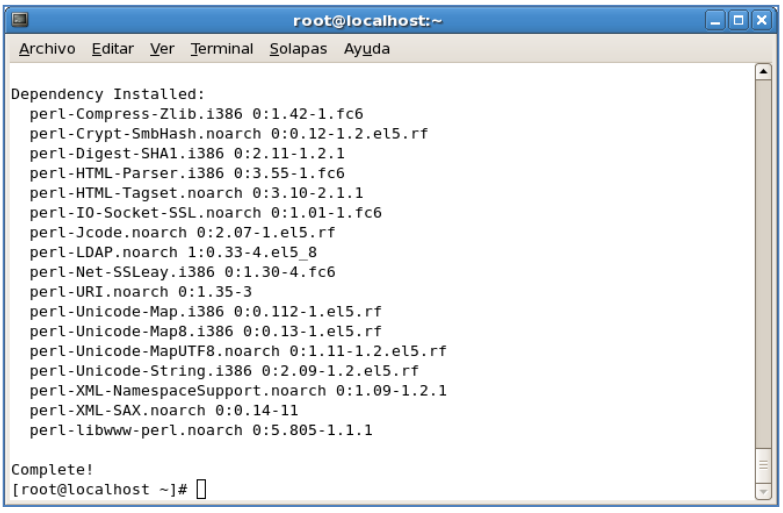


Figura IV. 58 Total de dependencias instaladas

Averiguamos el SID del servidor samba ejecutando **net getlocalsid** y se lo respalda, por si se realizan cambios en el host de la máquina o en el dominio.

Figura IV. 59 Respaldo del SID del servidor samba

Editemos el fichero **smbldap_bind.conf**

Figura IV. 60 Edición del fichero que configura el tipo de servidor

El fichero debe estar poblado de la siguiente manera, esto es para darle acceso a smb-tools la base de datos OpenLDAP.

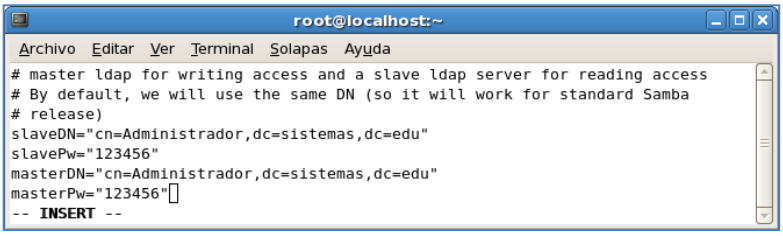


Figura IV. 61 Definición del nombre distintivo y la contraseña del servidor

Ahora si se edita la configuración principal, en el fichero **/etc/smbldap-tools/smbldap.conf.** Se agrega el SID que se copió anteriormente y más adelante el dominio del servidor samba como muestra la figura.

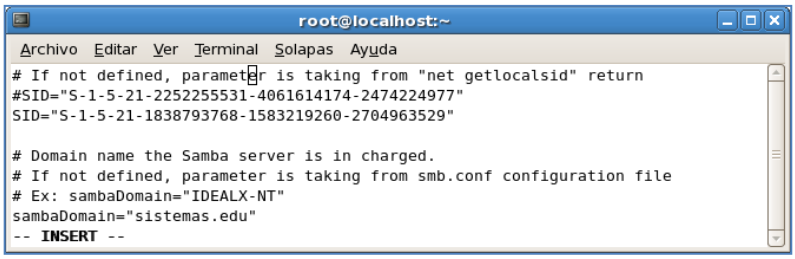


Figura IV. 62 Generando el SID del servidor samba

Se agrega la dirección del host de la máquina en el LDAP esclavo y master, asignando el puerto por defecto de LDAP que es el 389.

El fichero editado quedará de la siguiente manera:

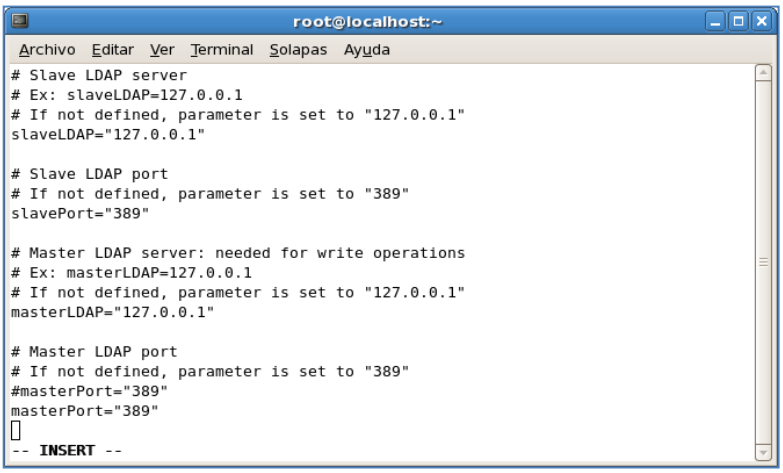


Figura IV. 63 Definición de los parámetros esclavo y maestro

Continuando con la edición del fichero smbldap.conf, asegurarse que el resto de los valores estén definidos de la siguiente manera.

smbldap-tools.conf : Q & D configuration file for smbldap-tools

This code was developed by IDEALX (http://IDEALX.org/) and

contributors (their names can be found in the CONTRIBUTORS file).

```
#
#               Copyright (C) 2001-2002 IDEALX
#
#  This program is free software; you can redistribute it and/or
#  modify it under the terms of the GNU General Public License
#  as published by the Free Software Foundation; either version 2
#  of the License, or (at your option) any later version.
#
#  This program is distributed in the hope that it will be useful,
#  but WITHOUT ANY WARRANTY; without even the implied warranty of
#  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#  GNU General Public License for more details.
#
#  You should have received a copy of the GNU General Public License
#  along with this program; if not, write to the Free Software
#  Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
#  USA.

#  Purpose :
#       . be the configuration file for all smbldap-tools scripts

##############################################################################
# General Configuration
##############################################################################

# Put your own SID. To obtain this number do: "net getlocalsid".
# If not defined, parameter is taking from "net getlocalsid" return
```

SID="S-1-5-21-4010884646-2165387387-290633870"

Domain name the Samba server is in charged.

If not defined, parameter is taking from smb.conf configuration file

Ex: sambaDomain="IDEALX-NT"

sambaDomain="sistemas.edu"

##

LDAP Configuration

##

Notes: to use to dual ldap servers backend for Samba, you must patch

Samba with the dual-head patch from IDEALX. If not using this patch

just use the same server for slaveLDAP and masterLDAP.

Those two servers declarations can also be used when you have

. one master LDAP server where all writing operations must be done

. one slave LDAP server where all reading operations must be done

(typically a replication directory)

Slave LDAP server

Ex: slaveLDAP=127.0.0.1

If not defined, parameter is set to "127.0.0.1"

slaveLDAP=localhost

Slave LDAP port

If not defined, parameter is set to "389"

slavePort=389

Master LDAP server: needed for write operations

Ex: masterLDAP=127.0.0.1

If not defined, parameter is set to "127.0.0.1"

masterLDAP=172.30.104.141

Master LDAP port

If not defined, parameter is set to "389"

masterPort=389

Use TLS for LDAP

If set to 1, this option will use start_tls for connection

(you should also used the port 389)

If not defined, parameter is set to "1"

ldapTLS="0"

How to verify the server's certificate (none, optional or require)

see "man Net::LDAP" in start_tls section for more details

verify=""

CA certificate

see "man Net::LDAP" in start_tls section for more details

cafile=""

certificate to use to connect to the ldap server

see "man Net::LDAP" in start_tls section for more details

clientcert=""

```
# key certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientkey=""

# LDAP Suffix
# Ex: suffix=dc=IDEALX,dc=ORG
suffix=dc=sistemas,dc=edu

# Where are stored Users
# Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for usersdn
usersdn="ou=People,${suffix}"

# Where are stored Computers
# Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for computersdn
computersdn="ou=Computers,${suffix}"

# Where are stored Groups
# Ex: groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for groupsdn
groupsdn="ou=Group,${suffix}"

# Where are stored Idmap entries (used if samba is a domain member server)
# Ex: groupsdn="ou=Idmap,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for idmapdn
```

idmapdn="ou=Idmap,${suffix}"

Where to store next uidNumber and gidNumber available for new users and groups

If not defined, entries are stored in sambaDomainName object.

Ex: sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"

Ex: sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"

sambaUnixIdPooldn="sambaDomainName=sistemas.edu,${suffix}"

Default scope Used

scope="sub"

Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA, CLEARTEXT)

hash_encrypt="SSHA"

if hash_encrypt is set to CRYPT, you may set a salt format.

default is "%s", but many systems will generate MD5 hashed

passwords if you use "1%.8s". This parameter is optional!

crypt_salt_format=""

##

Unix Accounts Configuration

##

Login defs

Default Login Shell

Ex: userLoginShell="/bin/bash"

userLoginShell="/bin/bash"

Home directory

Ex: userHome="/home/%U"

userHome="/home/%U"

Default mode used for user homeDirectory

userHomeDirectoryMode="700"

Gecos

userGecos="System User"

Default User (POSIX and Samba) GID

defaultUserGid="513"

Default Computer (Samba) GID

defaultComputerGid="515"

Skel dir

skeletonDir="/etc/skel"

Default password validation time (time in days) Comment the next line if

you don't want password to be enable for defaultMaxPasswordAge days (be

careful to the sambaPwdMustChange attribute's value)

defaultMaxPasswordAge="45"

```
#############################################################################
# SAMBA Configuration
#############################################################################

# The UNC path to home drives location (%U username substitution)
# Just set it to a null string if you want to use the smb.conf 'logon home'
# directive and/or disable roaming profiles
# Ex: userSmbHome="\\PDC-SMB3\%U"
userSmbHome="\LINUX\%U"

# The UNC path to profiles locations (%U username substitution)
# Just set it to a null string if you want to use the smb.conf 'logon path'
# directive and/or disable roaming profiles
# Ex: userProfile="\\PDC-SMB3\profiles\%U"
userProfile="\LINUX\profiles\%U"

# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
# Ex: userHomeDrive="H:"
userHomeDrive="Z:"

# The default user netlogon script name (%U username substitution)
# if not used, will be automatically username.cmd
# make sure script file is edited under dos
# Ex: userScript="startup.cmd" # make sure script file is edited under dos
userScript=""
```

```
# Domain appended to the users "mail"-attribute
# when smbldap-useradd -M is used
# Ex: mailDomain="idealx.com"
mailDomain=""

##############################################################################
#########
#
# SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
#
##############################################################################
#########

# Allows not to use smbpasswd (if with_smbpasswd="0" in smbldap.conf) but
# prefer Crypt::SmbHash library
with_smbpasswd="0"
smbpasswd="\usr\bin\smbpasswd"

# Allows not to use slappasswd (if with_slappasswd="0" in smbldap.conf)
# but prefer Crypt:: libraries
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"

# comment out the following line to get rid of the default banner
# no_banner="1"
```

Se crea la clave de acceso al Dominio samba con el comando **smbpasswd,** como se puede observar marca un error porque necesita que la clave sea la misma del súper usuario (root).

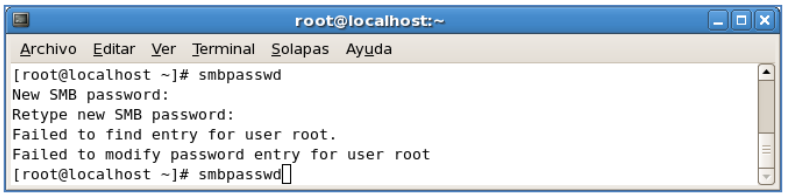


Figura IV. 64 Generando el password del servidor samba

Para revisar toda la configuración de los ficheros, debe ejecutar configure.pl en la siguiente dirección y con los permisos correspondientes de acceso.

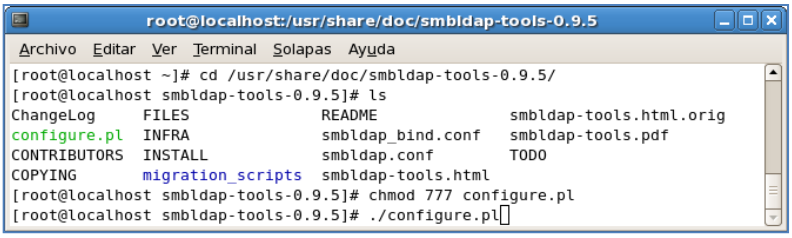


Figura IV. 65 Verificando la información del fichero smbldap.conf

Se comprueba que todos los servicios que se configuraron se inicien correctamente

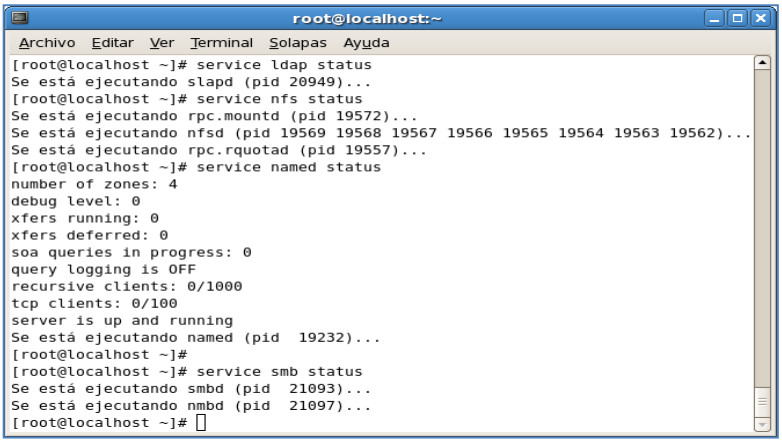


Figura IV. 66 Comprobación de todos los servicios en ejecución

Listo se terminó con la configuración de OpenLDAP con la integración DNS y SAMBA.

4.8. Unir al Dominio Samba Clientes Windows

En la terminal de comandos del sistema Linux se agregó el siguiente mandato con el fin de tener acceso a los usuarios del sistema, las mismas que fueron migradas a OpenLDAP anteriormente. Ingrese la misma contraseña del usuario del sistema.

Figura IV. 67 Agregando las cuentas del sistema a samba

Se crea como usuario al nombre del equipo de Windows, tal y como muestra la siguiente figura:

Figura IV. 68 Añadiendo a la máquina cliente como usuario

Se asigna la cuenta creada anteriormente a samba con el fin de que la máquina pueda tener acceso al dominio.

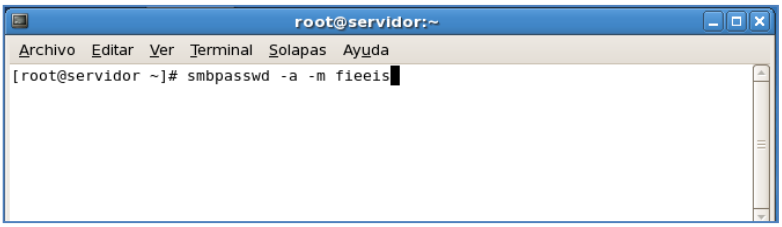


Figura IV. 69 Asignando la cuenta al sistema samba

Revise el fichero passwd para modificar el usuario que es la maquina Windows creado anteriormente y junto al nombre se le asigna un $.

Figura IV. 81: Editando la cuenta de la maquina cliente

Es importante que el administrador del sistema (root) este asignado a samba con la misma contraseña utilizada para ingresar al sistema. Esto ya se hizo anteriormente en la configuración de ficheros samba, pero puede volver hacerlo.

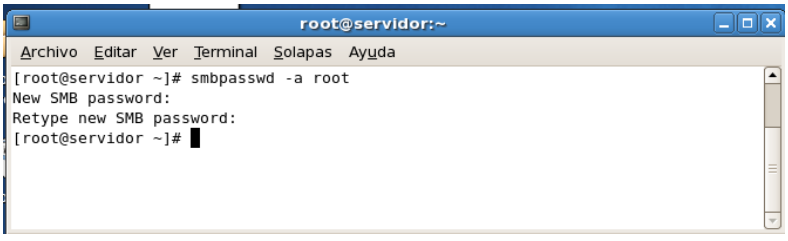


Figura IV. 70: Generando la contraseña de samba

Para ingresar al dominio sistema.edu desde Windows se lo hace desde propiedades del equipo – Nombre de equipo – Cambiar. Se agrega en dominio **sistemas .edu** y le pedirá un usuario y una contraseña para unirse al dominio.

La primera vez será con la cuenta del administrador root del sistema Linux y la contraseña.

Una vez conectado pedirá reiniciar el sistema y podrá ingresar con las cuentas que haya asignado a samba como muestra la figura.

Figura IV. 71 Autenticación al dominio samba ldap

Listo se autenticado al dominio samba con éxito y el menú de inicio muestra el usuario del sistema.

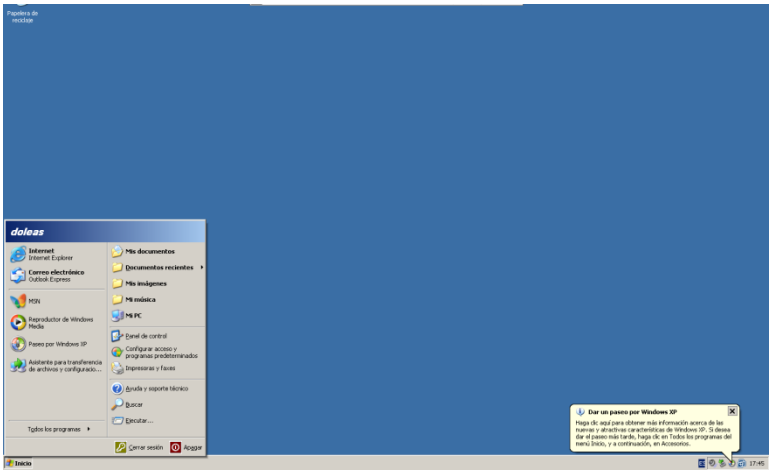


Figura IV. 72 Comprobación del ingreso a la cuenta samba ldap

4.9. Pruebas de conexión a la base de datos OpenLDAP

Para ver si el servidor LDAP está ejecutando la conexión del usuario autenticado se ejecuta el siguiente mandato de búsqueda en la terminal de comandos.

ldapsearch -x -b 'dc=sistemas, dc=edu' '(objectclass=*)'

Se observa el número de respuestas y entradas que tiene el servidor.

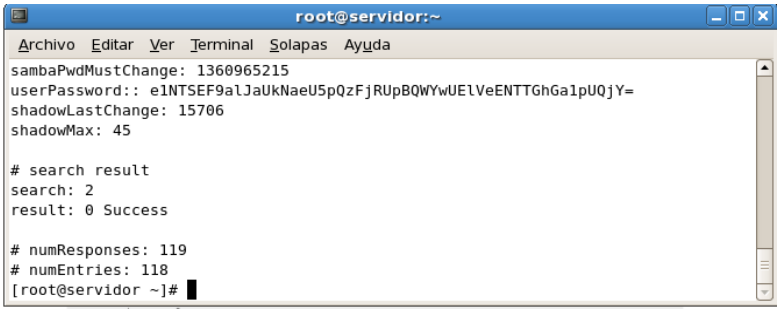


Figura IV. 73 Prueba de conexión

4.10. Administración LDAP

Hay una gran cantidad de programas para acceder a la administración de servidores LDAP, pero la mayoría sirve para administrar usuarios y grupos del sistema. La herramienta que se utilizó en esta configuración es PHP LDAP Admin.

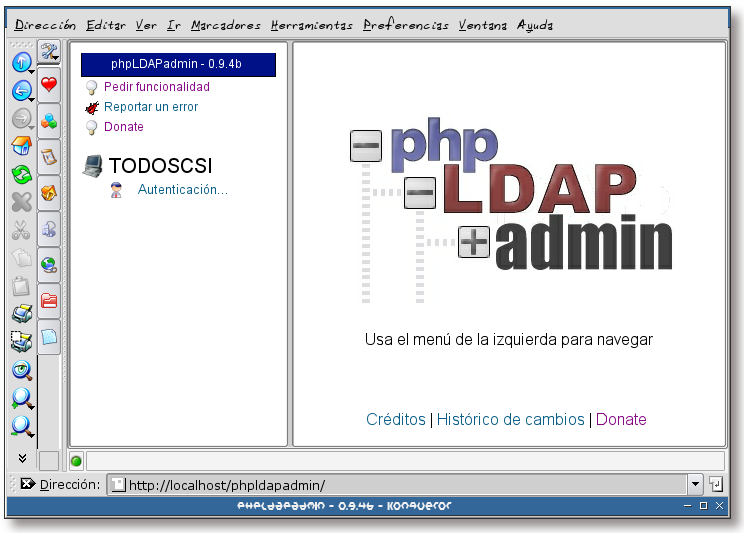


Figura IV. 74 Herramienta administrativa PHPLDAPADMIN

CONCLUSIONES

1. El estudio de la arquitectura del protocolo LDAP, permite conocer los servicios que ofrece y el comportamiento que tiene el protocolo, definiendo conceptos que son esenciales para la implementación.
2. El protocolo LDAP se encuentra en su 3ra versión y ya está estandarizada por el IETF (Grupo de trabajo de Ingeniería de Internet). Por lo tanto existen los RFC (petición de comentarios) para cada versión de internet.
3. LDAP presenta la información bajo la forma de una estructura jerárquica de directorios, formado por un conjunto de pares clave/valor denominadas atributos.
4. La investigación realizada en páginas de internet actuales, en foros y por medio de una encuesta en línea permitió definir que OpenLDAP y OpenDS son las implementaciones más adecuada para el análisis.
5. El análisis comparativo de las Implementaciones del protocolo LDAP, dieron como resultado que la herramienta más optima para la implantación de un sistema de autenticación es OpenLDAP, de a cuerdo a los resultados y valores obtenidos.
6. La diferencia de los resultados obtenidos en el análisis comparativo de las implementaciones es mínimo, ya que OpenLDAP tiene el 50.49% y OpenDS el 49.51%.
7. La implementación de OpenLDAP como un sistema de autenticación implantada en los laboratorios de la EIS, permite el control de cuentas de usuario de una manera organizada y jerárquica, administrada desde un servidor.
8. La implantación de un sistema de autenticación permite la integración de sistemas, DNS, NFS y SAMBA

RECOMENDACIONES

1. Se debe tener claro todos los conceptos de la estructura que tiene definida LDAP, para poder aplicar sus servicios.
2. Se debe utilizar LDAP para llevar registros de información que no vayan a ser actualizados permanentemente.
3. Se recomienda utilizar un estudio comparativo para escenarios similares, en los que se necesita establecer el grado de cumplimiento de ciertos estándares.
4. Para poder implantar un sistema de autenticación LDAP, es necesario la integración de sistemas, como DNS, NFS y SAMBA
5. LDAP debe implantarse en empresas u organizaciones que manejan gran cantidad de información de usuarios y diferentes plataformas, porque ofrece seguridad e integridad de los datos.
6. Es recomendable el uso de la implementación OpenLDAP, ya que es software libre y la licencia no tiene costo.
7. Para implementar LDAP como un servidor de autenticación, se recomienda que los recursos hardware sean óptimos, para evitar problemas en el rendimiento del equipo.
8. Es necesario realizar respaldos permanentes de la base de datos, ya que si ocurre un desperfecto se la puede restaurar inmediatamente.

RESUMEN

El “ANALISIS DE LAS IMPLEMENTACIONES DEL PROTOCOLO LDAP. CASO PRACTICO: IMPLANTACION DE UN SISTEMA DE AUTENTICACION APLICADO A LOS LABORATORIOS DE LA EIS”, se realizó con el propósito de llevar el control de ingresos de estudiantes a los computadores de los laboratorios de la Escuela de Ingeniería en Sistemas de la ESPOCH, generando cuentas de usuario para administrar el acceso desde un servidor.

Mediante Estadística Descriptiva se realizó un análisis comparativo de las implementaciones de OpenLDAP y OpenDS, aplicando módulos de prueba por cada uno de los indicadores definidos que son: Instalación y Administración, Autenticación, Seguridad y Rendimiento, de esta manera se pudo obtener valores cuantitativos y realizar la representación de los datos en un diagrama de barras simple.

Por observación directa de los resultados obtenidos, se determinó que la implementación más idónea para implantar un servidor de autenticación es OpenLDAP, que alcanzó un porcentaje del 50.49%, seguido de OpenDS con un porcentaje del 49.51%.

La diferencia de los resultados de las Implementaciones es mínima, debido a que OpenDS es mejor en la instalación y administración, en cambio OpenLDAP es superior en la autenticación de los usuarios y en el rendimiento del servidor

La implantación del sistema de autenticación se lo realizó bajo el sistema operativo de software libre CentOS, configurando la implementación OpenLDAP, y a la vez se tuvo que integrar diferentes servicios, para poder tener acceso a las múltiples plataformas.

Es necesario realizar respaldos permanentes de la base de datos, ya que si ocurre un desperfecto se la puede restaurar inmediatamente.

ABSTRACT

"LDAP (Light Directory Access Protocol) PROTOCOL IMPLEMENTATION ANALYSIS, A PRACTICAL CASE: AN AUTHENTICATION SYSTEM IMPLEMENTATION APPLIED TO EIS (School of Systems Engineering) LABORATORIES." The purpose of this analysis was to monitor the students` access to computers in the School of Systems Engineering laboratories at ESPOCH (Escuela Superior Politécnica de Chimborazo), generating, this way, user`s accounts for administrating access from a server.

An open LDAP (Light Directory Access Protocol) and open DS (Direct Service) comparative analysis was executed by means of Descriptive Statistics using testing modules in each definite indicator, for example, installation and administration, authentication, security and output; therefore, it was possible to obtain what follows: Quantitative values, and the doing of data representation through simple bar graphs.

Through direct observation of the obtained results, it was determined that the most suitable implementation for implanting an authentication server constitutes the Open LDAP which reached 50.49 per cent, followed by the Open DS with a 49.51 per cent.

The implementation results difference is minimal because the Open DS is better concerning installation and administration; whereas the Open LDAP is best due to users` authentication and server performance.

The authentication system implantation was done under CentOS free software operating system, configuring this way the Open LDAP implementation, at the same time, several services were integrated to accessing multiple platforms.

It is necessary to accomplish permanent backups, in case failure occurred, so that it can be immediately reset.

BIBLIOGRAFIA

1. **ACTIVE DIRECTORY**
   http://es.wikipedia.org/wiki/Active_Directory
   2011 - 02 - 16

2. **APACHEDS**
   http://directory.apache.org/apacheds/1.0/apacheds-v10-features.html
   2012 - 09 - 12

3. **AUTENTICACIÓN**
   http://es.wikipedia.org/wiki/Autenticaci%C3%B3n
   2011 – 02 - 16

4. **CURSO OPENLDAP**
   http://www.redes-linux.com/manuales/openldap/curso_openldap.pdf
   2011 - 02 - 22

5. **CURSO OPENLDAP**
   http://www.redes-linux.com/manuales/openldap/curso_openldap.pdf
   2011 - 08 - 26

6. **COMPARISON OF DIRECTORY / LDAP SERVERS**
   http://thoughtblender.info/2008/11/04/comparison-of-directory-ldap-servers/
   2012 - 09 - 12

7. **HISTORIA LDAP**
   http://www.ldapconfig.net/2011/09/un-poco-de-historia.html
   2012 - 09 - 17

8. **HISTORIA OPENDS**

http://es.knowledger.de/0131553/OpenDS

2012 - 09 - 17

9. **LDAP**

http://es.wikipedia.org/wiki/LDAP

2011 - 02 - 22

10. **LDAP**

http://es.wikipedia.org/wiki/LDAP

2011 - 08 - 24

11. **LDAP**

http://es.wikipedia.org/wiki/LDAP

2012 - 09 - 12

12. **OPENLDAP**

http://es.wikipedia.org/wiki/OpenLDAP

2012 - 09 - 17

13. **PROTOCOLO LDAP**

http://es.kioskea.net/contents/internet/ldap.php3

2011 - 08 - 30

14. **PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS (LDAP)**

http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ldap.html

2012 - 09 - 17

15. **SERVICIO DE DIRECTORIO DE OPENLDAP**

http://biblioteca.utec.edu.sv/siab/virtual/articulos_soft_libre/Servicio_de_escritorio_OpenLDAP.pdf

[2011 - 08 - 24]

16. **UN SERVIDOR DE DIRECTORIO DE FUENTE ABIERTA**
http://mscerts.programming4.us/es/645174.aspx
[2012 - 09 - 17]

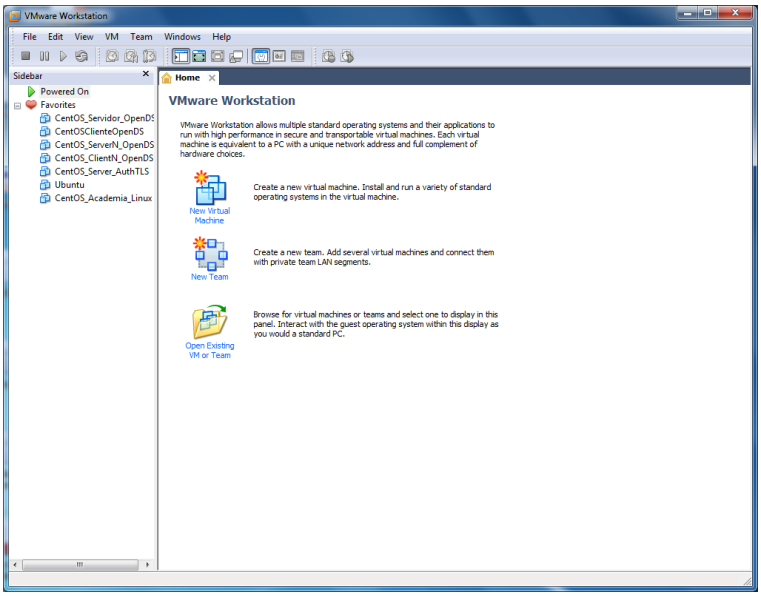
17. **UTILIZACIÓN DEL REGISTRO LDAP**
http://publib.boulder.ibm.com/tividd/td/ITAME/GC23-4684-00/es_ES/HTML/adminmst11.htm
[2011 - 08 - 26]

ANEXOS

ANEXO 1

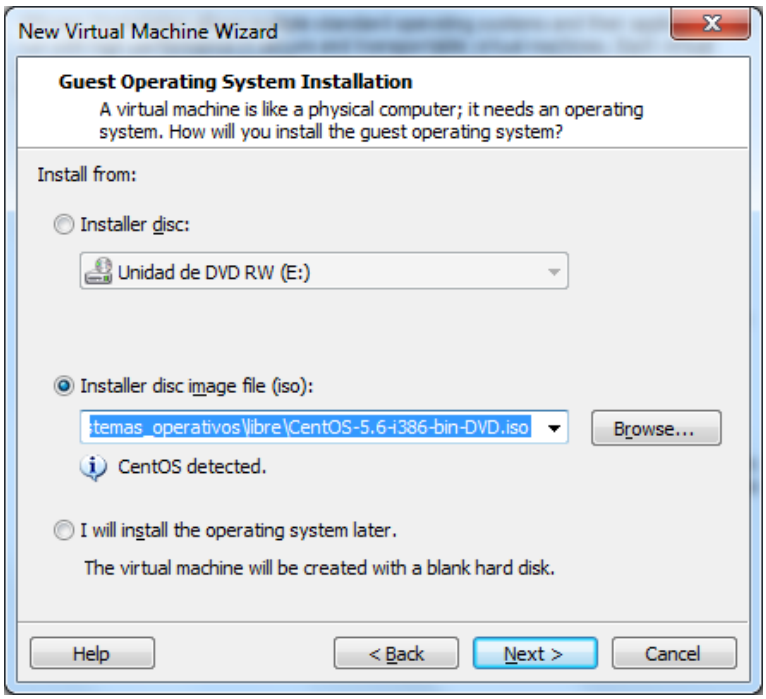
INSTALACION DE CENTOS

Ejecutamos la Maquina virtual VMware 7 y damos clic en New Virtual Machine

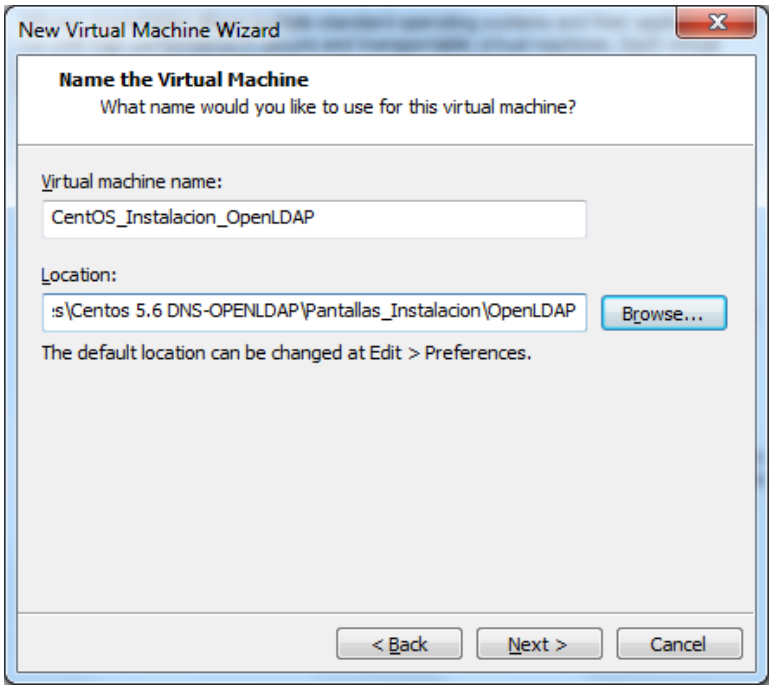


Se elije el modo de instalación, en este caso se realiza con una imagen que está ubicada en un servidor de archivos, a la dirección \\172.30.104.10\software\sistemas_operativos\libre\CentOS-5.6-i386-bin-DVD.iso.

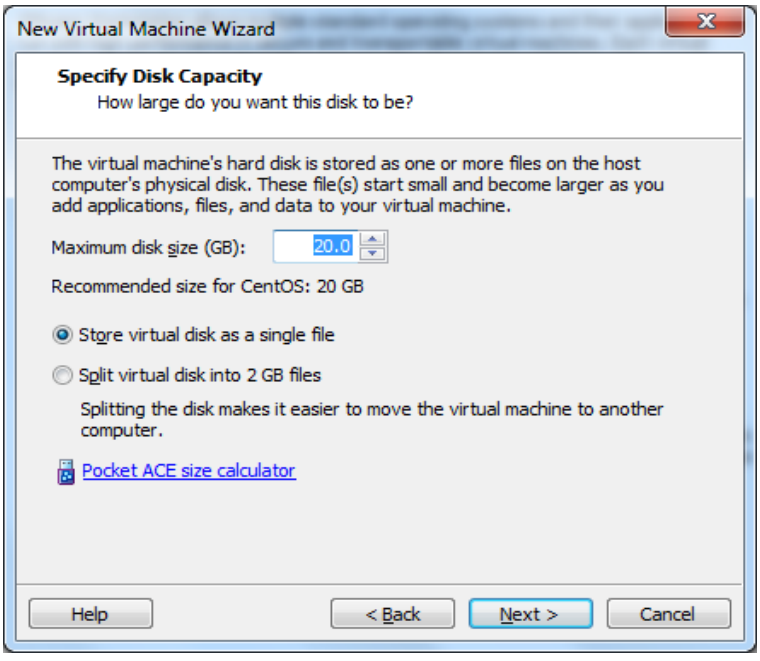
Damos clic en siguiente.



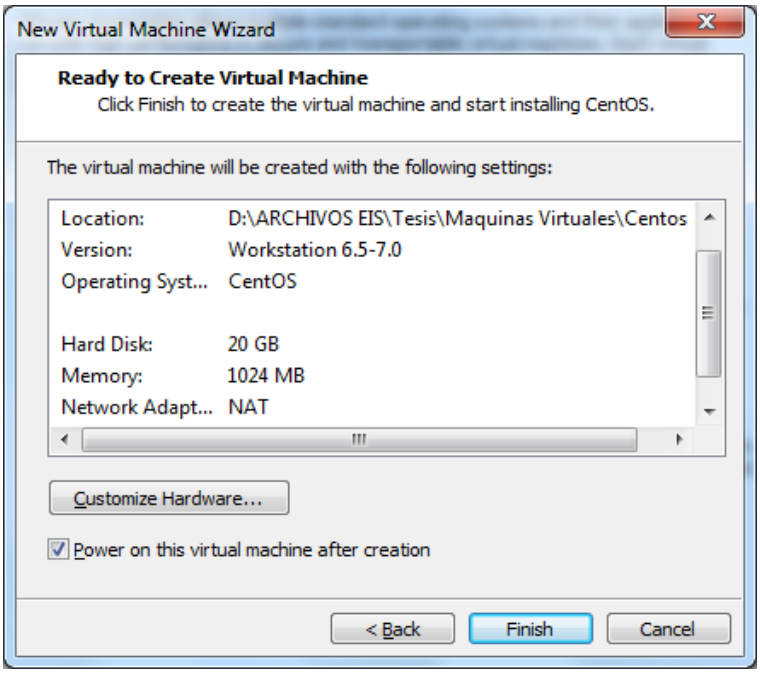
En esta pantalla por defecto aparecerá el nombre del sistemas operativo, en este caso es CentOS, en el cual se añadió el nombre a CentOS_Instalacion_OpenLDAP y nos pedirá que seleccionemos la ubicación en donde estará alojada la maquina virtual. A continuación damos clic en Next.



Pedirá que seleccionemos la capacidad máxima en disco duro, por defecto aparece 20 GB, que consideramos suficiente para nuestro entorno de pruebas.



En esta última pantalla aparecerá todos los datos o características de la maquina virtual, como se puede apreciar, por defecto da un número en memoria de lo que se puede utilizar, en este caso es de 1 GB, y se debe a que nuestra máquina cuenta con 4 GB de memoria RAM. Algo nuevo que también podemos observar es el tipo de red que nos proporciona, en este caso es NAT. Si deseamos cambiar la configuración de nuestra virtual, solo damos clic en Customize Hardware…

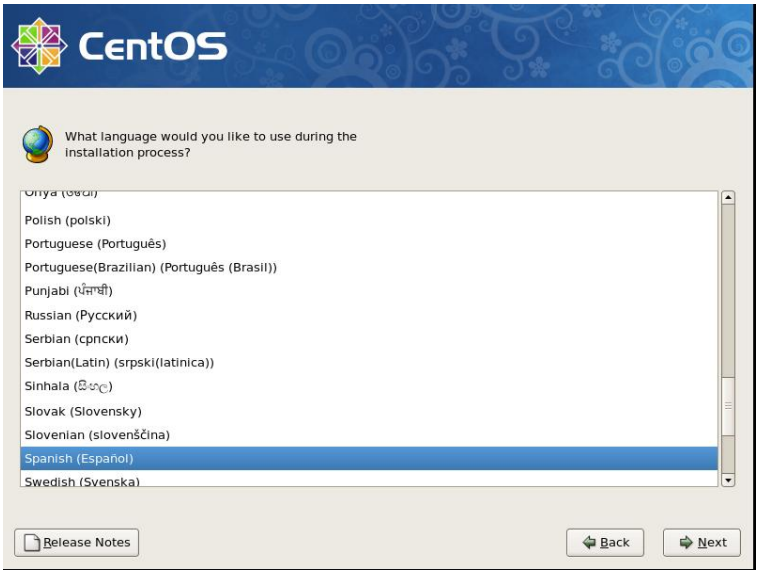


Empezamos con la instalación de CentOS5.6, y aparece la pantalla inicial de bienvenida, Damos Enter para continuar.

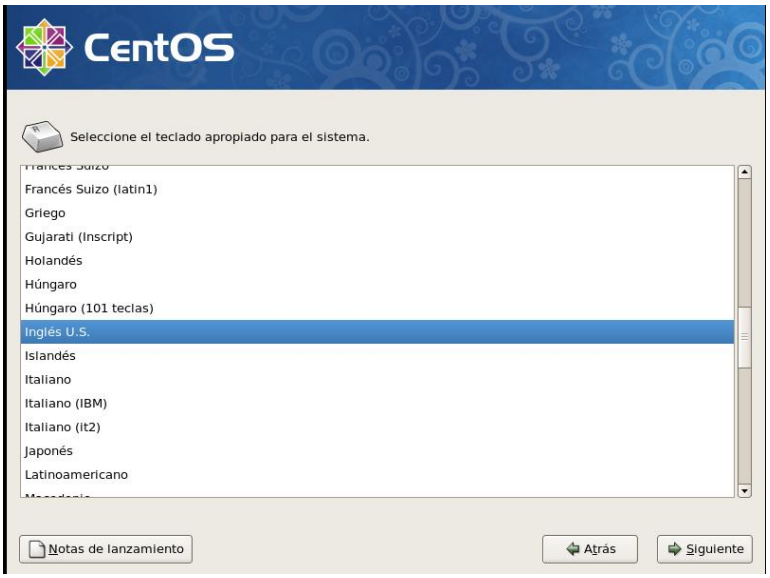
En esta pantalla damos clic en Skip, para omitir el paso de ejecutar una prueba del CD antes de la instalación.

A continuación muestra la interfaz gráfica para proceder con la instalación.

Elija el idioma que va a estar durante todo el proceso de instalación, en este caso seleccionamos español.

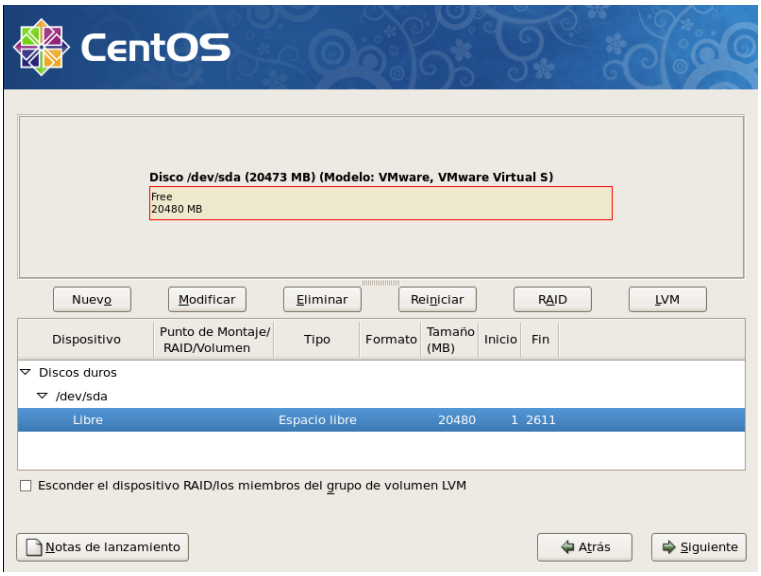


Se selecciona en qué idioma quiere configurar en el teclado, en este caso elegimos el inglés, ya que se ajusta mejor al momento de ejecutar líneas de código en una terminal de comando. Damos clic en Siguiente.



A continuación solicita si deseamos personalizar las particiones de nuestro disco. Entonces se elije Diseño personalizado y siguiente.

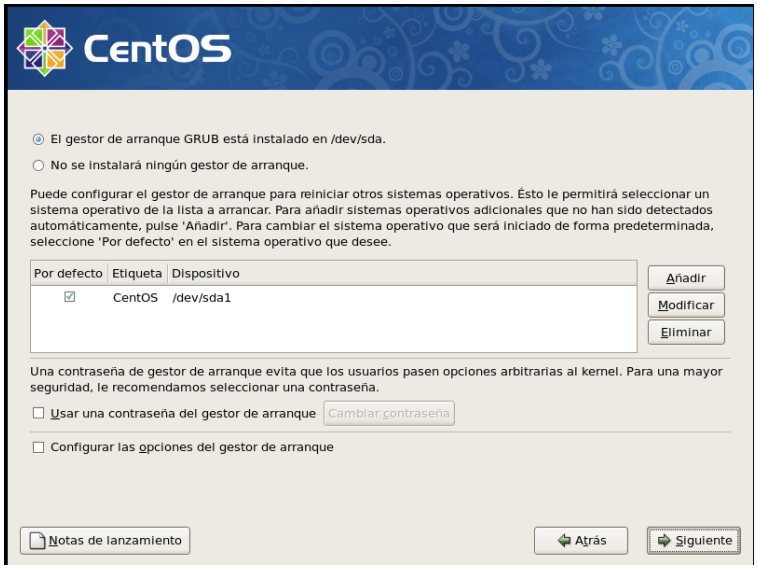
En esta pantalla muestra cómo crear nuestra tabla de particiones, y para esto en el espacio libre seleccionado, damos clic en Nuevo.



La primera partición que vamos a crear será la partición SWAP, que consiste en la utilización de un espacio de memoria virtual en caso de que la memoria RAM no sea suficiente. Le hemos dado un espacio de 4000 MB. Damos clic en Aceptar.

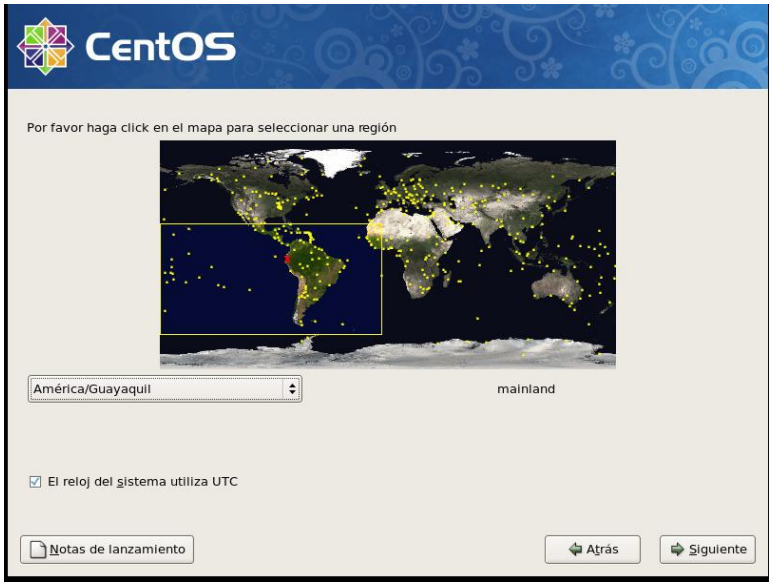
Una vez creada la partición SWAP, se prosigue con el resto de particiones, en este caso se creo una sola partición para todos los directorios, bajo la raíz /, y el sistema de archivos que utilizaremos es ext3. Hecho lo anterior se define el tamaño que del disco, en este caso se utiliza el máximo permitido.

En la siguiente pantalla muestra si desea instalar un gestor de arranque en el cual por defecto le dejamos en el GRUB, no se hace nada y de ahí siguiente.



Aquí en esta pantalla está ubicado la configuración de red y el nombre del host, esto es algo que permite avanzar en la configuración y si no lo deja para después.

En esta pantalla se define la región en la cual se encuentre ubicado, dejamos activado por defecto el reloj UTC. Damos clic en Siguiente.



Aquí nos pide que asignemos una contraseña para el súper usuario root, este es el usuario administrador que tendrá los permisos de hacer cualquier configuración en el sistema. Clic en Siguiente.

En esta pantalla nos muestra que tareas adicionales se puede aplicar para el sistema operativo, se elije personalizar y clic en Siguiente. Por defecto se puede mantener en Desktop – GENOME que es la interfaz gráfica en la cual se va a trabajar.

A continuación se selecciona que aplicaciones o servicios se necesita utilizar, en este caso puede marcar un Servidor DNS y un Servidor de Red por los paquetes que ofrece. Con esto se ha terminado de configurar la instalación.

Arranca con el formateo del sistema de archivos del disco y empieza la instalación de los paquetes.

Terminado el proceso de instalación solicita Reiniciar el sistema para efectuar los cambios.

Ahora aparece la pantalla de Bienvenida y se prosigue con los últimos pasos de la instalación.

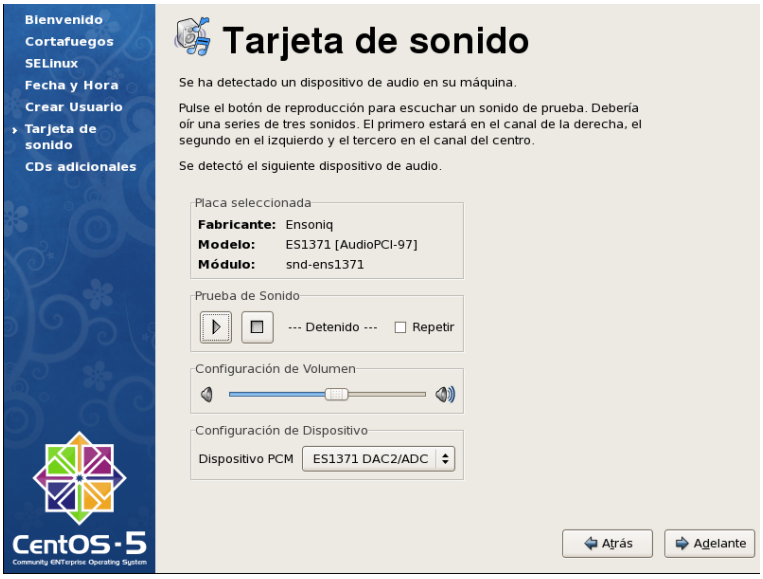
En esta pantalla se deshabilita la configuración de cortafuegos para que no hay conflicto en la implementación a futuro.

Se deshabilita la configuración de SELinux, que es una seguridad propia del sistema operativo CentOS lo que va a permitir total libertad para las posteriores configuraciones.

En esta pantalla muestra la configuración de Hora y Fecha del sistema, si no está acorde a la hora actual, puede realizar cambios.

En esta pantalla permite crear el primer usuario del sistema, aquí debe llenar todas las cajas de texto con lo que requiere, como muestra esta pantalla.

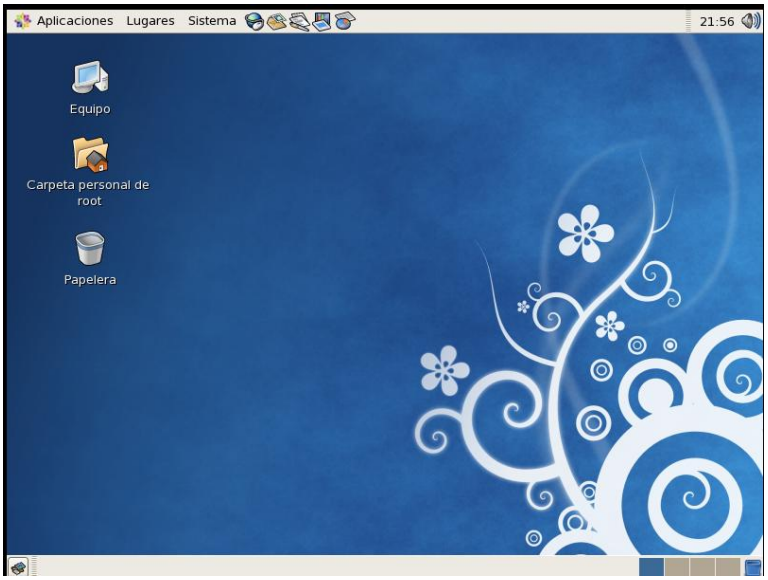
En esta pantalla indica que el sistema ha detectado un dispositivo de sonido, esto también podría configurar si en caso existiera otra tarjeta.



En el caso de que quisiéramos instalar algo adicionalmente, en esta pantalla da la opción de poder instalarlo. Luego de este último paso haga clic en finalizar, entonces el sistema pide ser reiniciado.

Terminada la instalación muestra en pantalla el inicio de sesión y con qué usuario usted desea ingresar. En este caso para poder realizar la implementación de LDAP inicie la sesión como súper usuario root.

Se ha iniciado sesión como súper usuario, y ya puede trabajar dentro del sistema operativo Linux CentOS5.6


Aplicaciones
Lugares
Sistema
21:56
Equipo
Carpeta personal de root
Papelera

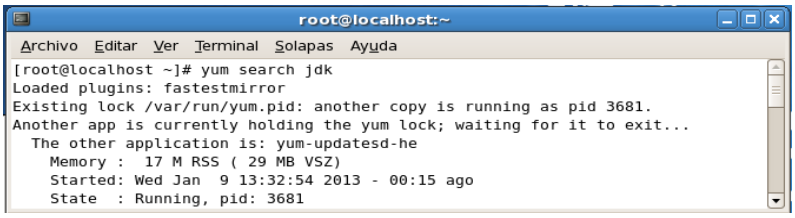
ANEXO2

INSTALACION Y CONFIGURACION DE OPENDS

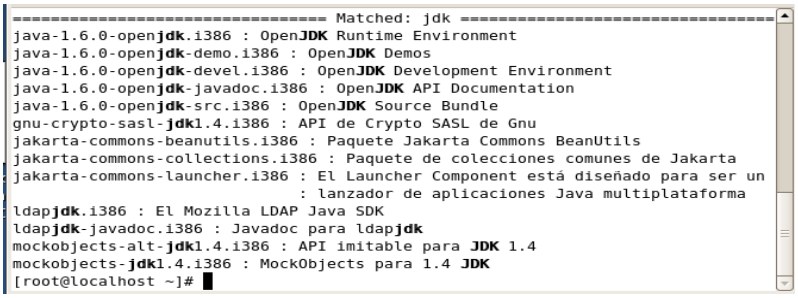
Para la instalación y configuración de OpenDS es necesario ingresar como súper usuario root, tanto para el administrador como para el cliente.

Instalación de las dependencias

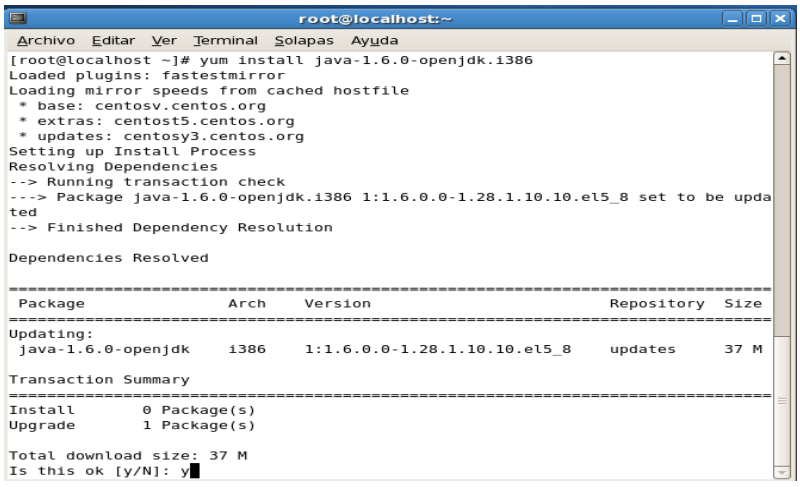
Primero se buscó el paquete de Java JDK que es necesario para la instalación de OpenDS, mediante el comando yum search como muestra la imagen.



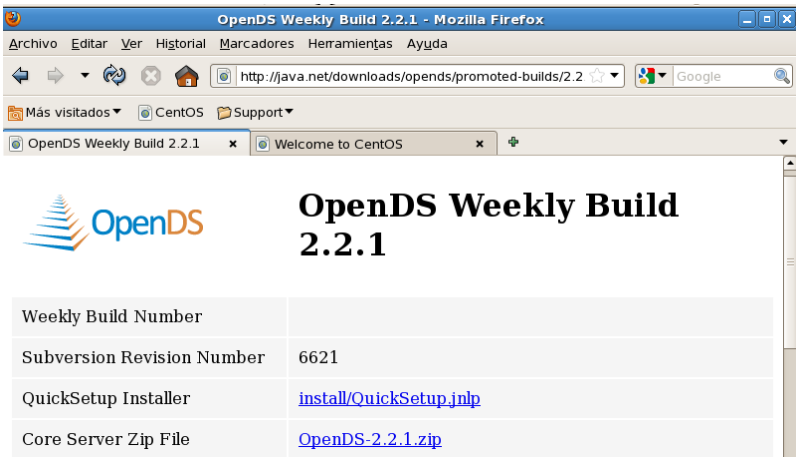
Una vez ejecutado el comando le muestra una lista de todos los paquetes disponibles y verifique que se encuentre la dependencia java-1.6.0-openjdk.i386



Luego de identificar el paquete JDK puede proceder a instalarlo con el comando yum install.



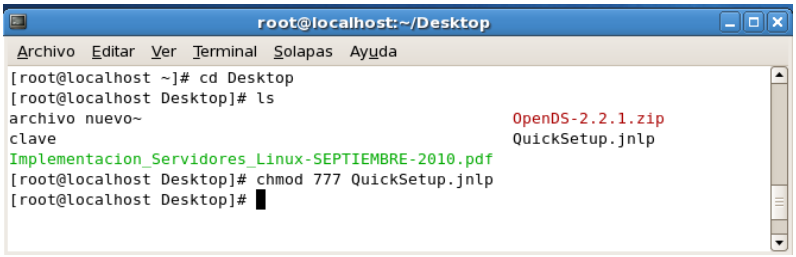
Cuando ya se haya completado la instalación salga de la terminal y ejecute el navegador de CentOS, que se encuentra en el menú ubicado en la parte superior y coloque la dirección http://java.net/downloads/opends/promoted-builds/2.2.1/



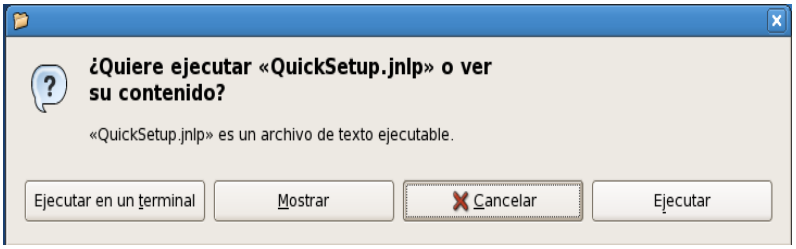
En la imagen anterior se podrá observar los dos paquetes el InstallQuickSetup.jnlp y el OpenDS-2.2.1.zip, y se procede a descargar los dos paquetes.

El primer paquete que se va a instalar es el QuickSetup.jnpl que es la herramienta gráfica que permitirá la ejecución de OpenDS.

Lo primero que tiene que hacer es buscar el archivo donde fue descargado para proceder a darle todos los permisos y permita su instalación.

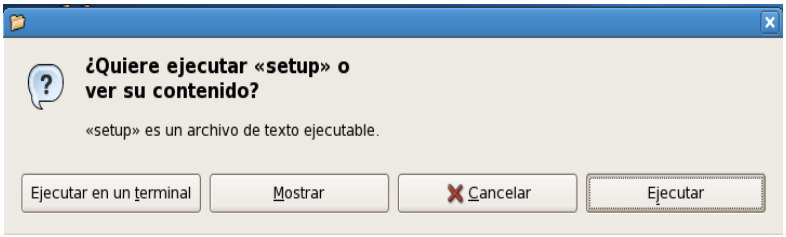


Al archivo QuickSetup.jnlp hágale doble clic y pulse el botón ejecutar.



Configuración del Servidor OpenDS

Luego de haber ejecutado la herramienta anterior, abra la carpeta descomprimida de OpenDS y ejecute setup como muestra la figura.

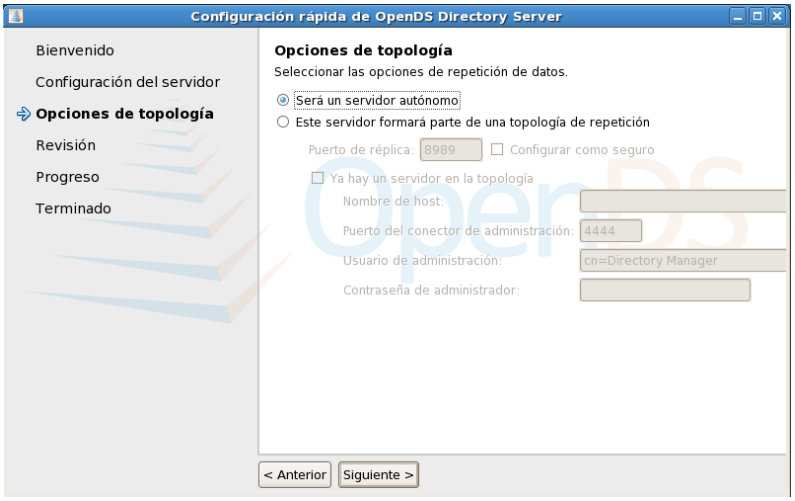


Cuando ya empieza a correr la instalación de OpenDS, se muestra la pantalla de bienvenida. Presione Siguiente.

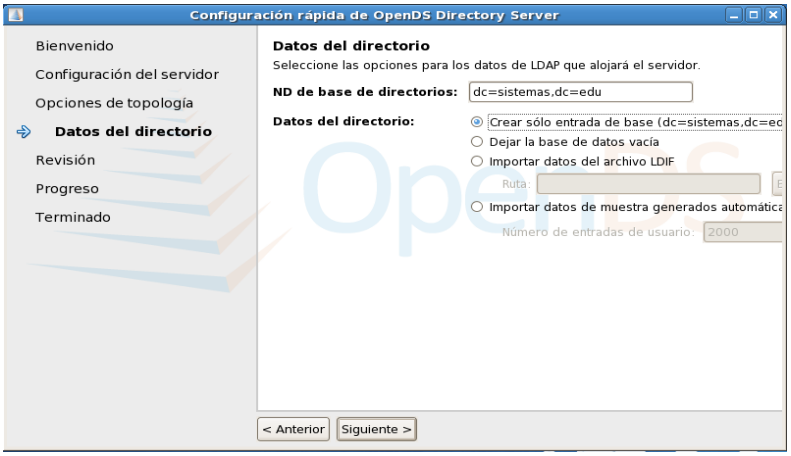
A continuación se procede a configurar el servidor. Aquí muestra el nombre del host, el puerto que por defecto escucha ldap es el 389, el puerto del administrador que es el 4444 y si desea puede configurar el acceso seguro a ldap con autenticación SSL o TLS, a demás nos muestra el nombre del usuario administrador por defecto, el cual

permite modificar, y por último se ingresa una contraseña para el acceso al servidor ldap. Damos clic en Siguiente.

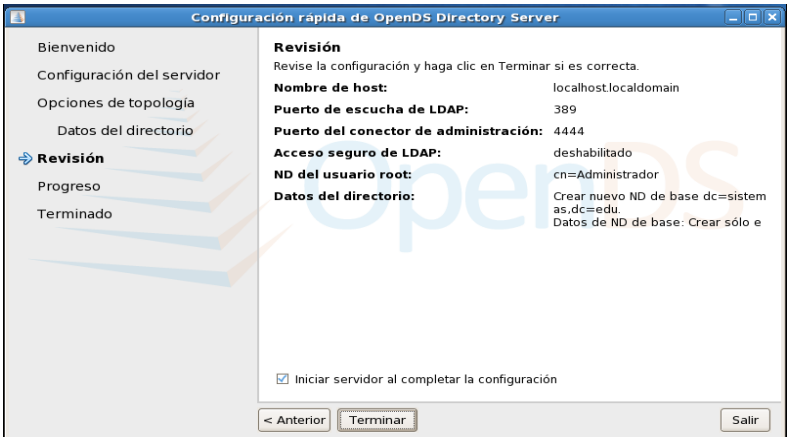
En esta pantalla se muestra las opciones de topología, puede ser autónomo o perteneciente a una topología de repetición. En este caso dejamos las opciones por defecto y damos clic en Siguiente.

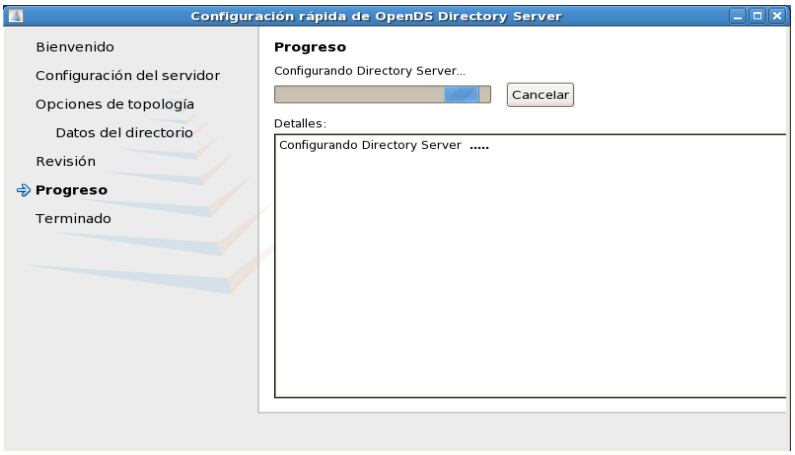


Ahora proceda a configurar los datos del directorio, como el nombre distintivo dc=sistemas, dc=edu y como desea que se generen los datos del directorio.



Terminado lo anterior se puede visualizar en la pantalla un resumen de toda la configuración que realizamos anteriormente. Si todo esta correcto damos clic en Terminar.

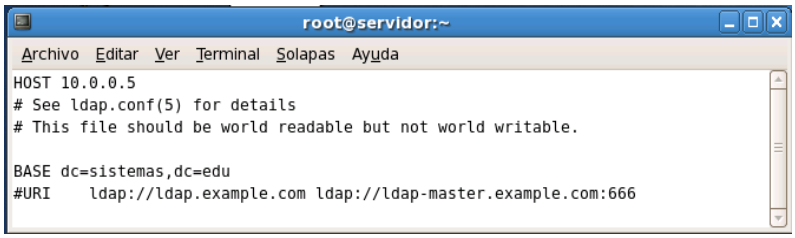




Ha finalizado correctamente la configuración de OpenDS, y nos indica la ubicación donde se puede ejecutar el servidor /root/Desktop/OpenDS-2.2.1/bin/control-panel.

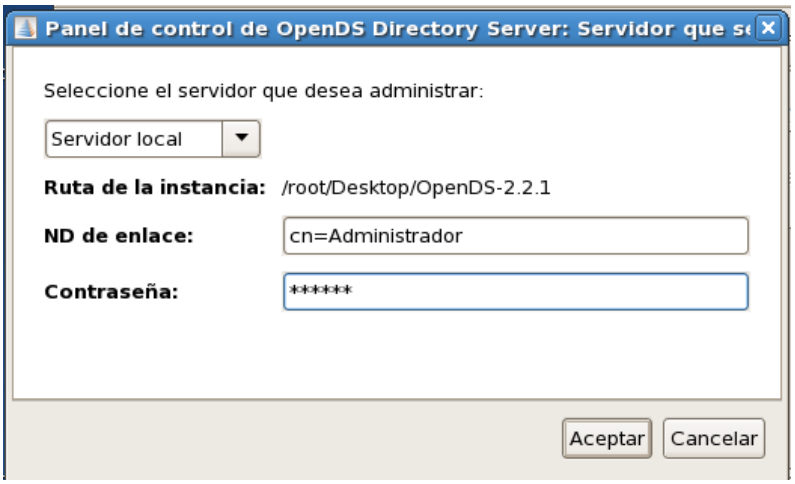
Es necesario instalar el paquete openldap-clients, que sirve para poder establecer la conexión local con el servidor.

Una vez instalado se procede a editar el archivo **/etc/openldap/ldap.conf** y estableca en el HOST la dirección IP del servidor y en BASE el dc=sistemas, dc=edu que definimos como dominio común del administrador.

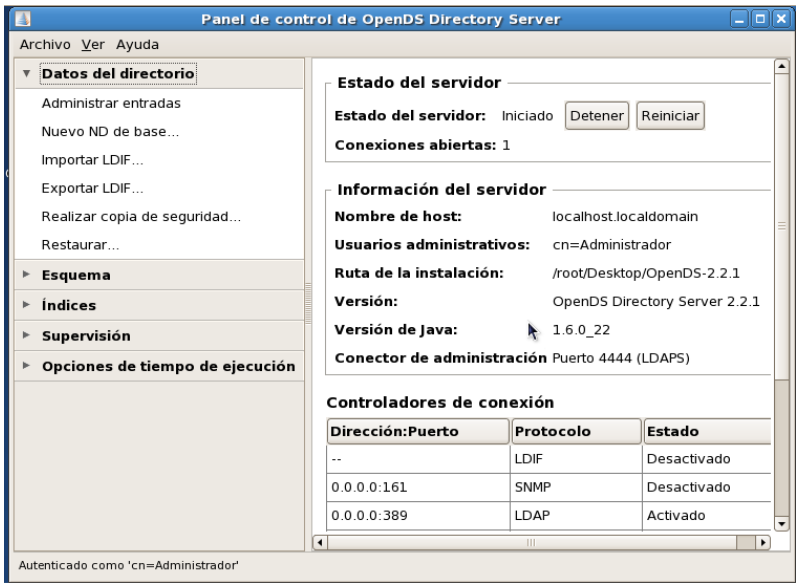


Administración del Servidor

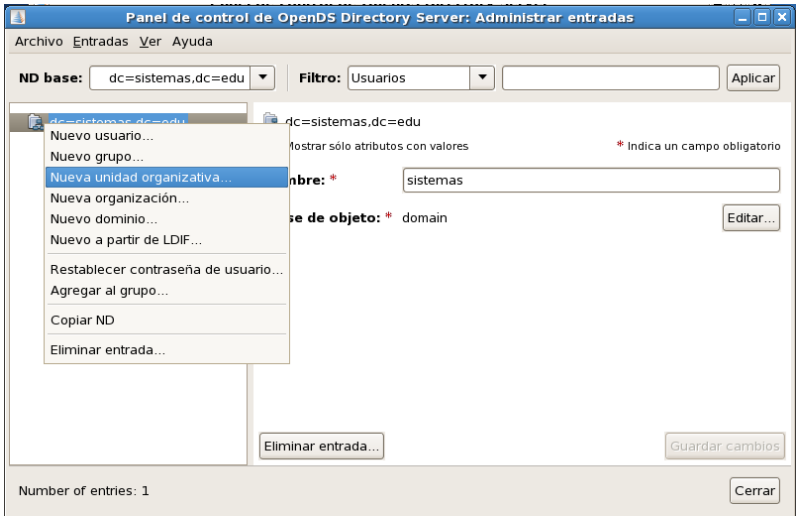
Primeramente inicie el servidor OpenDS con el nombre del administrador y contraseña configurado en la sección anterior.



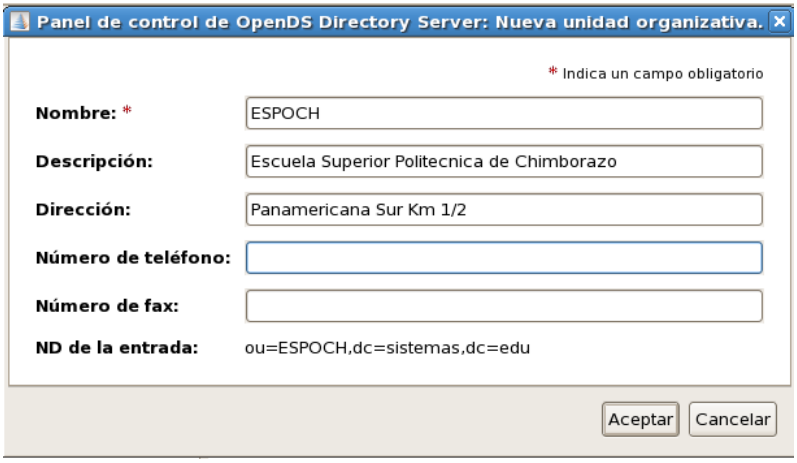
Este panel de control es la pantalla principal para la administración del servidor OpenDS, desde aquí debe empezar a crear los usuarios en la opción Administrar entradas.



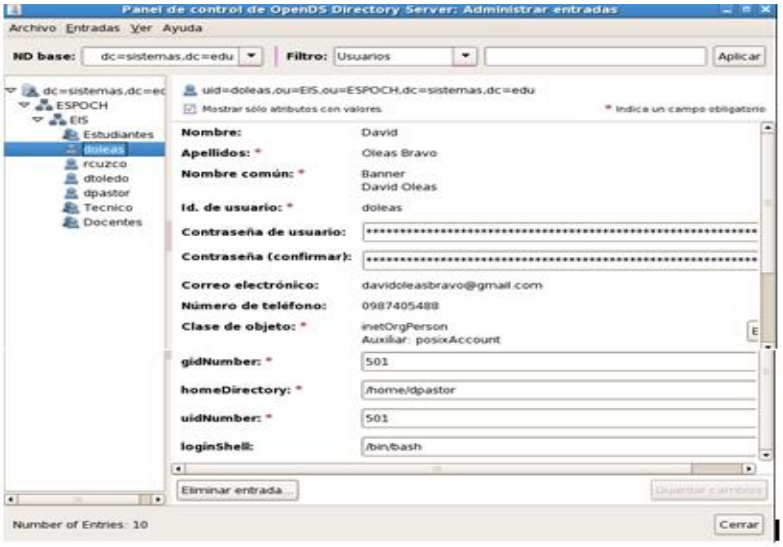
Para organizar mejor los datos, se crea unidades organizativas, en las cuales van a estar asociados grupo y usuarios de acuerdo a una estructura jerárquica que plantee. Se procede a dar clic derecho en ND dc=sistemas, dc=edu y se elige la opción Nueva unidad organizativa.



Llene los campos con la información requerida y clic en Aceptar.



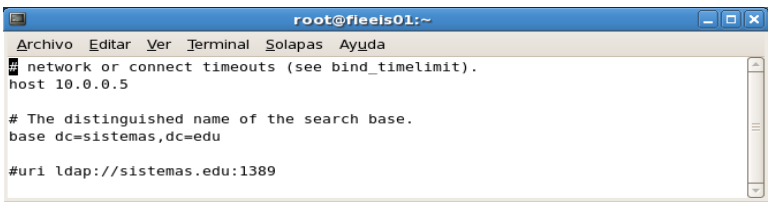
Una vez creado, Unidades organizativas, Grupos, Usuarios, la estructura queda de la siguiente manera. La figura muestra los detalles de un usuario ingresado donde hay que tomar en cuenta el campo del **Id. de usuario**, que se refiere al nombre del usuario creado en el sistema operativo ubicado en el directorio /home, al igual que los campos gidNumber y uidNumber, deben tener el mismo valor que el numero de usuario en el fichero /etc/passwd.



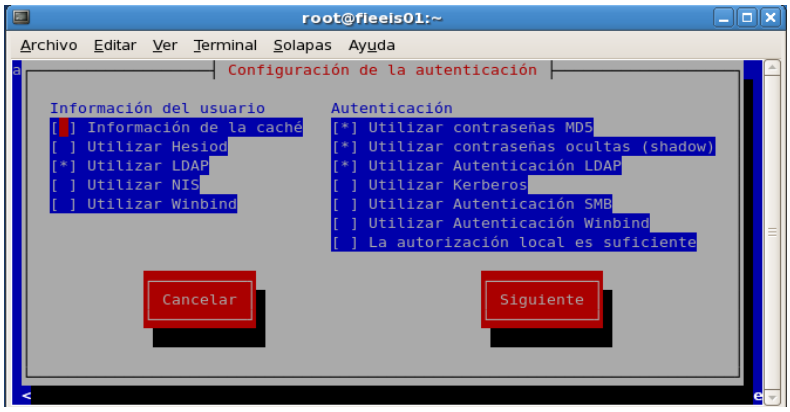
Por último en el campo Clase de objetos se añade el objeto auxiliar posixAccount, dando clic en el botón Editar, es necesario agregar este objeto porque las cuentas de usuario creadas son de este tipo.

Configuración del Cliente

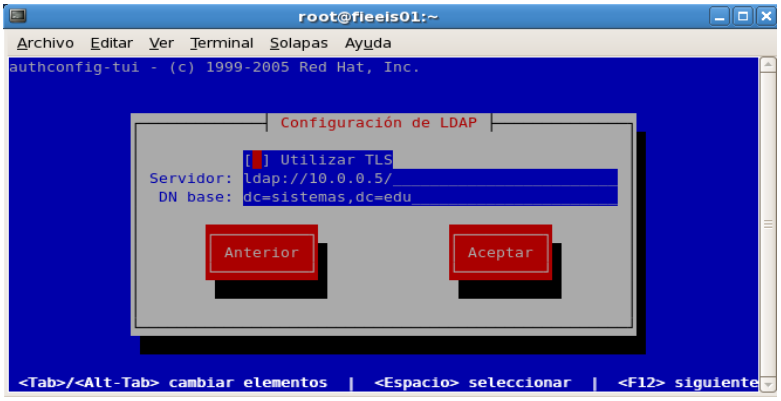
Edite el fichero ***/etc/ldap.conf*** y modifique el atributo **host** añadiendo la dirección IP del servidor y el nombre distintivo **base dc=sistemas, dc=edu** que es el dominio del servidor OpenDS que se asignó.



Ejecutando el comando **authconfig-tui** muestra la siguiente pantalla, cerciórese que este activado en la información del usuario **Utilizar LDAP** y en Autenticación el casillero **Utilizar Autenticación LDAP**



Una vez que damos siguiente en la pantalla anterior muestra lo siguiente, que por defecto ya debe estar ubicado la dirección del servidor y el nombre distintivo base.



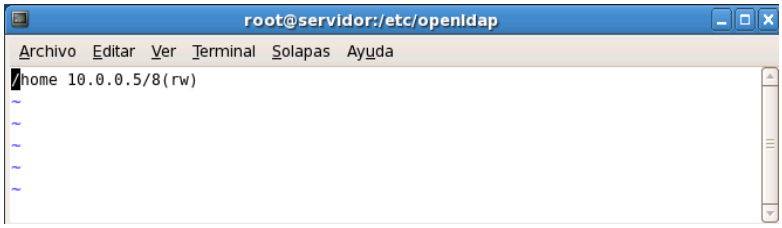
HOME REMOTO

Configuración de la Exportación del Home

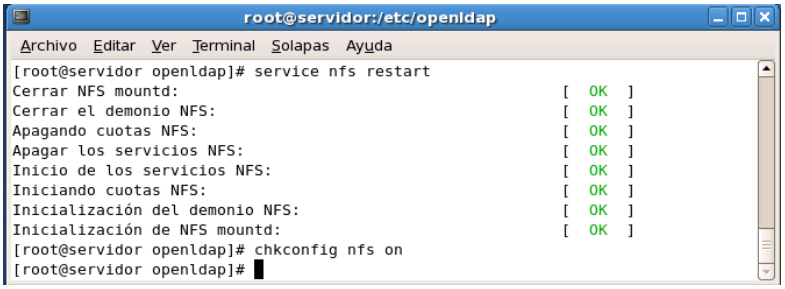
Este paso es muy necesario para poder replicar las cuentas de usuario que están creadas en el home, de lo contrario no tiene el cliente comunicación para poder hacer la autenticación.

Lo primero es editar el fichero /etc/exports.

Dentro del fichero se asigna la siguiente línea de código, que quiere decir que el home de usuario del la dirección 10.0.0.5/8 tiene permisos de lectura y escritura, y puede ser replicado por medio de nfs.

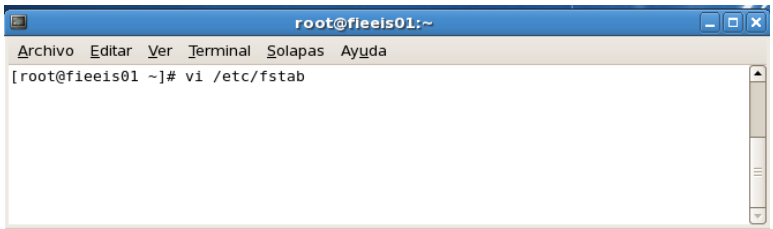


Se levanta el servicio de nfs, y luego con el siguiente mandato ejecutado permitirá que se ejecute automáticamente cada que inicie el servidor

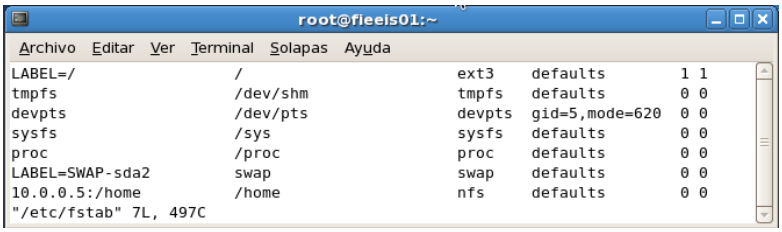


Configuración del Cliente para el montaje del Home remoto

Se tiene que asegurar de que el home es un punto de montaje válido, para ir a configurar el fichero **fstab**.



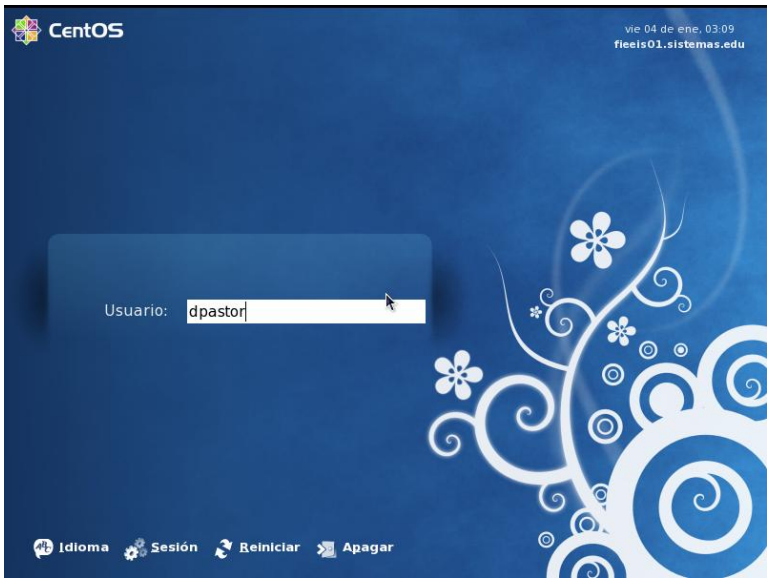
Una vez que entra al fichero, lo edita y al final agregue la siguiente línea donde hace referencia al punto de montaje en la dirección del servidor y con qué tipo de servicio va a poder llegar a él, en este caso es **nfs**.



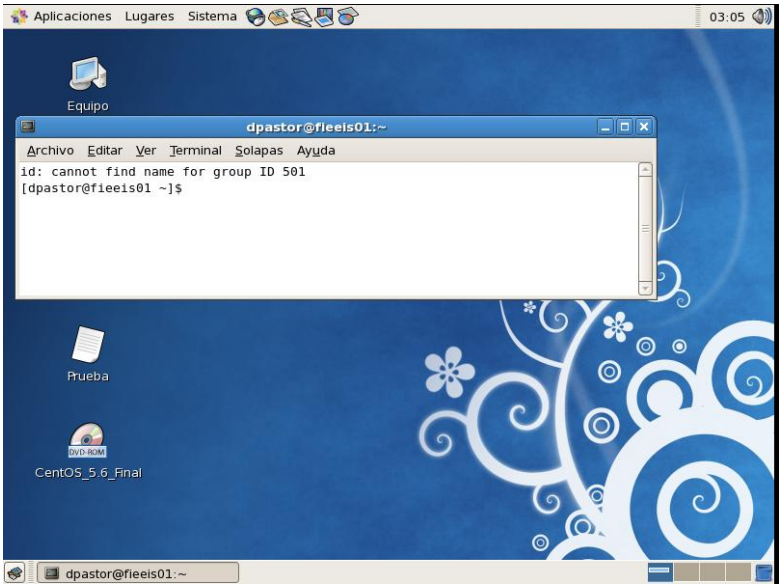
AUTENTICACION DEL CLIENTE AL SERVIDOR OPENDS

Prueba de Autenticación

Para realizar una prueba de autenticación debe seleccionar1 uno de los usuarios creados en el servidor y en el Panel de Control de OpenDS asignado anteriormente



Una vez autenticado el usuario se verifica el iniciamos sesión tan solo con abrir una terminal ya mostrará el usuario y el nombre del host.



Nota: Para autenticar usuarios Windows es necesario instalar y configurar Samba, como referencia se pueden vasar en la Implementación del Servidor OpenLDAP descrito en el capítulo 4, Configuración Samba.

ANEXO 3

MODULOS DE PRUEBA

Módulo 1: Instalación y Administración de las implementaciones del protocolo LDAP en OpenLDAP y OpenDS.

Módulo 1 Implementado sobre OpenLDAP

- **Tiempo de Instalación**

El tiempo de instalación es de 25m10.852

Transformación = (25*60)+10+(852/100) = 1510.852

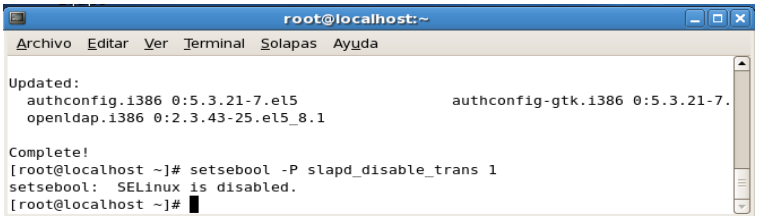
Total = 1510.852+779.557 = 2290.409

Porcentaje = (1510.852*100)/2290.409 = 65.96%

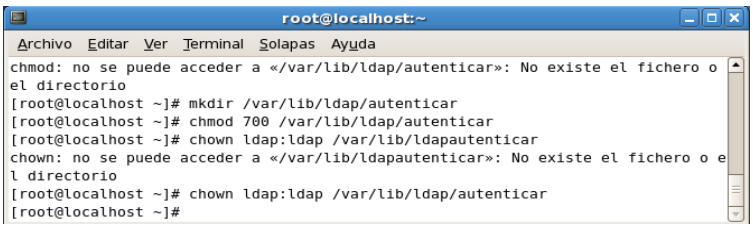
- **Grado de Complejidad de Configuración**

Números de Procesos de configuración OpenLDAP.

1. **Desactivar la Protección del Sistema**

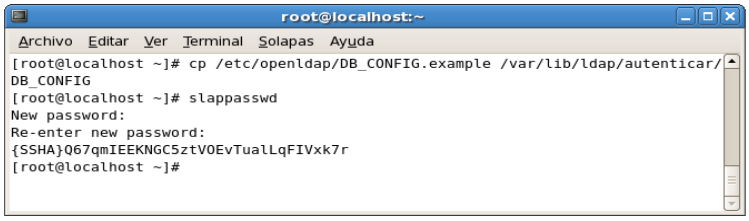


2. **Creación de Directorios**



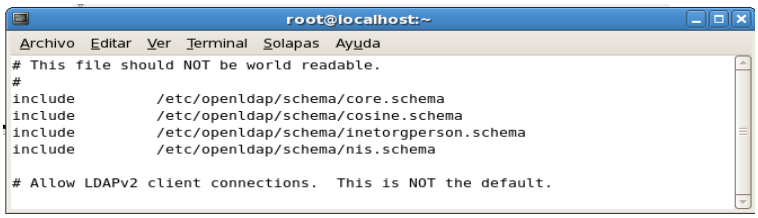
3. Copiar la Base de Datos en el Directorio Autenticar

4. Generación de la clave de acceso para LDAP

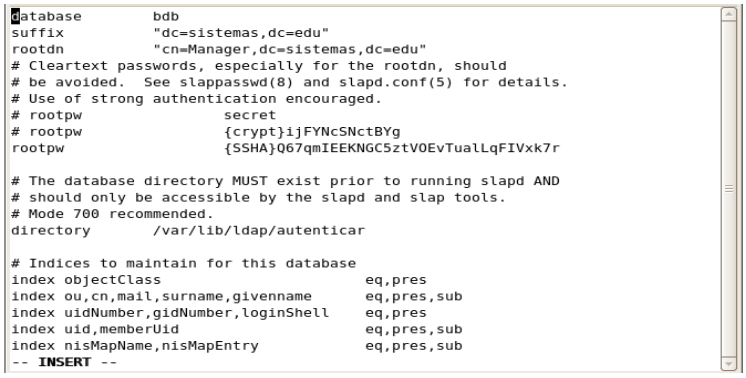


5. Editar el fichero de configuración de LDAP slapd.conf

6. Verificar los esquemas de configuración

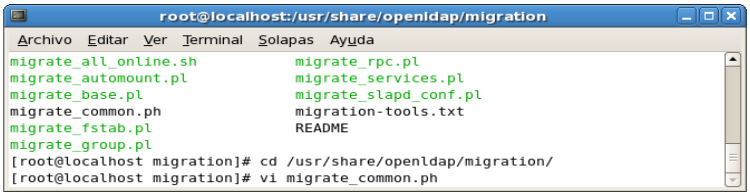


7. Modificar los valores en los campos

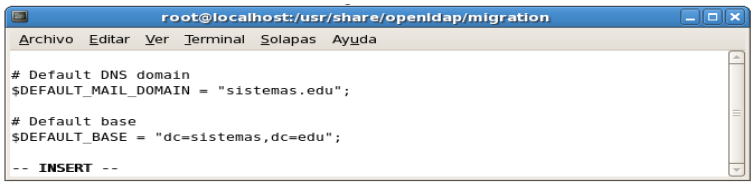


8. Levantamos el Servicio ldap

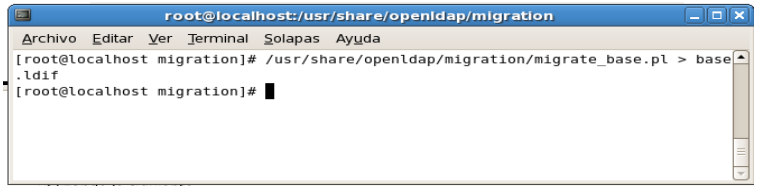
9. Migración de las cuentas existentes en el Sistema



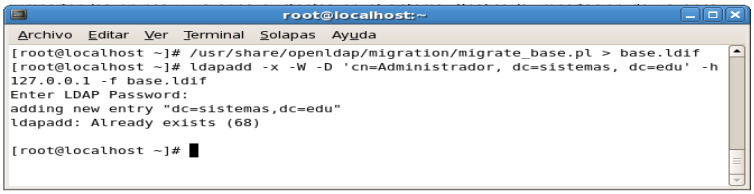
10. Editamos el archivo de la Migración



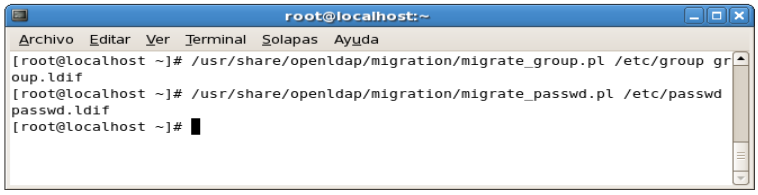
11. Direccionamos el fichero mígrate_base.pl > base.pl



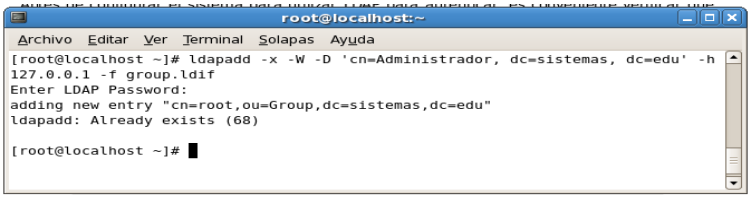
12. Añadimos las entradas al archivo base.ldif



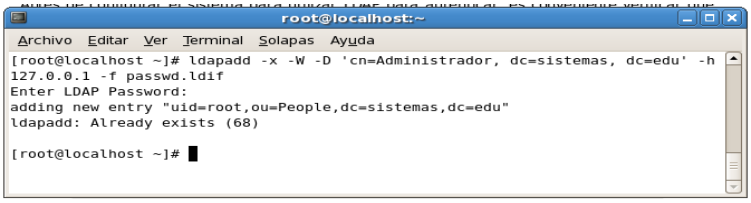
13. Creamos los ficheros para los usuarios



14. Migramos los grupos del sistema



15. Migramos todas las cuentas de usuario



Para poder medir este módulo se sumó el total de procesos de configuración obtenidos entre las dos implementaciones.

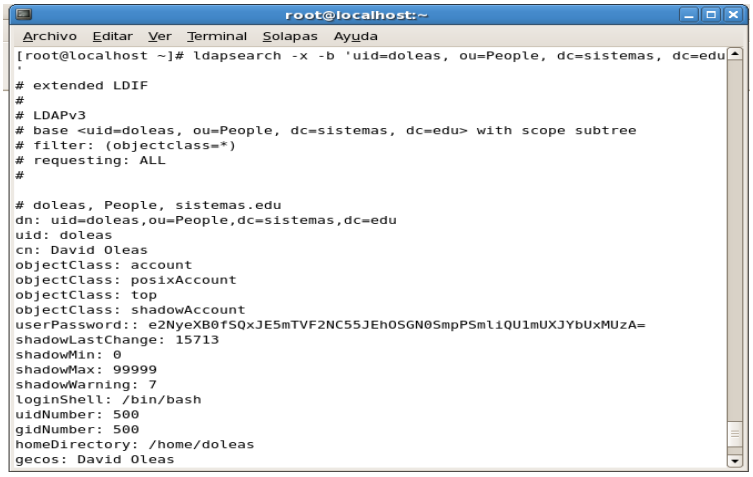
Número de procesos de OpenLDAP	**15**
Número de procesos de OpenDS	**6**
Total	**21**

Se aplica una regla de tres sobre el total de procesos obtenidos $\frac{15*100}{21} = \mathbf{71,42}\%$

- **Nivel de Control de Acceso**

No cuenta con Interfaz Administrativas

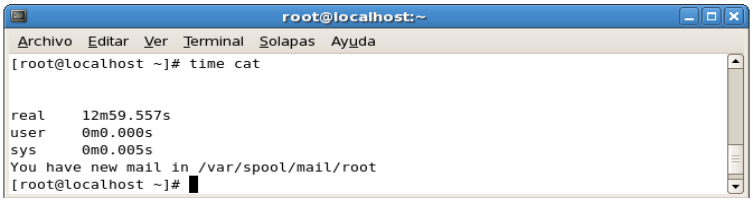
- **Grado de Factibilidad en la Administración**



Utilizando código para la administración, claramente se observa que los datos son medianamente difíciles de interpretar sabiendo que debe haber un nivel medio de conocimiento informático.

Módulo 1 implementado sobre OpenDS

- **Tiempo de Instalación**



El tiempo de instalación es de 12m59.557s ejecutando la instalación que abarca la configuración básica.

Transformación = (12*60)+59+(557/100) = 779.557

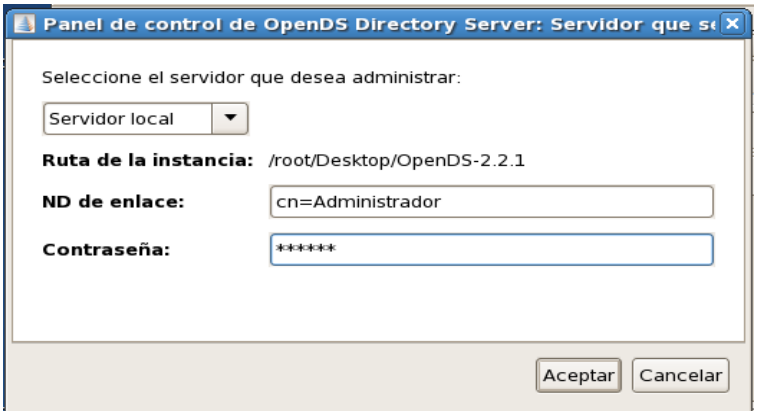
Total = 779.557+1510.852 = 2290.409

Porcentaje = (779.557 *100)/2290.409 = 34.04%

- **Grado de Complejidad de Configuración**

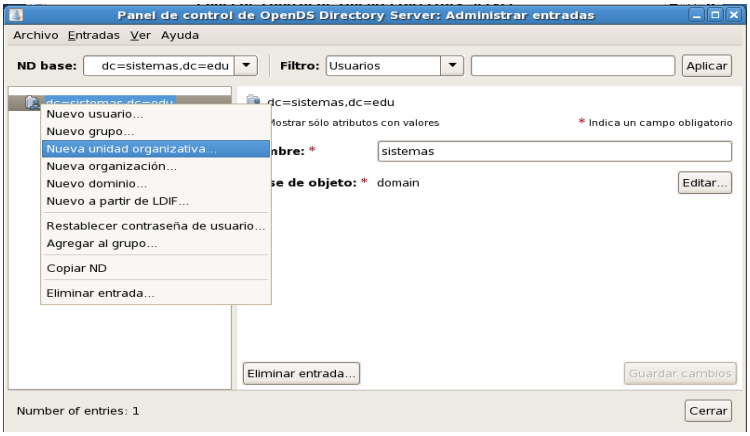
Número de Proceso de configuración OpenDS.

1. **Iniciamos el Servidor del Servidor**

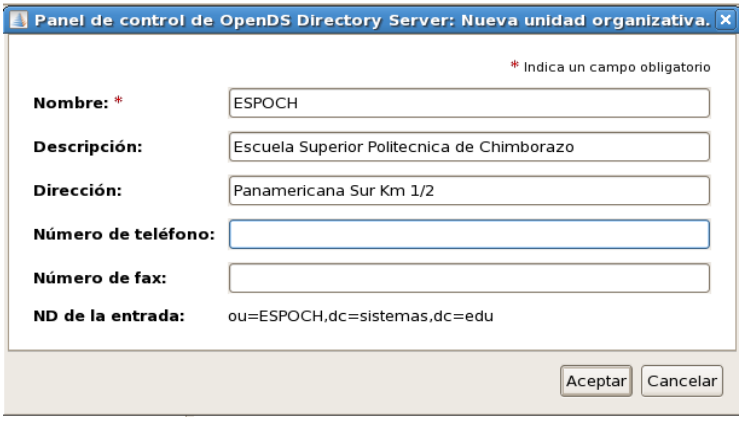


2. Presentación del Panel de Control

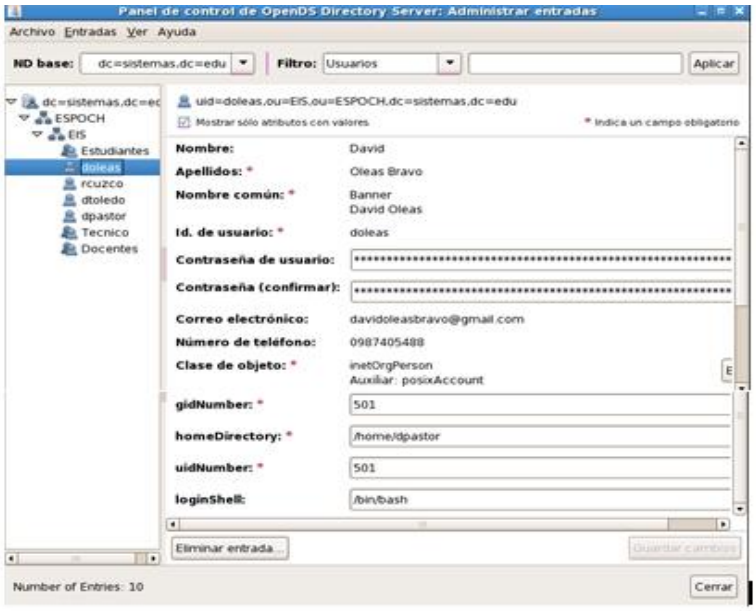
3. Nos ubicamos en el dominio base de OpenDS



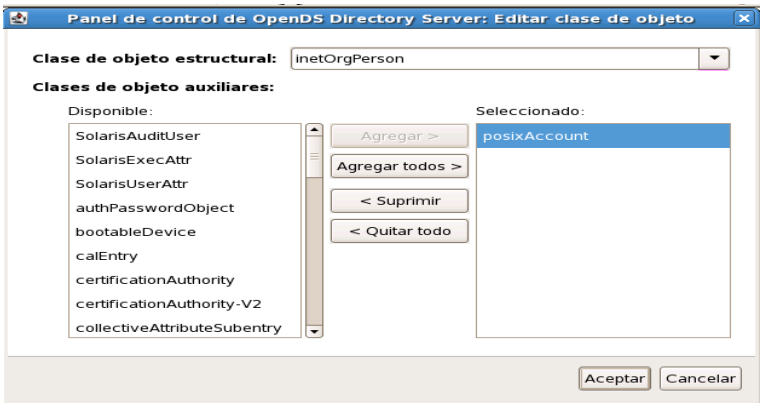
4. Llenamos los campos



5. Generado Grupos y Usuarios



6. Editamos las clases de objetos



Para poder medir este módulo se suma el total de procesos de configuración obtenidos entre las dos implementaciones.

Número de procesos de instalación de OpenLDAP **15**

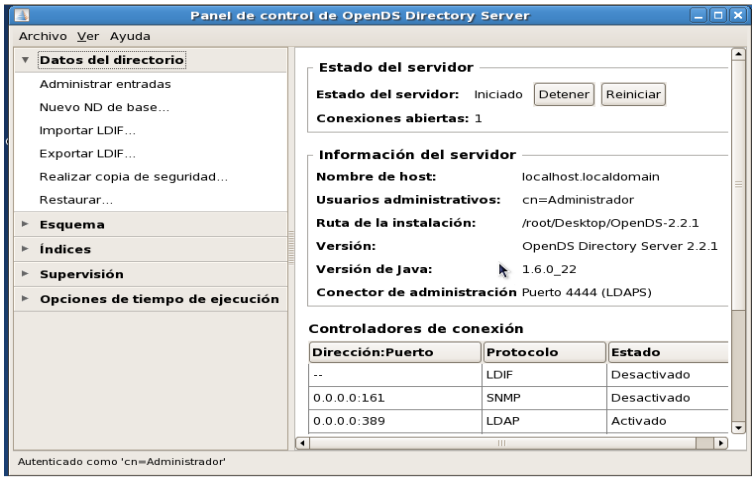
Número de procesos de instalación de OpenDS **6**

Total **21**

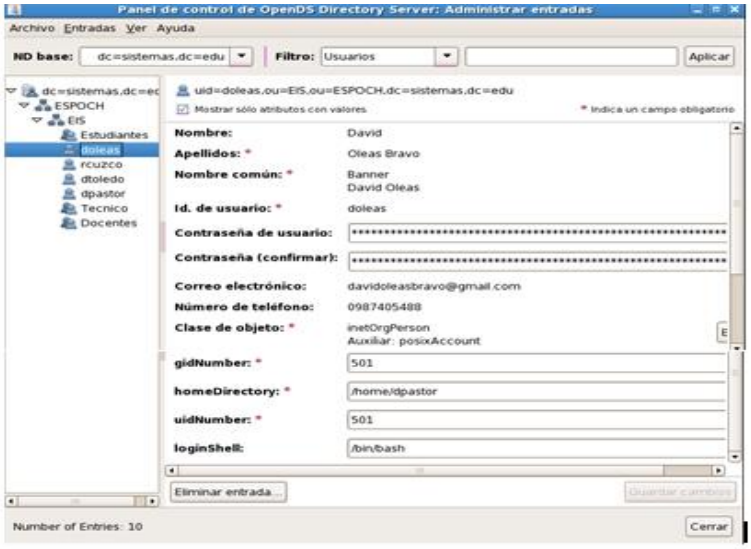
Se aplica una regla de tres sobre el total de procesos obtenidos $\frac{6*100}{21} = \mathbf{28,57}\%$

- **Nivel de Control de Acceso**

Si presenta Interfaz gráfica.



- **Grado de Factibilidad en la Administración**

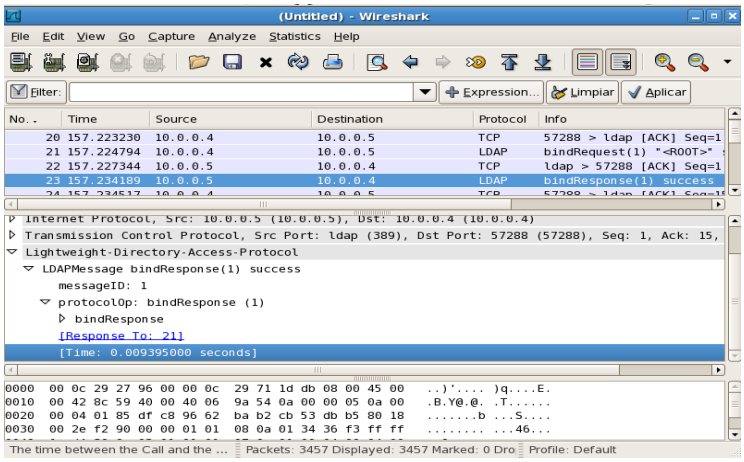


Por simple observación directa los datos son **fáciles** de interpretar por el entorno que muestra la interfaz administrativa. Tomando en cuenta que el administrador tiene conocimientos de nivel medio.

Módulo 2: Autenticación al establecer sesión, determinando los algoritmos de cifrado que soportan las implementaciones OpenLDAP y OpenDS.

Módulo 2 Implementado sobre OpenLDAP

- **Tiempo en establecer Sesión**



Latencia:

Retardo Nodo = 0.009395000

Tiempo Tx

Tamaño de la Trama = 80 bytes = 640bits

Velocidad Tx Tarjeta = 100Mbps = $100 * 10^6$

Tiempo Tx = $\frac{640*1seg}{100*10^6} = 0.0000064$

Tiempo de Propagación

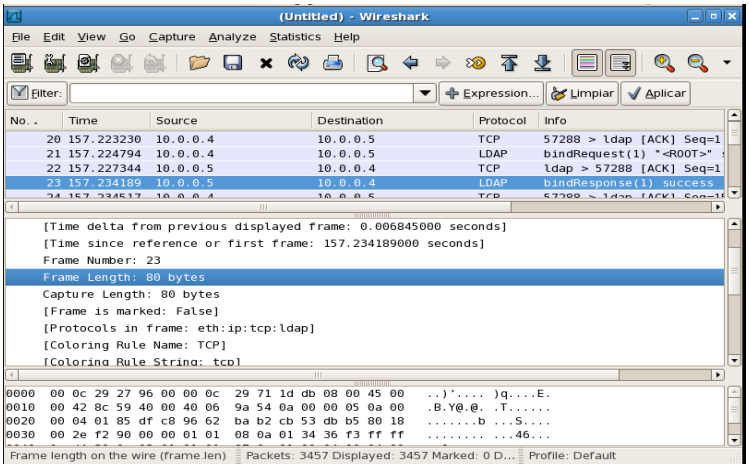
Velocidad de la luz = $3 * 10^8\ m/seg$ aplico ¾ de la velocidad = $225 * 10^6$ m/seg

Distancia del Equipo = 10 m

Tiempo de Propagación = $\frac{5}{225*10^6} = 0.000000044$

Tiempo en Establecer Sesión = Retardo de Nodo + Tiempo Tx + Tiempo de Propagación = 0.009395000 + 0.0000064 + 0.000000044 = 0.009401488

Cantidad de Paquetes de Entrada/Salida

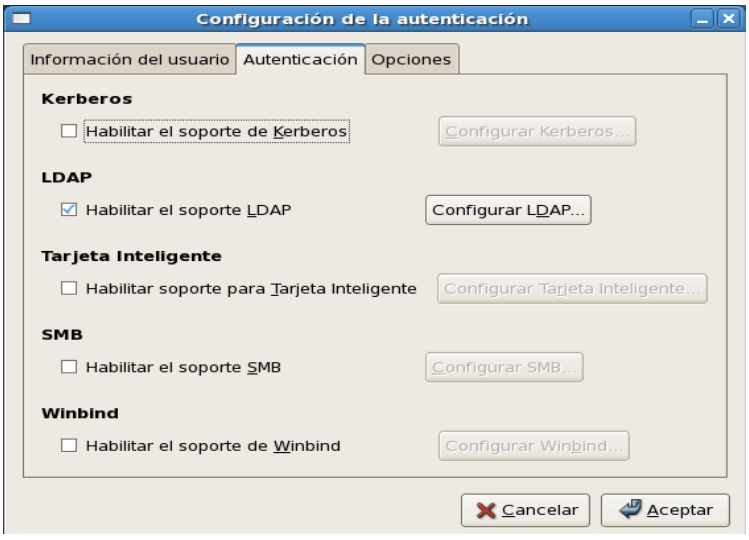


Para la resolución de este indicador se tomó el tamaño de las tramas como muestra la figura y se ha sumado las dos para darles un valor porcentual.

Total de Paquetes = 80bytes OpenLDAP + 80bytes OpenDS = 160 bytes

Cantidad de paquetes E/S = (80 bytes * 100)/160 bytes = 50%

- **Cantidad de Algoritmos de Cifrado**



Para medir el indicador de cantidad de algoritmos de cifrado, se ha tomado el total que ofrece sistema, que son 5.

Total de Algoritmos de cifrado entre OpenLDAP y OpenDS = 6

Cálculo Inverso = 6 – 5 = 1 Aplico es te método porque en este caso a mayor cantidad mejor autenticación.

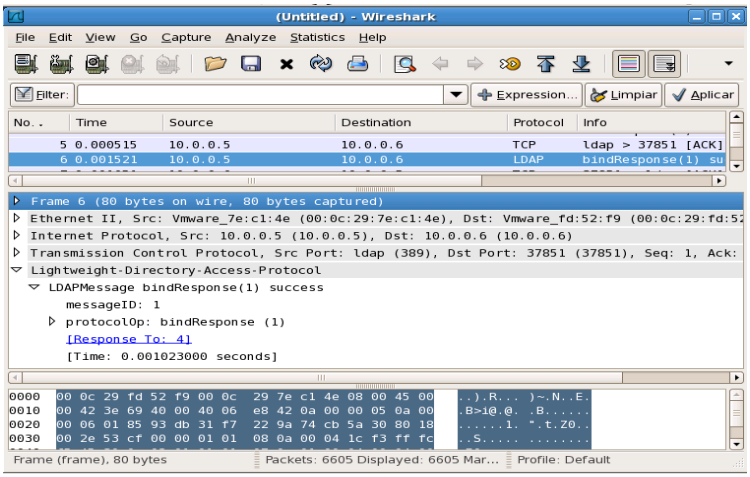
Cantidad de Algoritmos de Cifrado% = (5 * 100)/10 = 16.66% **Compatibilidad con**

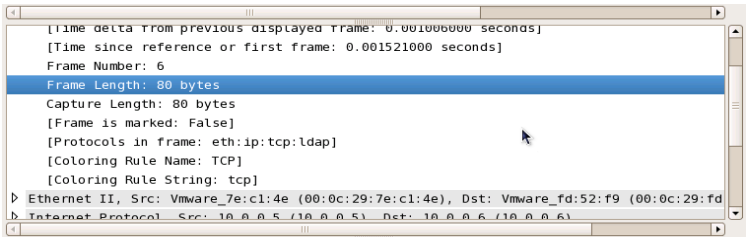
Compatibilidad con Métodos de Cifrado

Si aplica compatibilidad con otros métodos de cifrado NSS y PAM

Módulo 2 Implementado sobre OpenDS

- **Tiempo en establecer Sesión**





Latencia:

Retardo Nodo = 0.001023000

Tiempo Tx

Tamaño de la Trama = 80 bytes = 640bits

Velocidad Tx Tarjeta = 100Mbps = $100 * 10^6$

Tiempo Tx = $\frac{640*1seg}{100*10^6} = 0.0000064$

Tiempo de Propagación

Velocidad de la luz = $3 * 10^8\ m/seg$ aplico ¾ de la velocidad = $225 * 10^6$ m/seg

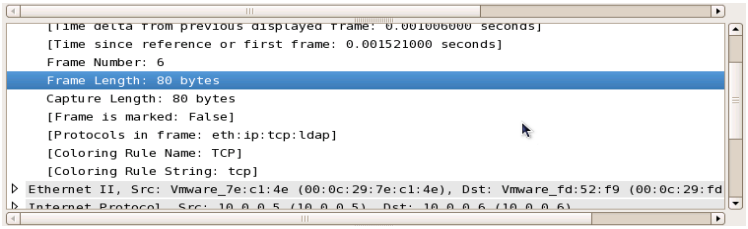
Distancia del Equipo = 10 m

Tiempo de Propagación = $\frac{5}{225*10^6} = 0.000000044$

Al final multiplico por 1000 para dar valores porcentuales

Tiempo en Establecer Sesión = Retardo de Nodo + Tiempo Tx + Tiempo de Propagación = 0.001023000 + 0.0000064 + 0.000000044 = 0.001029444

- **Cantidad de Paquetes de Entrada/Salida**



Para la resolución de este indicador se ha tomado el tamaño de las tramas como muestra la figura y se ha sumado las dos para darles un valor porcentual.

Total de Paquetes = 80bytes OpenLDAP + 80bytes OpenDS = 160 bytes

Cantidad de paquetes E/S = (80 bytes * 100)/160 bytes = 50%

- **Cantidad de Algoritmos de Cifrado**

Para medir el indicador de cantidad de algoritmos de cifrado, se ha tomado el objeto estructural que ofrece el panel de control de OpenDS que es solo 1.

Total de Algoritmos de cifrado entre OpenLDAP y OpenDS= 6

Cálculo Inverso = 6 - 1 Aplico es te método porque en este caso a mayor cantidad mejor autenticación.

Cantidad de Algoritmos de Cifrado = (5 * 100)/6 = 83.33%

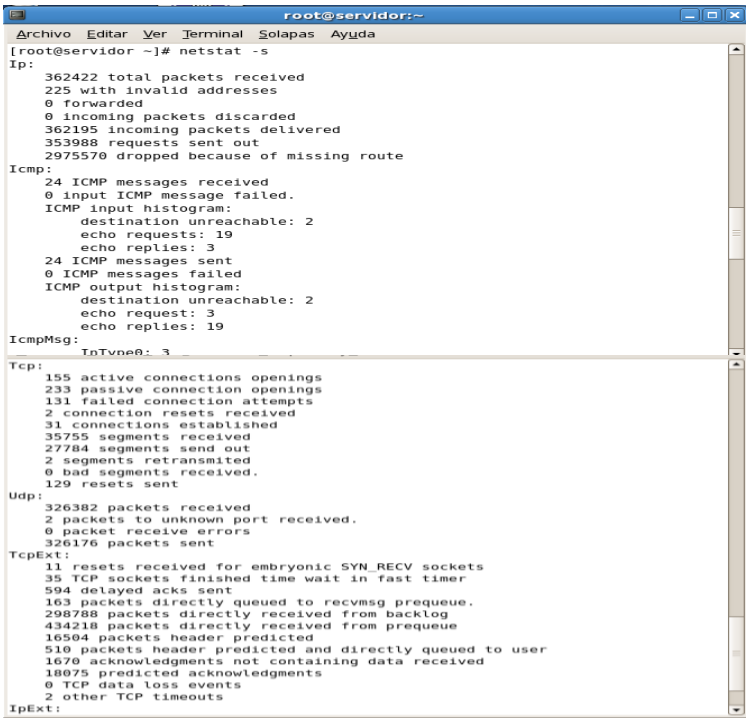
- **Compatibilidad con Métodos de Cifrado**

No aplica compatibilidad con otros métodos de cifrado

Módulo 3: Seguridad utilizada por las herramientas de administración de las implementaciones OpenLDAP y OpenDS.

Módulo 3 Implementado sobre OpenLDAP

- **Cantidad de Protocolos**

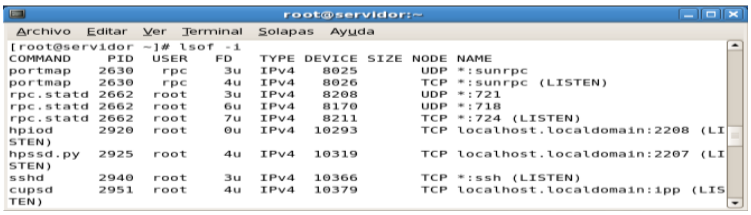


Aquí se pudo observar que la cantidad de protocolos es igual a 7 y que para poder medir este parámetro hay que sumar el total de protocolos de las 2 implementaciones.

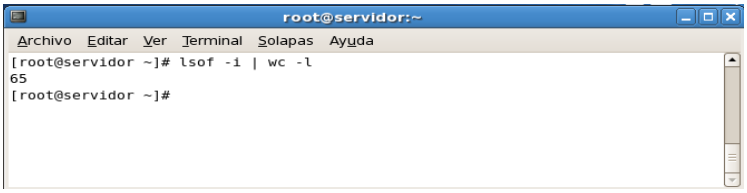
Total de Protocolos = 7 OpenLDAP + 7 OpenDS = 14

Cantidad de Protocolos = (7 * 100)/14 = 50%

- **Cantidad de Sockets**



Para obtener un número más preciso del número de sockets lo podemos hacer con la siguiente línea de comando.

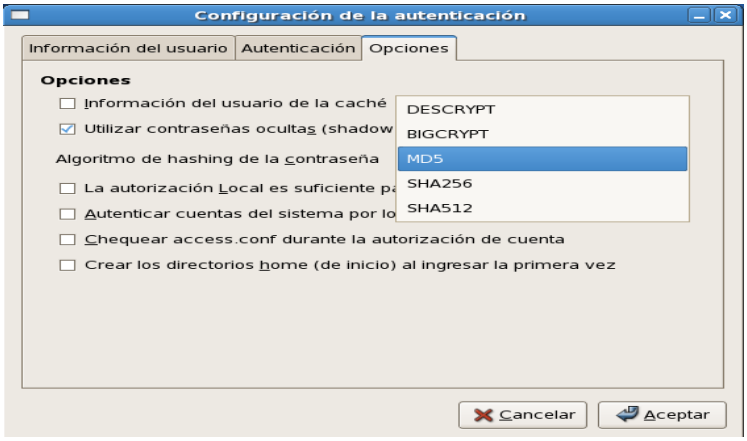


El número de sockets es de 65, para obtener un porcentaje de este indicador vamos a sumar el total de sockets de las dos implementaciones.

Total de Sockets = 65 Sockets OpenLDAP + 62 Sockets OpenDS = 127

Cantidad de Sockets = (65 * 100)/127 = 51.18%

- **Cantidad de Algoritmos Hashing**



El número de algoritmos Hashing es de 5, para obtener un porcentaje de este indicador vamos a sumar el total de sockets de las dos implementaciones.

Total de Sockets = 5 algoritmos OpenLDAP + 5 algoritmos OpenDS = 10

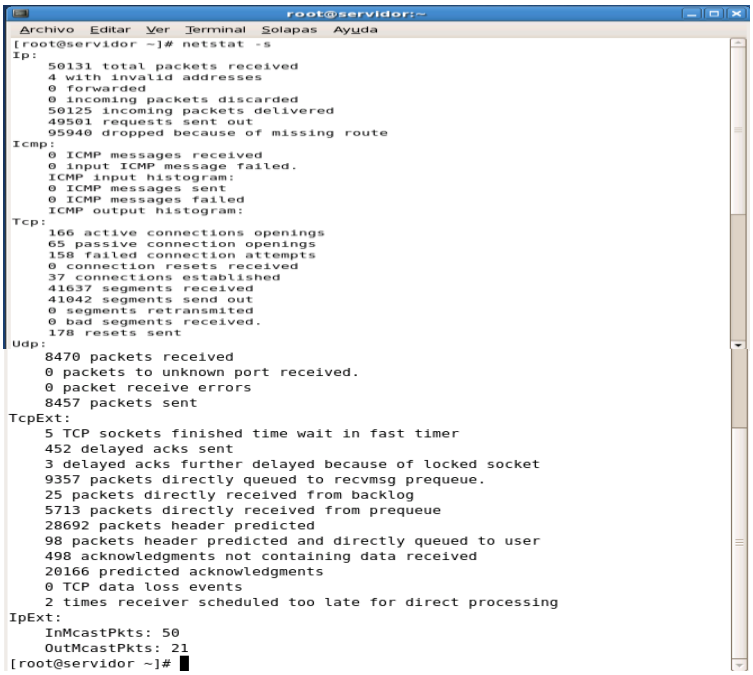
Cantidad de Sockets = (5 * 100)/10 = 50%

- **Soporte de Respaldo de Datos**

Si cuenta un proceso de Respaldo de la Base de Datos

Módulo 3 Implementado sobre OpenDS

- **Cantidad de Protocolos**

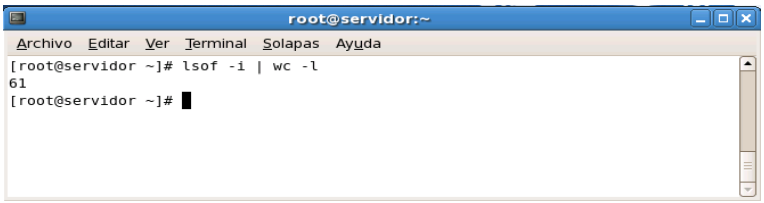


Aquí podemos observar que la cantidad de protocolos es igual a 7 y para poder medir este parámetro lo vamos hacer bajo el total de protocolos de las 2 implementaciones.

Total de Protocolos = 7 OpenLDAP + 7 OpenDS = 14

Cantidad de Protocolos = (7 * 100)/14 = 50%

- **Cantidad de Sockets**

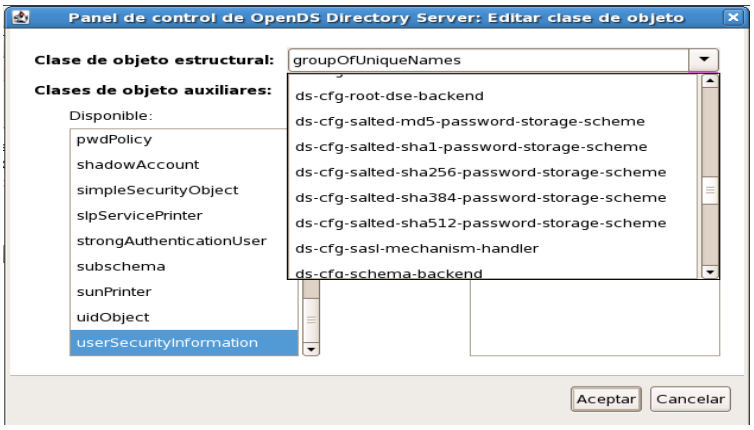


El número de sockets es de 61, para obtener un porcentaje de este indicador vamos a sumar el total de sockets de las dos implementaciones.

Total de Sockets = 65 Sockets OpenLDAP + 61 Sockets OpenDS = 126

Cantidad de Sockets = (61 * 100)/126 = 48.41%

- **Cantidad de Algoritmos Hashing**

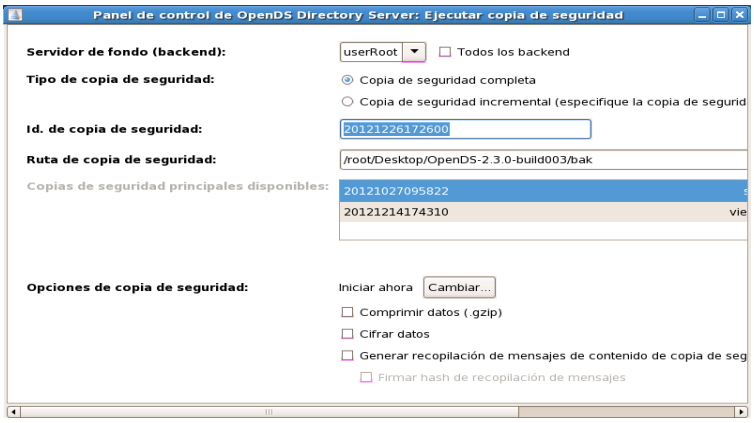


El número de algoritmos Hashing es de 5, para obtener un porcentaje de este indicador vamos a sumar el total de sockets de las dos implementaciones.

Total de Sockets = 5 algoritmos OpenLDAP + 5 algoritmos OpenDS = 10

Cantidad de Sockets = (5 * 100)/10 = 50%

- **Soporte de Respaldo de Datos**

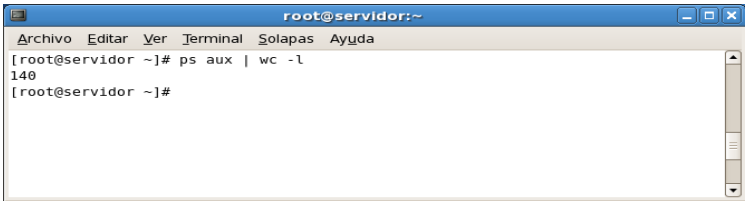


Si cuenta con un respaldo de la base de datos

Módulo 4: Consumo de recursos de las implementaciones del protocolo LDAP tanto en OpenLDAP como en OpenDS.

Módulo 4 Implementado sobre OpenLDAP

- **Consumo de Procesos**



Por coincidencia el consumo de procesos es igual a 140, y para medir este indicador se debe sumar el total de procesos como se establece a continuación:

Total de procesos = 140 OpenLDAP + 140 OpenDS

Consumo de Procesos% = (140*100)/283 = 49.47%

- **Cantidad de Memoria**

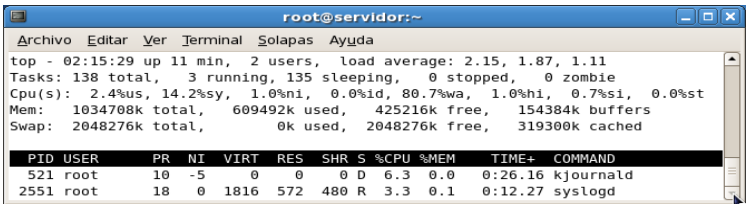
Le vamos a dar el valor porcentual de la memoria utilizada haciendo una regla de 3 con los siguientes valores mostrados anteriormente en la figura.

Memoria Total = 1034708

Memoria Usada = 606928

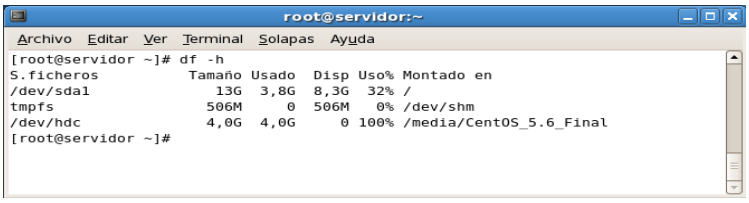
Cantidad de Memoria% = (606928*100)/1034708 = 58.65%

- **Nivel de Carga del CPU**



En el nivel de carga del CPU se mide directamente con el porcentaje que muestra en pantalla, su valor es del 14%

- **Utilización de Disco Duro**



La utilización de disco duro de nuestro servidor es del 32%

Módulo 4 Implementado sobre OpenDS

- **Consumo de Procesos**

El consumo de procesos es igual a 143, y lógicamente es debido a que no se está ejecutando nada más que la implementación OpenDS

Total de procesos = 140 OpenLDAP + 143 OpenDS = 283

Consumo de Procesos% = (143*100)/283 = 50,53%

- **Cantidad de Memoria**

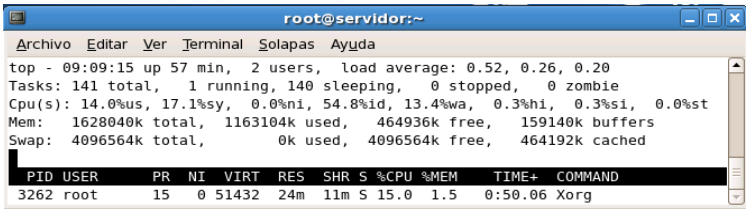
Se da el valor porcentual de la memoria utilizada haciendo una regla de 3 con los siguientes valores mostrados anteriormente en la figura.

Memoria Total = 1628040

Memoria Usada = 1112636

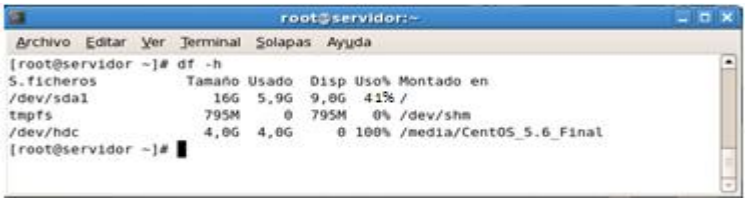
Cantidad de Memoria% = (1112636*100)/1628040 = 68.34%

- **Nivel de Carga del CPU**



En el nivel de carga del CPU se mide directamente con el porcentaje que muestra en pantalla, su valor es del 17%

- **Utilización de Disco Duro**



La utilización de disco duro de nuestro servidor tiene un porcentaje directo del 41%

ANEXO 4

Encuesta de Tesis

Pregunta:

¿Cuáles son las Implementaciones LDAP que conoces o has utilizado?

Vota con + en el comentario publicado que consideres apropiado.

Resultados		**Porcentajes**
OpenLDAP	7	43.75%
OpenDS	6	37.50%
ApacheDS	2	12.50%
FedoraDS	1	6.25%

Los siguiente resultados muestran que las implementaciones más populares son OpenLDAP y OpenDS