

**Implementación de un Servidor Samba con autenticación LDAP como alternativa Libre a los Servidores de Dominio Windows.**

**ING. Lázaro J. Ramos Alfonso**

lramos.ssp@infomed.sld.cu

**MSc Miriel Martín Mesa**

miriel@uclv.edu.cu

# Índice

ÍNDICE .....	ii
INTRODUCCIÓN .....	1
Capítulo 1. Introducción a los servidores de dominio .....	3
1.1. Windows NT .....	3
1.1.1. Windows NT 3.1 .....	3
1.1.2. Windows NT 4.0 .....	4
1.1.3. Windows Server 2000 .....	4
1.1.4. Windows Server 2003 .....	5
1.1.5. Windows Server 2008 .....	7
1.2. Directorio Activo (Active Directory o AD) .....	8
1.2.1. Funcionamiento .....	9
1.2.2. Requisitos de instalación .....	9
1.2.3. Direccionamiento a los recursos de Active Directory .....	10
1.2.4. Diferencias entre Active Directory y Windows NT .....	10
1.2.5. Alternativas a Active Directory .....	10
1.3. Elección del software .....	11
Capítulo 2. Samba + Ldap como Controlador de dominio primario(PDC) .....	13
2.1. Samba .....	13
2.1.1. Conceptos teóricos .....	13
2.1.2. Visión general de Samba .....	13
2.1.3. ¿Qué novedades ofrece el Samba 3? .....	15
2.1.4. Samba 4 .....	16
2.1.5. Configuración de Samba .....	16
2.1.6. Instalación .....	18
2.2. OpenLDAP .....	18
2.2.1. Conceptos Teóricos .....	18
2.2.2. ¿Qué tipo de información se puede almacenar en un directorio? .....	18
2.2.3. ¿Cómo se almacena la información? .....	18
2.2.4. ¿Cómo se accede a la información? .....	19
2.2.5. ¿Cómo se protege la información de los accesos no autorizados? .....	19
2.2.6. Esquemas (Schemas) .....	19
2.2.7. ¿Cómo trabaja LDAP? .....	20
2.2.8. LDAP versión 3 .....	20
2.2.9. ¿Qué es slapd? .....	20
2.2.10. ¿Qué es Slurpd? .....	21
2.2.11. Configuración .....	21
2.2.12. Instalación .....	21
2.3. PHPLDAPADMIN .....	21
2.3.1. Conceptos teóricos .....	21
2.3.2. Instalación .....	21
2.4. Account-Manager (LAM) .....	22
2.4.1. Conceptos teóricos .....	22
Capítulo 3. Guía de implementación de un Servidor Samba + LDAP como Controlador de Dominio Principal en Debian GNU/Linux versión 5 o Debian Lenny .....	23
3.1. Nota introductoria .....	23
3.2. Instalando los paquetes que se van a utilizar .....	23
3.3. Configurando SLAPD .....	23
3.4. Preparando el esquema de LDAP para samba .....	23
3.5. Instalación de phpLDAPadmin y LDAP-Account-Manager .....	24
3.6. Preparando Samba .....	24
3.7. Configurando smbldap-tools .....	24

<i>3.8. Replicar el esquema de LDAP para Samba:</i> .....	25
<i>3.9. Configurar PAM/NSS con LDAP</i> .....	25
<i>3.10. Nota adicional</i> .....	27
<i>Conclusiones</i> .....	28
<i>Referencias Bibliográficas</i> .....	29

## INTRODUCCIÓN

Las redes de computadoras son hoy parte indispensable de las instituciones que cuentan con un número considerable de ordenadores en operación, frecuentemente alejadas entre sí, con los objetivos de compartir recursos (Información, Aplicaciones, Periférico), proveer de confiabilidad y de lograr comunicación entre las distintas estaciones de trabajo. El trabajo en red ofrece numerosas ventajas como son: la reducción de costos al compartir información y periféricos, la adquisición de datos oportunamente, mejoría para la organización y la comunicación de las empresas, mantener bases de datos actualizadas instantáneamente y accesibles desde distintos puntos, facilitar la copia de respaldo de los datos, etc.

En las redes institucionales, en muchas ocasiones, es de interés contar con un directorio centralizado de cuentas de usuarios y contraseñas con el objetivo, primero, de que cada usuario pueda abrir sesión en las distintas computadoras del dominio sin necesidad de crear las cuentas localmente en cada una de ellas, tener mejor control de los usuarios que se van agregando y desagregando a la red, así como un mejor control sobre los recursos a los que se va a acceder.

La incorporación del Directorio Activo de Microsoft, como solución comercial del servidor de Directorio es hoy muy difundido en las organizaciones, sobre todo porque proporciona herramientas gráficas de administración y configuración del directorio muy fáciles de utilizar; pretendiendo aislar al administrador de la red, de los conocimientos avanzados acerca de los protocolos y estándares que implementa.

En el caso de nuestro país debido al embargo, desde el punto de vista económico, opciones como las de usar un servidor de Windows NT, Windows 2000 Advanced Server, Windows 2003 Advanced Server, u otro servidor de Microsoft Windows, como Controlador Primario de Dominio (Primary Domain Controller o PDC) quedan descartadas. Por esta razón la implementación de estos servicios con servidores amparados por las licencias de libres distribución no solamente ofrece una solución a este problema, sino que además son herramientas altamente configurables que garantizan la personalización, mantenimiento y las copias de respaldo de las bases de usuarios.

Este trabajo presenta un método de integración de una red heterogénea con múltiples clientes, y donde cada uno de ellos pueda tener sistemas operativos diferentes, sobre los cuales pueden operar una infinidad de usuarios contra una base de datos común, utilizando un directorio LDAP para almacenar la información relativa a los usuarios.

Para la solución de este problema surgen las siguientes interrogantes:

- ¿Cuáles son los principales servidores de dominio que son auspiciados por licencias de libre distribución?
- ¿Cuál de los servidores de dominio, de software libre, es el más indicado para una alternativa libre a una solución de una red empresarial?
- ¿Cuál sería la propuesta de configuraciones a implementar?

Para dar respuestas a esas interrogantes el objetivo general de este trabajo es disponer de un estudio detallado de los servidores de dominio de Windows y de algunos de los principales servidores de dominio de Linux, seleccionando la mejor alternativa atendiendo a desempeño, características, roles que puede realizar y que además este registrado por una licencia de libre distribución, etc. Para esto se han propuesto los siguientes objetivos específicos:

1. Realizar un trabajo introductorio sobre los servidores de dominio, características, conceptos, etc.
2. Realizar un análisis detallado de los servidores de dominio Windows.
3. Realizar un estudio de los principales servidores de dominio de software libre y hacer una comparación entre ellos
4. Realizar un análisis detallado del servidor de dominio Samba.
5. Realizar un breve estudio del servicio de directorio Ldap.
6. Realizar una guía detallada de la implementación de un servidor Samba + Ldap como Controlador de dominio primario (PDC).

## **Capítulo 1. Introducción a los servidores de dominio**

La administración de una red local bajo Windows NT se basa en los dominios y relaciones de confianza.

La unidad básica de la administración centralizada y la seguridad en Windows NT Server es el dominio. Un dominio es un conjunto de servidores que ejecutan Windows NT Server y que, en cierto modo, funcionan como un único sistema. Todos los servidores con Windows NT Server de un dominio utilizan el mismo conjunto de cuentas de usuario, por lo que sólo es necesario escribir una vez la información de una cuenta de usuario para que todos los servidores del dominio la reconozcan.

Dentro de los servidores de un dominio existen dos jerarquías: el servidor Controlador de Dominio Primario (Primary Domain Controller o PDC) y los servidores Controlador de Dominio Secundario (Backup Domain Controller o BDC). Por cada dominio ha de haber un Controlador de Dominio Primario y sólo uno, y posiblemente varios Controlador de Dominio Secundario. Cuando el administrador del dominio da de alta un nuevo usuario, lo hace sobre el PDC. Los datos sobre los usuarios se guardan en una base de datos llamada SAM, que la tiene cualquier servidor. El PDC se encarga de copiar esa base de datos de usuarios a todos los BDCs de su dominio de manera periódica. Con sólo dar de alta un usuario en el PDC, ese usuario automáticamente puede acceder a cualquier servidor del dominio usando el mismo nombre de usuario y la misma contraseña. Este proceso de copia periódica de la SAM se denomina replicación.

La agrupación de computadoras en dominios proporciona dos grandes ventajas a los usuarios y administradores de la red. Lo que es más importante, los servidores de un dominio constituyen una unidad administrativa única que comparte la información de seguridad y de cuentas de usuario. Cada dominio posee una base de datos que contiene las cuentas de los usuarios y grupos, y las configuraciones del plan de seguridad. Todos los servidores del dominio que funcionen como controlador principal de dominio o como controlador de reserva mantendrán una copia de esta base de datos.

La segunda ventaja de los dominios es la comodidad que brindan al usuario: cuando un usuario examine la red para buscar recursos disponibles, observará que está agrupada en dominios, en lugar de ver los servidores e impresoras de toda la red al mismo tiempo.

### **1.1. Windows NT**

Windows NT es una familia de sistemas operativos producidos por Microsoft, cuya primera versión fue publicada en 1993.

Previamente a la aparición del famoso Windows 95 la empresa Microsoft concibió una nueva línea de sistemas operativos orientados a estaciones de trabajo y servidores de red. Un sistema operativo con interfaz gráfica propia, estable y con características similares a los sistemas de red UNIX

#### **1.1.1. Windows NT 3.1**

Windows NT 3.1 es la primera versión de Windows NT. Este sistema ofrecía las siguientes características:

- Es compatible con 5 subsistemas: Win16, Win32, DOS, POSIX, OS/2.
- Multitarea.
- Kernel protegido, evitando que una aplicación inestable bloquee el sistema.

- Funciona como un cliente al servidor en un ambiente de red, compatible con sistema de multiproceso.
- Admite hasta 256 usuarios y administración de multidominio.

### **1.1.2. Windows NT 4.0**

Windows NT 4.0 fue la cuarta versión del sistema operativo de Microsoft Windows NT, lanzado en 1996. Es un sistema Windows de 32-bit disponible para estaciones de trabajo y versiones para servidores con una interfaz gráfica similar a la de Windows 95. Las letras NT provienen de la designación del producto como "Nueva Tecnología" (New Technology) según Bill Gates, pero nunca más tuvo un significado especial.

Con la salida de Windows 2000, Windows NT 4.0 se quedó obsoleto, pero todavía su uso está muy extendido (a fecha de 2005) a pesar de los esfuerzos de Microsoft por persuadir a los comerciantes para que se actualicen a nuevas versiones de Windows.

#### Características:

La característica más resaltable es que en las versiones para estaciones de trabajo y servidores Windows NT 4.0 han ganado la interfaz de Windows 95. Las ediciones para servidores de Windows NT 4.0 también incorporan un Servidor Web, Internet Information Server 2.0. También soporta de forma nativa los plugins y extensiones de Microsoft Frontpage, una aplicación para la creación de sitio web y su mantenimiento. Otras características importantes son Microsoft Transaction Server para aplicaciones en red, y Microsoft Message Queue Server (MSMQ), para mejorar las comunicaciones.

### **1.1.3. Windows Server 2000**

Windows 2000, se puso en circulación el 17 de febrero de 2000 con un cambio de nomenclatura para su sistema NT. Así, Windows NT 5.0 pasó a llamarse Windows 2000. Fue sucedido por Windows XP para equipos de escritorio en octubre de 2001 y Windows Server 2003 para servidores en abril de 2003. En este Sistema Operativo, se introdujeron algunas modificaciones respecto a sus predecesores como el sistema de archivos NTFS 5 y la capacidad de cifrar y comprimir archivos. Introdujo también las mejoras en el sistema de componentes COM, introduciendo COM+ que unificó en un solo paquete de los servicios anexados y la tecnología COM y MTS de Windows NT4, con nuevas ventajas.

Es el primer Windows capaz de reconocer memorias USB sin la necesidad de instalar controladores.

Existen cuatro variantes de Windows 2000 que son: Professional, Server, Advanced Server y Datacenter Server. Estas dos últimas variantes son ampliaciones del propio Windows 2000 Server. Windows 2000 Server es el sistema operativo para empresas y es ideal para ejecutar sus servidores de red o los servidores de archivo, impresión, intranet o de aplicaciones.

Es un sistema operativo más eficaz que Windows NT 4, ideal para ejecutar aplicaciones de negocios en línea, soluciones en comercio electrónico, etc. Ofrece una estructura completa de clústeres para alta disponibilidad y escalabilidad y admite el multiprocesamiento simétrico de ocho vías (SMP) además de memoria hasta de 8 GB con la Extensión de dirección física de Intel (PAE).

Windows 2000 Datacenter Server es una versión de primer nivel especializada para Windows 2000 Server, que admite el multiprocesamiento simétrico (SMP) de 32 vías y hasta 64 GB de memoria física. Al igual que Windows 2000 Advanced Server, proporciona los servicios de clústeres y equilibrio de carga al igual que las funciones estándar. Además, Windows 2000 Datacenter Server es óptimo para gran almacenamiento de datos, análisis econométricos, simulaciones a gran escala en ciencia e

ingeniería, procesamiento de transacciones en línea, proyectos de consolidación de servidor así como para ISP a gran escala y alojamiento de sitios Webs.

#### **1.1.4. Windows Server 2003**

Windows Server 2003 salió al mercado en el año 2003. Está basada en tecnología NT y su versión del núcleo NT es la 5.2.

En términos generales, Windows Server 2003 se podría considerar como un Windows XP modificado, no con menos funciones, sino que estas están deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor. Sin embargo, es posible volver a activar las características mediante comandos.

##### Características:

- Sistema de archivos NTFS:
  1. Cuotas
  2. Cifrado y compresión de archivos, carpetas y no unidades completas.
  3. Permite montar dispositivos de almacenamiento sobre sistemas de archivos de otros dispositivos al estilo Unix.
- Gestión de almacenamiento, backups... incluye gestión jerárquica del almacenamiento, consiste en utilizar un algoritmo de caché para pasar los datos menos usados de discos duros a medios ópticos o similares más lentos, y volverlos a leer a disco duro cuando se necesitan.
- Windows Driver Model: Implementación básica de los dispositivos más utilizados, de esa manera los fabricantes de dispositivos sólo han de programar ciertas especificaciones de su hardware.
- ActiveDirectory Directorio de organización basado en LDAP, permite gestionar de forma centralizada la seguridad de una red corporativa a nivel local.
- Autenticación Kerberos5
- DNS con registro de IP's dinámicamente
- Políticas de seguridad

##### Servidores:

Los servidores que maneja Windows 2003 son:

- Servidor de archivos
- Servidor de impresiones
- Servidor de aplicaciones
- Servidor de correo (SMTP/POP)
- Servidor de terminal
- Servidor de Redes privadas virtuales (VPN) (o acceso remoto al servidor)
- Controlador de Dominios (mediante Active Directory)
- Servidor DNS

- Servidor DHCP
- Servidor de Streaming de Vídeo
- Servidor WINS

#### Mejoras respecto a Windows 2000 Server

1. Durante la instalación arranca con el mínimo de servicios activados para no comprometer la seguridad del sistema
2. Mejoras en el manejo de políticas de seguridad
3. Active Directory ya no utiliza NetBIOS sino que es necesaria la presencia de un DNS (Servidor de Nombres de Dominio) que soporte Service Records (detección de servicios ofrecidos por una máquina a través de un DNS)

#### Versiones:

Actualmente existen cuatro versiones de Windows 2003, todas ellas cuentan a su vez con versiones de 32 y 64 bits (excepto Web Edition). Las versiones son:

- Web Edition Diseñado para los servicios y el hospedaje Web.
- Standard Edition El más versátil de todos, ofrece un gran número de servicios útiles para empresas de cualquier tamaño.
- Enterprise Edition Para empresas de mayor tamaño que la Standard Edition.
- Datacenter Edition Para empresas que requieran bases de datos más escalables y un procesamiento de transacciones de gran volumen.

#### Service Pack 1 (SP1):

El 30 de marzo de 2005, Microsoft lanza (Service Pack 1), para todas las versiones de Windows 2003. Con él, dotan al Sistema operativo de las mejoras incluidas en el SP2 de Windows XP, tales como una nueva interfaz para el Cortafuegos (aunque al tratarse de un servidor, el cortafuegos estará deshabilitado por defecto), o la corrección de todos los bugs aparecidos hasta la fecha en Windows Server 2003. El soporte de Windows Server 2003 Service Pack 1 finalizó el 14 de abril de 2009.

#### Service Pack 2 (SP2):

El 12 de marzo de 2007 se lanzó el Service Pack 2 de Windows Server 2003. Este SP2 está concebido como una actualización para Windows Server 2003 R2, a su vez una actualización del Server 2003 original que Microsoft lanzó en diciembre de 2005. No obstante, este Service Pack se instala tanto sobre versiones R2 del sistema como sobre la versión original.

Entre las novedades que podemos encontrar en este Service Pack destacamos:

- Microsoft Management Console (MMC) 3.0, que hace del proceso de creación de directivas (policy) de grupos introducido en el anterior service pack, algo más intuitivo y manejable.
- Windows Deployment Services en sustitución de Remote Installation Services para la realización de instalaciones remotas del sistema (sin encontrarse delante de la computadora en la cual se va a instalar ni tener el DVD del sistema en el lector de esta).

- Scalable Networking Pack (SNP) permite escalar las redes corporativas (hacerlas crecer y controlar dicho crecimiento en la dirección que queramos) para hacer frente a las crecientes demandas de ancho de banda por parte de algunas aplicaciones concretas.
- El cliente de conexión a redes inalámbricas soporta ahora autenticación WPA2.
- Incluye todas las actualizaciones de seguridad y parches lanzados hasta la fecha.

Este Service Pack ya puede descargarse para su instalación o en formato de imagen ISO para grabar en CD o DVD para las plataformas de 32 y 64 bits. El Soporte Técnico para este Service Pack finalizará 12 ó 24 meses presentado el próximo Service Pack, o cuando finalice el ciclo de vida del producto, lo que ocurra primero.

### **1.1.5. Windows Server 2008**

Windows Server 2008 es el sucesor de Windows Server 2003, distribuido al público casi cinco años antes. Al igual que Windows Vista, Windows Server 2008 se basa en el núcleo Windows NT 6.0. Posteriormente se lanzó una segunda versión, denominada Windows Server 2008 R2.

#### Características:

Hay algunas diferencias con respecto a la arquitectura del nuevo Windows Server 2008, que pueden cambiar drásticamente la manera en que se usa este sistema operativo. Estos cambios afectan a la manera en que se gestiona el sistema hasta el punto de que se puede llegar a controlar el hardware de forma más efectiva, se puede controlar mucho mejor de forma remota y cambiar de forma radical la política de seguridad. Entre las mejoras que se incluyen, están:

- Nuevo proceso de reparación de sistemas NTFS: proceso en segundo plano que repara los archivos dañados.
- Creación de sesiones de usuario en paralelo: reduce tiempos de espera en los Terminal Services y en la creación de sesiones de usuario a gran escala.
- Cierre limpio de Servicios.
- Sistema de archivos SMB2: de 30 a 40 veces más rápido el acceso a los servidores multimedia.
- Address Space Load Randomization (ASLR): protección contra malware en la carga de controladores en memoria.
- Windows Hardware Error Architecture (WHEA): protocolo mejorado y estandarizado de reporte de errores.
- Virtualización de Windows Server: mejoras en el rendimiento de la virtualización.
- PowerShell: inclusión de una consola mejorada con soporte GUI para administración.
- Server Core: el núcleo del sistema se ha renovado con muchas y nuevas mejoras.

#### Ediciones:

La mayoría de las ediciones de Windows Server 2008 están disponibles en x86-64 (64 bits) y x86 (32 bits). Windows Server 2008 para sistemas basados en Itanium soporta procesadores IA-64. La versión IA-64 se ha optimizado para escenarios con altas cargas de trabajo como servidores de bases de datos y aplicaciones de línea de negocios (LOB). Por ende no está optimizado para su uso como servidor de archivos o servidor de medios. Microsoft ha anunciado que Windows Server 2008 será el último

sistema operativo para servidores disponible en 32 bits. Windows Server 2008 está disponible en las ediciones que figuran a continuación, similar a Windows Server 2003:

- Windows Server 2008 Standard Edition (x86 y x86-64)
- Windows Server 2008 R2 Todas las Ediciones (Solo 64Bit)
- Windows Server 2008 Enterprise Edition (x86 y x86-64)
- Windows Server 2008 Datacenter Edition (x86 y x86-64)
- Windows HPC Server 2008 (reemplaza Windows Compute Cluster Server 2003)
- Windows Web Server 2008 (x86 y x86-64)
- Windows Storage Server 2008 (x86 y x86-64)
- Windows Small Business Server 2008 (Nombre clave "Cougar") (x86-64) para pequeñas empresas
- Windows Essential Business Server 2008 (Nombre clave "Centro") (x86-64) para empresas de tamaño medio
- Windows Server 2008 para sistemas basados en Itanium
- Windows Server 2008 Foundation Server

#### Service Pack 2:

Debido a que Windows Server 2008 se basa en el núcleo Windows NT 6.0 Service Pack 1, la versión final (RTM) es considerada como Service Pack 1; de acuerdo a esto, el primer service pack lanzado será llamado "Service Pack 2". Anunciado el 24 de octubre de 2008, este service pack contiene los mismos cambios y mejoras que el equivalente próximo a salir Windows Vista Service Pack 2, así como la versión final de Hyper-V (1.0) y mejoras que le permiten una reducción del 10% en el uso de energía.

## **1.2. Directorio Activo (Active Directory o AD)**

Directorio Activo es el término que utiliza la Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadoras. Usa distintos protocolos, algunos de los principales son: Kerberos, LDAP, DNS y DHCP.

El Active Directory Está basado en una serie de estándares llamados (X.500). Posee una estructura jerárquica que le permite mantener una serie de objetos con elementos de la red (usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso).

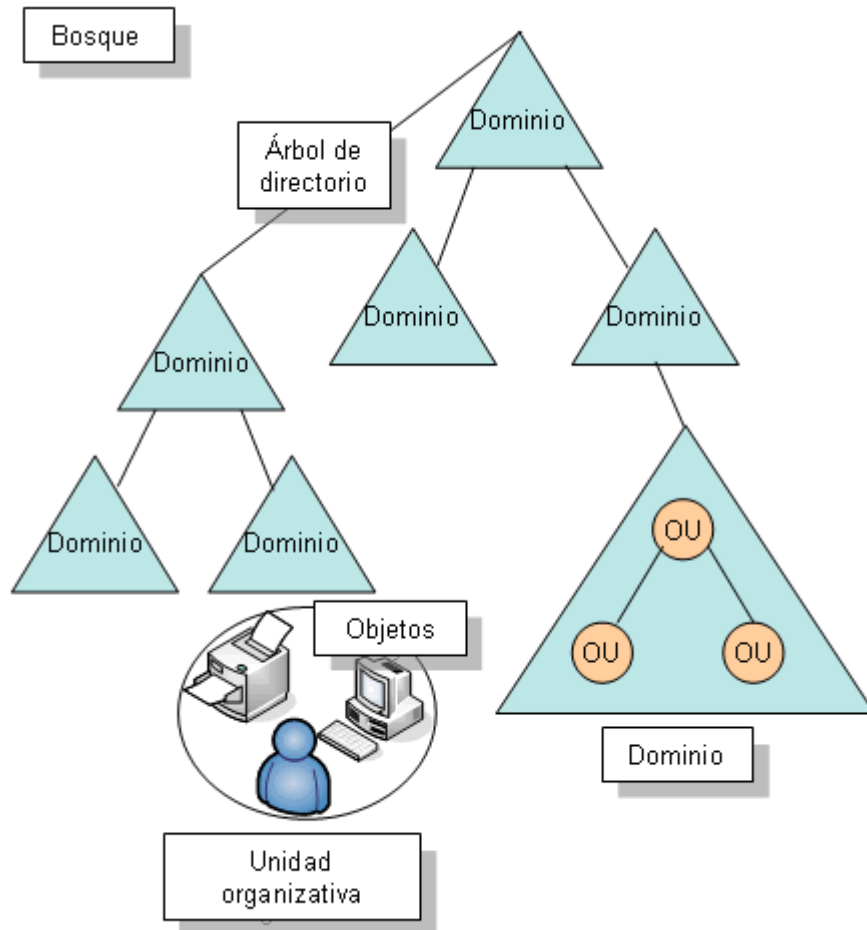


Figura 1. Estructura del Directorio Activo

Los Dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, por esta razón Active Directory requiere uno o más servidores DNS que permitan direccionar los elementos que pertenecen a la red, como son el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios.

Un ejemplo de la estructura descendente (o herencia), es que si un usuario pertenece a un dominio, será reconocido en todo el árbol generado a partir de ese dominio, sin necesidad de pertenecer a cada uno de los subdominios.

### 1.2.1. Funcionamiento

Como este protocolo está implementado de forma similar a una base de datos su funcionamiento es parecida a otras estructuras LDAP; almacena en forma centralizada toda la información relativa a un dominio de autenticación. Esto posee la ventaja de que se puede sincronizar los distintos servidores de autenticación de todo el dominio.

Cada uno de los objetos de Active Directory tendrán atributos que permite identificarlos de manera única; por ejemplo los usuarios tendrán campos «nombre», «email», etcétera.

### 1.2.2. Requisitos de instalación

Estos son los requisitos recomendados para la creación de un dominio:

- Tener cualquier versión Server de Windows 2000 o 2003 (Server, Advanced Server o Datacenter Server), en el caso de 2003 server, tener instalado el service pack 1 en la máquina.
- Protocolo TCP/IP instalado y configurado manualmente, es decir, sin contar con una dirección asignada por DHCP,
- Tener un servidor de nombre de DNS, para resolver la dirección de los distintos recursos físicos presentes en la red
- Poseer más de 250 MB en una unidad de disco formateada en NTFS.

### **1.2.3. Direccionamiento a los recursos de Active Directory**

Los direccionamientos a recursos de Active Directory son estándares con la Convención Universal de Nombrado (UNC), Localizador Uniforme de Recursos (URL) y nombrado de LDAP.

Cada objeto de la red posee un nombre de distinción (en inglés, Distinguished name (DN)), así un usuario llamado Pepe en una Unidad Organizativa (en inglés, Organizational Units, OU) llamada Comercial y un dominio co.cu, puede escribirse de las siguientes formas para ser direccionado:

- En DN sería CN=Pepe, OU=Comercial, DC=co, DC=cu, donde
- CN es el nombre común (en inglés, Common Name)
- DC es clase de objeto de dominio (en inglés, Domain object Class).
- En forma canónica sería co.cu/Comercial/Pepe

Los otros métodos de direccionamiento constituyen una forma local de localizar un recurso

- Distinción de Nombre Relativo (en inglés, Relative Distinguished Name (RDN)), que busca un recurso sólo con el Nombre Común (CN).
- Globally Unique Identifier (GUID), que genera una cadena de 128 bits que es usado por Active Directory para buscar y replicar información.

Ciertos tipos de objetos poseen un Nombre de Usuario Principal (en inglés, User Principal Name (UPN)) que permite el ingreso abreviado a un recurso o un directorio de la red. Su forma es objetodered@dominio.

### **1.2.4. Diferencias entre Active Directory y Windows NT**

En Windows NT Server solo se podía prever un solo dominio de administración, en Active Directory se puede crear estructuras jerárquicas de dominio y subdominios, facilitando la estructuración de los recursos según su localización o función dentro de la organización a la que sirven. Otra diferencia importante es el uso de estándares como X.500 y LDAP para el acceso a la información.

### **1.2.5. Alternativas a Active Directory**

Hoy en día existen distintas variantes a Active Directory, algunas de las más importantes se mencionan a continuación:

- Samba: Es un programa de código libre que tiene disponible un controlador de dominios compatible con Windows NT 4
- Mandriva Directory Server: Es un programa de código libre. Ofrece una interfaz web para manejar el controlador de dominio Samba y el servicio de directorio LDAP

- Novell eDirectory: Es una multiplataforma que puede correr sobre cualquier sistema operativo (Linux, AIX, Solaris, Novell Netware, UNIX y además integra LDAP v.3 Nativo). Es el precursor en materia de estructuras de Directorio, ya que fue introducido en 1990 con la versión de Novell Netware 4.0. Aunque AD de Microsoft alcanzó mayor popularidad, todavía no puede igualar la fiabilidad y calidad de eDirectory y su capacidad Multiplataforma.
- Sun Java ES Directory Server y OpenDS: Son otras alternativas basadas en java. El primero es un producto de Sun Microsystems y el segundo una alternativa de código abierto.
- WBSAgnitio: Es una alternativa que integra OpenLDAP, Heimdal kerberos, Samba y además certificación digital y Bind9 (modificado para usar LDAP como backend).(Wikipedia Foundation #9, 2010)
- Likewise Open: Es un proyecto de código abierto patrocinado por Likewise Software para integrar la autenticación de sistemas Linux, Unix, Windows, y Macintosh con Directorio Activo.

De las soluciones mencionadas, Samba es la mejor opción como alternativa libre al Servidor de Dominio de Windows, a continuación se exponen algunas de las razones:

- Funciona como Servidor de Archivos.
- Funciona como Servidor de Impresión.
- Funciona como Controlador de Dominio Primario.
- Funciona como Servidor Primario WINS.
- Permite la autenticación a una gran variedad de clientes de la familia de Microsoft Windows(95, 98, Me, NT, 2000, XP, etc).
- Soporta la autenticación a través de un Servidor LDAP

Además es un software licenciado por patentes de libre distribución y es soportado por una gran variedad de plataformas. Entre los sistemas tipo Unix en los que se puede ejecutar Samba, están las distribuciones GNU/Linux, Solaris y las diferentes variantes BSD entre las que podemos encontrar el Mac OS X Server de Apple.(Wikipedia Foundation #2, 2010)

### **1.3. Elección del software**

#### Debian como Sistema Operativo:

La base de este trabajo es un Sistema Operativo libre fundamentado en el proyecto GNU, cuyo objetivo era crear un Sistema Operativo completamente libre.

En 1992 el núcleo de Linux fue combinado con el GNU, resultando en un Sistema Operativo Libre y completamente funcional. El Sistema Operativo formado por esta combinación usualmente se conoce como “GNU/Linux” o como una “distribución Linux” y existen numerosas variantes(Wikipedia Foundation #1, 2010). La distribución Linux que se usa en este proyecto es la versión estable Debian GNU/Linux versión 5 o Lenny.

Los principales motivos son:

- Amparado por licencias de libre distribución (GNU)
- Ningún coste del software
- Rápido

- Estable
- Reconoce una gran cantidad de Hardware estándar(Debian, #23)

Haciendo una comparación entre Windows 2008 y Linux Debian versión 5 tenemos que:

Los requerimientos mínimos para Windows Server 2008 se muestran a continuación:

*Tabla 1. Requisitos de hardware para Windows Server 2008*

Requisitos del sistema	
Velocidad mínima de la CPU	1 GHz (x86) o 1.4 GHz (x64)
Velocidad recomendada de la CPU	2 GHz o superior
Memoria RAM mínima	512 MB RAM (podría limitarse el rendimiento y algunas características)
Memoria RAM mínima recomendada	2 GB RAM o más
Espacio en disco para la instalación	1,5 GB

Los precios para algunas de las versiones son los siguientes

- Windows Server 2008 Standard: 999 dólares con 5 licencias cliente.
- Windows Server 2008 Enterprise: 3.999 dólares con 25 licencias cliente.
- Windows Web Server 2008: 469 dólares.
- Windows Server 2008 Datacenter: 2.999 dólares por procesador.
- Windows Server 2008 para sistemas Itanium 2.999 dólares por procesador.

Para Debian GNU/Linux versión 5 los principales requisitos de hardware son

*Tabla 2. Requisitos de hardware para GNU/Linux Debian versión 5*

Requisitos del sistema	
Velocidad mínima de la CPU	Pentium 4, a 1 GHz para un sistema de escritorio.
Memoria RAM mínima	64 MB
Memoria RAM mínima recomendada	256 MB Sin escritorio 512 MB Con escritorio
Espacio en disco para la instalación	1 GB Sin escritorio 5 GB Con escritorio

## Capítulo 2. Samba + Ldap como Controlador de dominio primario(PDC)

### 2.1. Samba

#### 2.1.1. Conceptos teóricos

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

- Compartir uno o varios sistemas de archivos
- Compartir uno o varios sistemas de archivos distribuidos
- Compartir impresoras instaladas en el servidor entre los clientes Windows de la red
- Ayudar a los clientes permitiéndoles navegar por la red
- Autenticar a los clientes que ingresan en un dominio Windows
- Proveer o ayudar con un servidor de resolución de nombres Windows (WINS)

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

Samba actualmente está mantenido y es ampliado por un grupo de voluntarios bajo la supervisión activa de Andrew Tridgell, su creador. Al igual que el núcleo Linux, sus autores lo distribuyen como software Open Source, bajo los términos de la licencia GPL (GNU General Public License). Desde su concepción, el desarrollo de Samba ha sido patrocinado en parte por la Australian National University, donde Andrew Tridgell hizo su doctorado. A partir de entonces, muchas otras organizaciones han patrocinado a los desarrolladores de Samba, incluyendo LinuxCare, VA Linux Systems, Hewlett-Packard e IBM.

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

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

Smbd: Permite la compartición de archivos e impresoras sobre una red SMB y proporciona autenticación y autorización de acceso para clientes SMB.

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

#### 2.1.2. Visión general de Samba

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

### nmbd

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

### smbd

El demonio smbd maneja los recursos compartidos entre el servidor Samba y sus clientes. Provee los servicios de servidor de archivos, impresión y búsqueda a los clientes SMB, maneja todas las notificaciones entre el servidor Samba y la red de clientes. Es también el responsable de la autenticación de usuarios, bloqueo de recursos y compartición de datos a través del protocolo SMB.

A partir de la versión 2.2 se añadió otro nuevo demonio:

### winbind

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

Samba posee además un conjunto de pequeñas herramientas para consola, a continuación se mencionan las más significativas:

### findsmb

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

### make smbcodepage

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

### net

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

### nmblookup

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

### pdbedit

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

### smbclient

Un cliente Unix similar a un cliente ftp, que se puede utilizar para conectarse a los recursos compartidos SMB y operar con ellos.

### smbcontrol

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

### smbgroupedit

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

### smbpasswd

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

### smbstatus

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

### testparm

Un programa que comprueba el archivo de configuración de Samba.

### testprns

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

### wbinfo

Una utilidad utilizada para realizar peticiones al demonio winbind.

Cada nueva liberación de Samba se somete a un chequeo intensivo antes de anunciarla y es actualizada rápidamente después de liberada si ocurren problemas o se encuentran efectos inesperados

## **2.1.3. ¿Qué novedades ofrece el Samba 3?**

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

En la tabla 3 se muestra un resumen de los roles que puede asumir un servidor de Samba 3.0 y cuáles son sus limitaciones:

Tabla 3. Roles de Samba 3.0

Roles existentes	Permitidos
Servidor de archivos	Sí
Servidor de impresión	Sí
Servidor Dfs de Microsoft	Sí
Controlador de dominio primario	Sí
Controlador de dominio secundario	No
Controlador de dominio <i>Active Directory</i>	No
Autenticación de clientes Windows 95/98/Me	Sí

Autenticación de clientes Windows NT/2000/XP	Sí
Buscador maestro local	Sí
Buscador de respaldo local	Sí
Buscador maestro de dominio	Sí
Servidor primario WINS	Sí
Servidor secundario WINS	No

Debido a que muchos de los protocolos del dominio Windows son propietarios y no han sido documentados por Microsoft se ha tenido que utilizar la ingeniería inversa para poder soportarlos. Por este motivo la versión 3.0 de Samba aún no soporta completamente Active Directory.(González, 2004)

#### **2.1.4. Samba 4**

Actualmente se está trabajando en la implementación de una cuarta versión de servidor de dominio Samba, llamada Samba 4. Consiste en una nueva reescritura del viejo código de Samba con el ambicioso objetivo de permitirle convertirse en un Controlador de Dominio de Directorio Activo.

Entre las mejoras propuestas están:

- Soporta autenticación con Directorio Activo y protocolos de administración.
- Servidor LDAP interno con soporte de Directorio Activo.
- Integración del servidor de nombres de dominio Bind9 para el soporte DNS del Directorio Activo.
- Soporte para Python para ser usado por los clientes y herramientas de administración.

#### **2.1.5. Configuración de Samba**

Al igual que todas las aplicaciones para Linux, Samba dispone de un archivo de texto para su configuración. En el caso de la distribución Debian GNU/Linux el fichero se encuentra en: /etc/samba/smb.conf

El archivo smb.conf está dividido en secciones identificadas con corchetes [ ]. Las secciones son las siguientes:

##### Sección [global]

Aquí se configuran los parámetros generales que determinarán el modo de comportamiento general del servidor samba. Los parámetros que se omitan tomarán el valor predefinido por defecto. Existen unos 300 parámetros que se pueden configurar en ésta sección. A continuación exponemos los parámetros más significativos según este trabajo y ejemplos de los valores que pueden tomar:

- workgroup: Definición del nombre del dominio. Ej: workgroup = MIDOMINIO
- netbios name: Nombre Netbios por el cual el servidor Samba se va a conocer. Ej: netbios name = Servidor
- server string: Descripción del servidor. Ej: server string = Servidor PDC Samba + LDAP
- encrypt passwords: Se activa el cifrado para el almacenado de las claves. Ej: encrypt passwords = true

- `passdb backend`: Se le indica a Samba que las claves se almacenarán y recuperarán del servidor definido. Ej: `ldapsam:ldap://midominio.cu`
- `passwd program`: Programa utilizado durante el cambio de clave de un usuario. Ej: `passwd program = /usr/sbin/smbldap-passwd -o %u`
- `ldap admin dn`: Se le especifica a Samba qué usuario es el administrador del directorio LDAP. Será el usuario utilizado por el servidor cuando se realicen operaciones de añadir, borrar o modificar cuentas de usuario. Ej: `ldap admin dn = cn=admin,dc=midominio,dc=cu`
- `ldap server`: Este parámetro contiene el FQDN del servidor ldap. Se necesita para encontrar la información sobre las cuentas de usuario. Ej: `ldap server = midominio.cu`
- `ldap port`: Indica el puerto por el que estará “escuchando” el servidor LDAP. Ej: `ldap port = 389`
- `ldap suffix`: Parámetro que especifica la base para todas las búsquedas en LDAP. Ej: `ldap suffix = dc=midominio,dc=cu`
- `ldap user suffix`: Indica donde se añaden los usuarios dentro del árbol. Ej: `ldap user suffix = ou=people`
- `ldap group suffix`: Indica donde se añaden los grupos de usuarios dentro del árbol. Ej: `ldap group suffix = ou=groups`
- `ldap machine suffix`: Indica donde se añaden las máquinas dentro del árbol. Ej: `ldap machine suffix = ou=computers`
- `preferred master`, `domain master`, `local master`, `domain logons`: Estos parámetros aseguran el control del dominio y el soporte de autenticación en red. Una descripción más detallada se puede encontrar en la página del manual `smb.conf`. Ej:

`preferred master = yes`

`domain master = yes`

`local master = yes`

`domain logons = yes`

#### Sección [homes]:

En ésta sección se configuran los parámetros para compartir la carpeta donde se almacena el perfil y todos los documentos (homes) de cada usuario. Es opcional. Si no existe, no se compartirán las carpetas home de cada usuario.

#### Una sección por cada carpeta compartida:

Cada vez que se comparte una carpeta, es necesario crear una sección donde se defina el nombre con que será compartido el recurso. Por ejemplo, si deseamos compartir la carpeta `/home/samba/libros` crearemos una sección [libros] donde se configurará dicho recurso compartido con los parámetros específicos para dicho recurso. Parámetros destacables:

- `browseable = yes`

Indica si el recurso compartido será visible cuando se escanea la red, por ejemplo haciendo clic en 'Mis sitios de red' en Windows

- `create mask = 0770`

Establece la máscara de creación de archivos, igual con directory mask para la creación de carpetas

- guest ok = yes

Indica que cualquier usuario sin contraseña tiene permiso de acceso

- valid users = pepe, juan

Indica qué usuarios pueden acceder al recurso

### **2.1.6. Instalación**

Las instalaciones de Samba y los demás software que se usaron en este trabajo las podemos encontrar en los repositorios de Debian. En el caso de Debian Lenny en el fichero /etc/apt/source.list le indicamos al sistema el repositorio que vamos a utilizar.

Para la realización de este programa se va a utilizar:

- samba
- smbclient
- smbfs
- smbldap-tools

## **2.2. OpenLDAP**

### **2.2.1. Conceptos Teóricos**

LDAP es un protocolo ligero para acceder al servicio de directorio, especialmente al basado en X.500. Se ejecuta sobre TCP/IP o sobre otros servicios de transferencia orientado a conexión. Su definición detallada está disponible en el RFC2251 “The Lightweight Directory Access Protocol (v3)” y en otro documento que comprende las especificaciones técnicas, RFC3377.

### **2.2.2. ¿Qué tipo de información se puede almacenar en un directorio?**

El modelo de información de LDAP está basado en entradas. Una entrada es una colección de atributos que tienen un único y global Nombre Distinguido (DN). El DN se utiliza para referirse a una entrada sin ambigüedades. Cada atributo de una entrada posee un tipo y uno o más valores. Los tipos son normalmente palabras nemotécnicas, como “cn” para common name, o “mail” para una dirección de correo. La sintaxis de los atributos depende del tipo de atributo. Por ejemplo, un atributo cn puede contener el valor “Lazaro J Ramos”. Un atributo email puede contener un valor “lramos@midominio.com”.

### **2.2.3. ¿Cómo se almacena la información?**

Las entradas están organizadas en una estructura jerárquica en árbol. Cada nodo del árbol de datos se lo denomina “entrada”. Cada entrada tiene una denominación, o DN(Distinguished Name, nombre distinguido), que se forma de la concatenación de los DNs relativos (o RDNs) de las entradas “padre” hasta llegar a la entrada “raíz” del árbol, como se muestra en la siguiente figura 2:

dc = DomainComponent  
ou = OrganizationalUnitName  
cn = CommonName

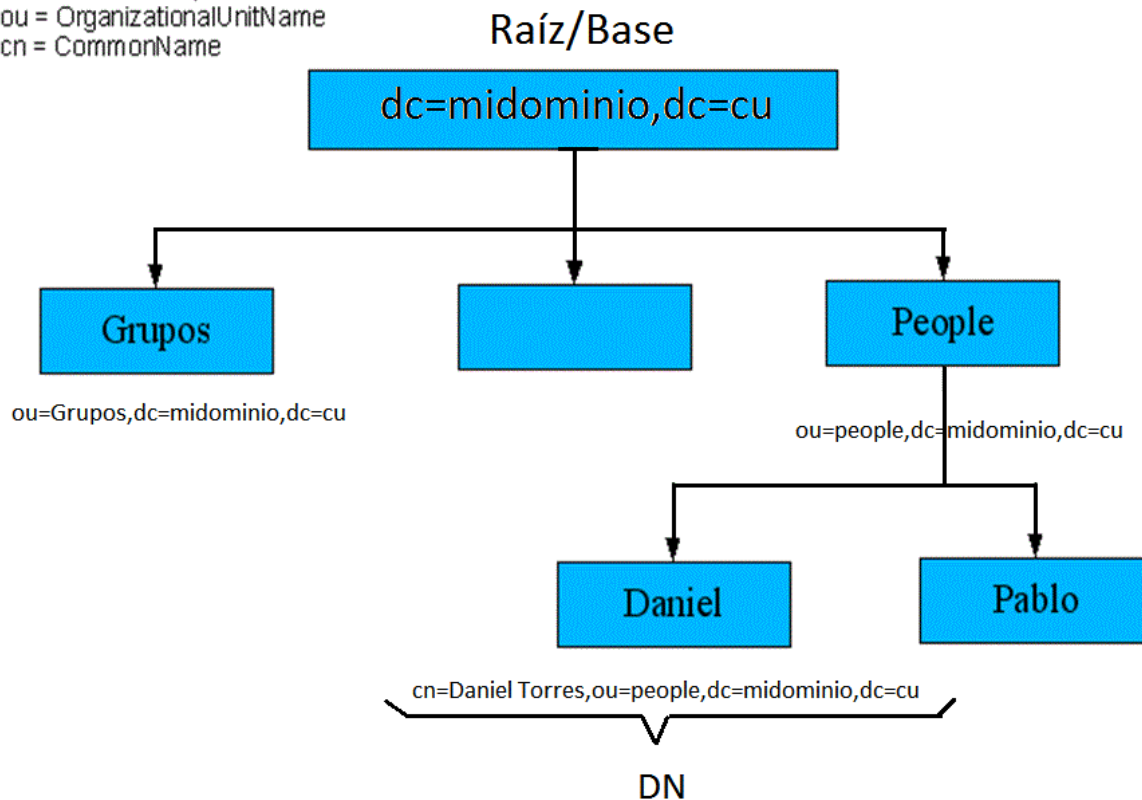


Figura 2. Estructura del árbol de LDAP

#### 2.2.4. ¿Cómo se accede a la información?

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

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

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

#### 2.2.6. Esquemas (Schemas)

En un directorio LDAP, el esquema es la colección de atributos definidos, clases de objetos definidas, y ACIs para controlar dónde es almacenado cada dato.

Cualquier base de datos, sin tener en cuenta su complejidad o tecnología subyacente, tiene un esquema. En términos simples, un esquema es el modelo de los datos, el diseño en lo tocante a cómo los datos se almacenan, qué tipos de datos son rastreados, y las relaciones entre datos almacenados en varias entradas.

Cuando se configura un directorio LDAP, la información para cualquier entrada dada se almacena en una serie de atributos. Se puede, además, crear nuevos tipos de valores que serán almacenados en el directorio.

### **2.2.7. ¿Cómo trabaja LDAP?**

El servicio de directorio de LDAP está basado en el modelo cliente/servidor. Uno o más servidores LDAP contienen los datos que conforman la información del árbol del directorio. El cliente se conecta a los servidores y les formula preguntas. Los servidores responden con una respuesta o con un puntero donde el cliente puede obtener información adicional.

### **2.2.8. LDAP versión 3**

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

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

### **2.2.9. ¿Qué es slapd?**

Slapd es un servidor de directorio LDAP que se ejecuta en distintas plataformas. Entre sus características más interesantes están:

- Slapd implementa la versión 3 de Lightweight Directory Access Protocol, además soporta LDAP sobre IPv4, IPv6 y Unix IPC.
- Tiene soporte de autenticación fuerte gracias al uso de SASL. La implementación SASL de slapd hace uso del software Cyrus SASL, el cual soporta un gran número de mecanismos de autenticación, como: DIGEST-MD5, EXTERNAL, y GSSAPI.
- Provee protecciones de privacidad e integridad gracias al uso de TLS (o SSL). La implementación TLS de slapd hace uso del software OpenSSL.
- Slapd provee facilidades de control de acceso muy potentes, permitiéndole controlar el acceso a la información de su(s) base(s) de datos. Puede controlar el acceso a las entradas basándose en la información de autorización de LDAP, en la dirección IP, en los nombres de dominio y otros criterios. slapd soporta tanto el control de acceso a la información dinámico como estático.
- Hace uso de hilos para obtener alto rendimiento. Un proceso único multihilo maneja todas las peticiones entrantes haciendo uso de una piscina de hilos. Esto reduce la carga del sistema a la vez que provee alto rendimiento.
- Se puede configurar para que mantenga copias de la información del directorio. Este esquema de replicación, un único maestro/múltiples esclavos, es vital en ambientes con un volumen alto de peticiones, donde un único servidor slapd no podría proveer la disponibilidad ni la confiabilidad

necesarias. Slapd incluye también un soporte experimental para la replicación de múltiples maestros. slapd soporta dos métodos de replicación: Sync LDAP y slurpd.

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

### **2.2.10. ¿ Qué es Slurpd?**

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

Slapd y Slurpd se comunican a través de un simple archivo de texto, que es utilizado para almacenar los cambios ocurridos.

### **2.2.11. Configuración**

La configuración de LDAP se realiza en el fichero `/etc/ldap/sldap.conf`

En el archivo `slapd.conf`, se definen los esquemas (schema) a utilizar en dependencia de la aplicación. A continuación se muestra un ejemplo de algunos de los esquemas que se pueden establecer:

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

### **2.2.12. Instalación**

Para la realización de este trabajo se usó:

- Slapd
- Libpam-ldap
- Libnss-ldap

## **2.3. PHPLDAPADMIN**

### **2.3.1. Conceptos teóricos**

PHPLDAPADMIN es una interfaz web escrita en PHP para la configuración de LDAP. Puede ser ejecutada en cualquier navegador de internet.

### **2.3.2. Instalación**

Serán necesarios los siguientes paquetes:

- apache2-suexec

- libapache2-mod-php5
- php5
- php5-cli
- php5-curl
- php5-gd php5-imap
- php5-ldap
- php5-mcrypt
- php5-mhash
- php5-sqlite
- php5-tidy php5-xmllrpc
- php-pear

## **2.4. Account-Manager (LAM)**

### **2.4.1. Conceptos teóricos**

LDAP Account Manager(LAM) es una interfaz Web para administrar varios tipos de cuentas en un directorio LDAP. Está escrito en PHP. En contraste con la herramienta PhpLDAPAdmin, se focaliza en las cuentas y brinda al usuario una vista más abstracta del su directorio. Está licenciada bajo GNU General Public License.(Nozawa)

LAM está diseñado especialmente para la administración del esquema samba de OpenLDAP, por este motivo, se decidió utilizar esta herramienta.

## Capítulo 3. Guía de implementación de un Servidor Samba + LDAP como Controlador de Dominio Principal en Debian GNU/Linux versión 5 o Debian Lenny.

### 3.1. Nota introductoria

La distribución usada para este trabajo es la versión estable de Debian, Lenny o versión 5. La ubicación de los archivos de configuración tratados en este documento pueden variar en dependencia de la distribución y la versión que tenga. Esta guía se ha elaborado tomando como base diversa documentación obtenida en internet y adaptada a las características de la institución en la que se implementó. Los comandos, para diferenciarlos, aparecerán sombreados y se deben llevar a cabo en la consola como usuario root.

Puede contactar a los autores para obtener los ficheros de configuración modificados que se referirán en esta guía, estos poseen una configuración estándar que debe ser personalizada según las características de la red y dominio donde se vaya a instalar. Se recomienda que se sobrescriban ficheros de configuración originales con los de dicha carpeta y se le ajusten los parámetros de configuración de acuerdo a las necesidades de la red donde se vaya a instalar.

### 3.2. Instalando los paquetes que se van a utilizar

Para instalar los paquetes requeridos se usó el gestor “aptitude”. Cualquier tipo de configuración durante el proceso de instalación puede ser cancelada.

```
aptitude install apache2-suexec libapache2-mod-php5 php5 php5-cli php5-curl php5-gd php5-imagick php5-ldap php5-mcrypt php5-mhash php5-sqlite php5-tidy php5-xmlrpc php-pear slapd mcrypt ldap-utils libgd-tools apache2-doc libpam-ldap libnss-ldap resolvconf samba swat smbclient smbfs smbldap-tools
```

### 3.3. Configurando SLAPD

Ejecutar el comando “`dpkg-reconfigure slapd`” y configurar SLAPD con los siguientes parámetros:

- Omit OpenLDAP server configuration?: No
- DNS domain name: institucion.cu
- Organization name: institucion.cu
- Administrator password: mipassword
- Database backend to use: HDB
- Do you want the database to be removed when slapd is purged? No
- Allow LDAPv2 protocol? No

Hacer una copia de seguridad de la base de datos LDAP

```
slapcat > ~/slapd.ldif
```

### 3.4. Preparando el esquema de LDAP para samba

```
zcat /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz > \  
/etc/ldap/schema/samba.schema
```

Generar la contraseña rootdn con MD5

```
slappasswd -h {MD5}
```

Reemplazar el fichero /etc/ldap/slapd.conf y ajustarle los siguientes parámetros:

- Suffix(Línea # 57):
- Rootdn(Línea # 61):
- Rootpw(Línea # 62):

Detener el nscd para compilar el LDAP:

```
/etc/init.d/nscd stop
```

Renovar la base de datos LDAP con los siguientes comandos:

```
/etc/init.d/slapd stop  
rm -rf /var/lib/ldap/*  
slapadd -l ~/slapd.ldif  
slapindex  
chown -Rf openldap:openldap /var/lib/ldap  
/etc/init.d/slapd start
```

Verificar los cambios con “slapcat”

### **3.5. Instalación de phpLDAPadmin y LDAP-Account-Manager**

```
aptitude install phpldapadmin ldap-account-manager
```

### **3.6. Preparando Samba**

Reemplazar el fichero /etc/samba/smb.conf y ajustar los parámetros siguientes:

- workgroup(Línea # 8)
- realm(Línea # 9)
- ldap admin dn(Línea # 39)
- ldap suffix(Línea # 44)

Cambiar la clave del LDAP para Samba:

```
smbpasswd -w mypassword
```

Reiniciar Samba con el siguiente comando:

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

Probar la configuración de Samba con el comando “testparm” y verificar cualquier mensaje de error.

### **3.7. Configurando smbldap-tools**

Preparando los ficheros de configuración de smbldap-tools

```
zcat /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz > \
```

```
/etc/smbldap-tools/smbldap.conf
cp /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf \
/etc/smbldap-tools/smbldap_bind.conf
```

Obtener el SID de Samba para usarlo en /etc/smbldap-tools/smbldap.conf:

```
net getlocalsid
```

Reemplazar /etc/smbldap-tools/smbldap.conf y ajustarla, los principales parámetros recomendados son los siguientes:

- sid (Línea # 37)
- sambaDomain (Línea # 42)
- suffix (Línea # 100)
- mailDomain (Línea # 206)

Reemplazar /etc/smbldap-tools/smbldap\_bind.conf y modificarle los parámetros:

- slaveDN (Línea # 8)
- slavePw (Línea # 9)
- masterDN (Línea # 10)
- masterPw (Línea # 11)

Cambiar los permisos a los ficheros de configuración

```
chmod 0644 /etc/smbldap-tools/smbldap.conf
chmod 0600 /etc/smbldap-tools/smbldap_bind.conf
```

### **3.8. Replicar el esquema de LDAP para Samba:**

```
smbldap-populate
```

### **3.9. Configurar PAM/NSS con LDAP**

Ejecutar el comando “dpkg-reconfigure libnss-ldap” y configurar los siguientes parámetros:

- LDAP server Uniform Resource Identifier: ldap://127.0.0.1
- Distinguished name of the search base: dc=institucion,dc=cu
- LDAP version to use: 3
- Does the LDAP database require login? No
- Special LDAP privileges for root? Yes
- Make the configuration file readable/writeable by its owner only? Yes
- LDAP account for root: cn=admin,dc= institucion,dc=cu
- LDAP root account password: mypassword

Reemplazar el fichero /etc/nsswitch.conf

Reemplazar el fichero /etc/ldap/ldap.conf y cambiar los valores de las opciones siguientes:

- base(Línea # 16)
- binddn(Línea # 17)
- bindpw(Línea # 18)
- nss\_base\_passwd(Línea # 24)
- nss\_base\_shadow(Línea # 25)
- nss\_base\_group(Línea # 26)

Reemplazar el fichero /etc/libnss-ldap.conf y modificar los siguientes parámetros:

- base(Línea # 24)
- rootbinddn (Línea # 53)
- nss\_base\_passwd (Línea # 194)
- nss\_base\_shadow(Línea # 195)
- nss\_base\_group(Línea # 196)

Chequear /etc/libnss-ldap.secret, en este fichero debe aparecer la contraseña que estamos usando, en el caso de esta guía “mypassword”

```
cat /etc/libnss-ldap.secret
```

Ejecutar el comando “dpkg-reconfigure libpam-ldap”:

- LDAP server Uniform Resource Identifier: ldap://127.0.0.1
- Distinguished name of the search base: dc=hkmadavidli,dc=edu,dc=hk
- LDAP version to use: 3
- Make local root Database admin. Yes
- Does the LDAP database require login? No
- LDAP account for root: cn=admin,dc=example,dc=com
- LDAP root account password: CHANGE
- Local crypt to use when changing passwords. MD5

Reemplazar el fichero /etc/pam\_ldap.conf y ajustarle los parámetros:

- base(Línea # 24)
- rootbinddn(Línea # 49)
- nss\_base\_passwd (Línea # 168)
- nss\_base\_shadow(Línea # 169)
- nss\_base\_group(Línea # 170)

Verificar en `/etc/pam_ldap.secret` que se encuentre la contraseña q se está usando, en el caso de esta guía es “mypassword”

```
cat /etc/pam_ldap.secret
```

Reemplazar los ficheros `/etc/pam.d/common-account`, `/etc/pam.d/common-auth`, `/etc/pam.d/common-password` y `/etc/pam.d/common-session` con las versiones pre-configuradas de esta guía.

### **3.10. Nota adicional**

Durante el inicio de Debian udevd buscará algunos usuarios y grupos que no existen, lo que dará lugar a varios mensajes de error. Una solución rápida a esto es crear los usuarios y los grupos en `/etc/passwd` y `/etc/groups`, así no se buscarán en LDAP antes que slapd inicie.

```
addgroup --system nvram
addgroup --system rdma
addgroup --system fuse
addgroup --system kvm
adduser --system --group --shell /usr/sbin/nologin --home /var/lib/tpm tss
```

Ahora, terminada la instalación se debe reiniciar Debian.

## **Conclusiones**

Como resultado de este trabajo se pueden arribar a las siguientes conclusiones:

Se realizó un estudio de la familia de servidores de Windows, revisando sus características y conceptos fundamentales que permiten tener una caracterización de este Sistema Operativo.

La investigación realizada permitió obtener una variante alternativa basada en software libre a los servidores de dominio Windows conocida como Samba de la cual se detallan sus principales parámetros de configuración.

La utilización de un servidor Samba + OpenLdap constituye una buena alternativa libre y económica de los Servidores de Dominio y al Directorio Activo teniendo un alto desempeño, pero aun su proceso de configuración y puesta punto pueden resultar trabajosos.

## Referencias Bibliográficas

- Delprado Guillermo. 2004. Conceptos Fundamentales de Active Directory, Grupos de usuario de Microsoft [Online]. Available: <http://www.mug.org.ar/Infraestructura/ArticInfraestructura/214.aspx> [Accessed 04 April 2010].
- Ayala, Luciana y col. Estructura Interna de Windows NT [Online]. Available: <http://www.monografias.com/trabajos6/esin/esin.shtml> [Accessed 20 April 2010].
- C.V, C. A. A. D. S. A. D. Comparación entre Samba vs Windows 2003 [Online]. Available: [http://www.cad.com.mx/comparacion\\_entre\\_samba\\_vs\\_windows\\_2003.htm](http://www.cad.com.mx/comparacion_entre_samba_vs_windows_2003.htm) [Accessed 06 June 2010].
- DEBIAN #1. Guía de instalación de Debian GNU/Linux [Online]. Available: <http://www.debian.org/releases/stable/i386/index.html.es> [Accessed 25 May 2010].
- DEBIAN #2. Razones para escoger Debian [Online]. Available: [http://www.debian.org/intro/why\\_debian.es.html](http://www.debian.org/intro/why_debian.es.html) [Accessed 30 May 2010].
- DEBIAN #3. 2010. Versiones de Debian [Online]. Available: <http://www.debian.org/releases/index.es.html> [Accessed 10 June 2010].
- GONZÁLEZ, S. G. 2004 Integración de redes con OpenLDAP, Samba, CUPS y PyKota [Online]. Available: <http://www.sergio-gonzalez.com/documentacion.php> [Accessed 15 April 2010].
- MICROSOFT CORPORATION. Ciclo de vida de Soporte Técnico de Microsoft [Online]. Microsoft. Available: <http://support.microsoft.com/lifecycle/?p1=12925> [Accessed 26 April 2010].
- MICROSOFT CORPORATION. Introducción a Active Directory, Microsoft [Online]. Available: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/7c981583-cf41-4e6c-b1f6-5b8863475ede.msp#> [Accessed 2010].
- MICROSOFT CORPORATION. 2007. Novedades de Active Directory [Online]. Available: <http://www.microsoft.com/spain/windowsserver2003/evaluation/overview/technologies/activedirectory.aspx> [Accessed 26 April 2010].
- MICROSOFT CORPORATION. 2007. Windows Server 2008, una nueva plataforma productiva [Online]. Available: <http://www.microsoft.com/latam/technet/articulos/tn/2007/jul-01.msp#> [Accessed 26 April 2010].
- MICROSOFT CORPORATION. 2008. Announcing Windows Server 2008 R2! [Online]. Available: <http://blogs.technet.com/windowsserver/archive/2008/10/28/announcing-windows-server-2008-r2.aspx> [Accessed 26 April 2010].
- MICROSOFT CORPORATION. 2008. Windows Server 2008 Service Pack 2 beta [Online]. Available: <http://blogs.technet.com/windowsserver/archive/2008/10/24/windows-server-2008-service-pack-2-beta.aspx> [Accessed 26 April 2010].
- NOTTINGHAM, C. 2006. R2 - Better than C3-PO [Online]. Available: <http://technet.microsoft.com/en-us/library/bb877978.aspx> [Accessed 26 April 2010].

- NOZAWA, J. M. T. Como configurar una GUI para un Dominio Samba openLDAP en Centos [Online]. Available: <http://www.alcancelibre.org/staticpages/index.php/Samba-LDAP-GUI-LAM-Centos5/print> [Accessed 02 June 2010].
- QUESADA, A. J. D. 2006/07. TUTORIAL AUTENTIFICACIÓN LDAP CONTRA SAMBA [Online]. Available: <http://www.ajduenas.com/wp-content/uploads/2007/07/proyecto-integrado-antonio-jesus-duenas.pdf> [Accessed].
- RANCHAL, J. 2007. Windows Server 2008: anuncio oficial de precios y versiones+ [Online]. Available: [http://www.theinquirer.es/2007/11/14/windows\\_server\\_2008\\_anuncio\\_oficial\\_de\\_precios\\_y\\_versiones.html](http://www.theinquirer.es/2007/11/14/windows_server_2008_anuncio_oficial_de_precios_y_versiones.html) [Accessed Mayo 30 2010].
- RODRÍGUEZ, G. A. 1997. Curso de Windows NT Server 4.
- SAHARON, Y. 2003. Active Directory Security Tips and Practices [Online]. Available: <http://technet.microsoft.com/en-us/library/bb877987.aspx> [Accessed 26 April 2010].
- SAHARON, Y. 2003. Active Directory Services in Windows Server 2003 [Online]. Microsoft. Available: <http://technet.microsoft.com/en-us/library/bb878028.aspx> [Accessed 26 April 2010].
- SARID, T. 2005. Windows Server 2003 Service Pack 1 [Online]. Available: <http://technet.microsoft.com/en-us/library/bb878019.aspx> [Accessed 26 April 2010].
- TANENBAUM, A. S. 1997. Redes de computadoras, Amsterdam.
- WIKIPEDIA FOUNDATION #1, I. 2010. GNU [Online]. Available: <http://es.wikipedia.org/wiki/GNU> [Accessed 26 April 2010].
- WIKIPEDIA FOUNDATION #2, I. 2010. Samba (programa) [Online]. Available: [http://es.wikipedia.org/wiki/Samba\\_\(programa\)](http://es.wikipedia.org/wiki/Samba_(programa)) [Accessed 06 June 2010].
- WIKIPEDIA FOUNDATION #3, I. 2010. Windows 2000 [Online]. Available: [http://es.wikipedia.org/wiki/Windows\\_2000](http://es.wikipedia.org/wiki/Windows_2000) [Accessed 12 April 2010].
- WIKIPEDIA FOUNDATION #4, I. 2010. Windows NT 4.0 [Online]. Available: [http://es.wikipedia.org/wiki/Windows\\_NT\\_4.0](http://es.wikipedia.org/wiki/Windows_NT_4.0) [Accessed 12 April 2010].
- WIKIPEDIA FOUNDATION #5, I. 2010. Windows NT [Online]. Available: [http://es.wikipedia.org/wiki/Windows\\_NT](http://es.wikipedia.org/wiki/Windows_NT) [Accessed 12 April 2010].
- WIKIPEDIA FOUNDATION #6, I. 2010. Windows Server 2003 [Online]. Available: [http://es.wikipedia.org/wiki/Windows\\_Server\\_2003](http://es.wikipedia.org/wiki/Windows_Server_2003) [Accessed 12 April 2010].
- WIKIPEDIA FOUNDATION #7, I. 2010. Windows Server 2008 [Online]. Available: [http://es.wikipedia.org/wiki/Windows\\_Server\\_2008](http://es.wikipedia.org/wiki/Windows_Server_2008) [Accessed 12 April 2010].
- WIKIPEDIA FOUNDATION #8, I. 2009. Windows NT 3.x [Online]. Available: [http://es.wikipedia.org/wiki/Windows\\_NT\\_3.x](http://es.wikipedia.org/wiki/Windows_NT_3.x) [Accessed 12 April 2010].
- WIKIPEDIA FOUNDATION #9, I. 2010. Active Directory [Online]. Available: [http://en.wikipedia.org/wiki/Active\\_Directory](http://en.wikipedia.org/wiki/Active_Directory) [Accessed 12 April 2010].