Universidad Central “Marta Abreu” de Las Villas

Facultad de Matemática, Física y Computación

Trabajo para optar por el Título de

Ingeniero Informático

Propuesta de servicios básicos de redes con software libre

Autor

José Daniel Villar González

Tutores

M.Sc. Manuel Castro Artiles

M.Sc. Samuel A. Rodríguez Beceiro

Santa Clara

Curso 2012-2013

"Año 55 de la Revolución"

Universidad Central “Marta Abreu” de Las Villas

Facultad de Matemática, Física y Computación

Trabajo para optar por el Título de

Ingeniero Informático

Propuesta de servicios básicos de redes con software libre

Autor

José Daniel Villar González (jvillar@uclv.edu.cu)

Tutores

M.Sc. Manuel Castro Artiles (mcastro@uclv.edu.cu)

M.Sc. Samuel A. Rodríguez Beceiro (samuel@ucp.vc.rimed.cu)

Santa Clara

Curso 2012-2013

"Año 55 de la Revolución"

Hago constar que el presente Trabajo para optar por el Título de Ingeniero Informático ha sido realizado en la facultad de Matemática-Física y Computación de la Universidad Central "Marta Abreu" de Las Villas (UCLV) como parte de la culminación de los estudios de Ingeniería Informática, autorizando a que el mismo sea utilizado por la institución para los fines que estime conveniente, tanto de forma total como parcial y que además no podrá ser presentado en eventos ni publicado sin la previa autorización de la UCLV.

_____

Firma del Autor

José Daniel Villar González

Los abajo firmantes, certifican que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y que el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____

Firma del Tutor

M.Sc. Manuel Castro Artiles

_____

Firma del Tutor

M.Sc. Samuel A. Rodríguez Beceiro

PENSAMIENTO

¡Triste época la nuestra! Es más fácil desintegrar un átomo que un prejuicio.

EINSTEIN

Es necesario que surjan nuevas ideas, que los jóvenes tengan el aliciente posible para disentir radicalmente de las estupideces de su época.

B. RUSELL

DEDICATORIA

Dedico este trabajo a:

- Dios, mi amigo fiel e incondicional, quien se ha manifestado de formas increíbles a lo largo de mi vida, ayudándome cuando más lo he necesitado, saber que siempre cuento con Él me hace sentir que no hay obstáculo que no pueda vencer.
- Mis padres, Risel y Daniel por todo su cuidado, apoyo y amor incondicional, los amo con sus defectos y virtudes, son un regalo especial de Dios en mi vida.
- Mis hermanas Ely y Yuly, por estar pendientes de mí, me siento muy afortunado por tenerlas y saber que siempre puedo contar con su apoyo, estoy muy orgulloso de ellas.
- Mis abuelos Ido y Migue, han sido como padres desde hace ya más de 7 años, les debo y agradezco mucho, su ayuda fue fundamental.
- Mi amiga Rachel, antes de conocerla pensaba que tenía muchos amigos, ahora me doy cuenta que esa palabras es más profunda de lo que a veces pensamos, su amistad ha sido un regalo muy especial, le debo mucho.
- Todos mis familiares y amigos, aquellos que de una forma u otra siempre han estado cuando los he necesitado, gracias por todo su apoyo.

AGRADECIMIENTOS

- Gracias a Dios por ser mi sustento, su amor y misericordia han sido infinitos en mi vida, gracias por ser mi amigo fiel.
- Gracias a mi madre, Risel González, mi padre, Daniel Villar, mis hermanas, Elizabeth y Yusleidys, mis cuñados Abdiel y Ariel, mis abuelos, mis primos, tíos y el resto de la familia, gracias por todo su amor.
- Gracias a todos mis tíos, Lesir, Roberto y Amparo, Juan y Mercedes, Eliseo y Baby, mis tías Eliza, María y el Évora, a mi tío Josué y Yanelys, Elías y Nerelys, mi tío Joel, gracias por sus oraciones, su amor y apoyo en todos estos años.
- A mis primos Ronald, Magdalena, Isaac, David, Raquel y Anna, Idalmis gracias por todo tu cariño, a Idania, Ira, Saray, en fin a todos gracias.
- A todos mis amigos, Rachel gracias por ser una hermana durante estos cinco años, pasamos momentos y compartimos cosas que nunca voy a olvidar, gracias por ser tan sincera conmigo, por escucharme y compartir mis problemas, y por todos tus consejos, eres lo máximo.
- Gracias a mis tutores Manuel Castro Artiles y Samuel Rodríguez por su dedicación y apoyo en la realización de este trabajo.
- Gracias a todos mis profesores de la facultad de Matemática, Física y Computación de la Universidad Central de Las Villas, por regalarme todos sus conocimientos de forma humilde y desinteresada.
- Gracias a todas aquellas personas, incluso a las que no conozco y sin saberlo me han ayudado.

Muchas gracias a todos.

Jose D. Villar González

RESUMEN

En la actualidad en Cuba la mayoría de los administradores de red utilizan los sistemas operativos de Microsoft para la gestión de casi todos los servicios de redes. Sin embargo desde abril del 2004 el Ministerio de la Informática y de Comunicaciones (MIC) dispuso la migración progresiva hacia software libre. Uno de los servidores de directorio en software libre más utilizados y que brinda una gran variedad de utilidades es el OpenLDAP que en unión con Samba logran establecer un dominio. Existen diferentes herramientas que permiten la administración del servidor de directorio OpenLDAP de forma visual, sin embargo no permiten explotar todas sus prestaciones y en muchos casos hay que trabajar con línea de comando, provocando rechazo a la migración a software libre.

En el presente trabajo se muestra cómo puede introducirse OpenLDAP y Samba en un ambiente heterogéneo para establecer dominios e integrar recursos en un dominio implementando diferentes servicios utilizando software libre que puede ser utilizado en cualquier empresa. Esa propuesta se hace sobre los servicios de directorios, correo electrónico, acceso a internet y servicios de infraestructura de redes.

ABSTRACT

Today in Cuba most network administrators use Microsoft operating systems to manage almost all network services. However, since April 2004 the Ministry of Informatics and Communications (MIC) ordered the gradual transition to free software. One of the most used directory servers in free software that provides a variety of utilities is OpenLDAP that in conjunction with Samba get to establish a domain. There are different tools for managing OpenLDAP directory server visually, however they do not allow to exploit all of its benefits and often have to work with command line, causing rejection of the migration to free software.

In this paper it is shown as OpenLDAP and Samba can be introduced in a heterogeneous environment to establish domains and integrate resources in a domain, implementing different services using free software that can be used in any company. This proposal is made on directory services, email, internet access, and network infrastructure services.

ÍNDICE

INTRODUCCIÓN

La información en todas sus formas se ha convertido en un activo de muy alto valor, es el recurso económico básico que genera mayor capital por lo que es necesario protegerla y asegurarla para garantizar su integridad, confidencialidad y disponibilidad. La utilización de computadoras en el manejo de la información como elemento indispensable en la actualidad ha permitido incrementar el uso de aplicaciones electrónicas como correo, comercio electrónico, transacciones y dinero electrónico, firmas y certificados digitales, acceso a bancos de datos y otras aplicaciones.

El conocimiento y manejo de distintas técnicas, procedimientos y herramientas de administración es una necesidad mundial y en especial de las empresas cubanas que cada día se incorporan con mayor fuerza al trabajo con sistemas informáticos en redes ofreciendo diversos servicios a sus usuarios. Una técnica muy utilizada actualmente consiste en utilizar máquinas virtuales para implementar los sistemas y probarlos antes de que entren en producción. Esto permite familiarizar a los administradores con los servicios que se ofrecen y ajustarlos a los requerimientos de la empresa antes de que los usuarios tengan acceso a los mismos, de igual forma se prueban diferentes herramientas y configuraciones que se desean utilizar.

El costo del software propietario obliga a que muchos países procuren vías alternativas en su desarrollo realizando la migración hacia el software libre y Cuba se encuentra enfrascada en este proceso que se desarrolla de manera progresiva dando pasos cada vez más orientados a la sustitución de aplicaciones y sistemas completos con software libre, a la vez que incentiva el desarrollo de soluciones propiamente cubanas para lo cual se han creado diversos centros que se encargan de este proceso a diferentes niveles y con diferentes responsabilidades.

Planteamiento del problema

En la actualidad se ha orientado el proceso de migración hacia software libre como la política para el país, este proceso se ve limitado por la falta de preparación de gran parte del personal dedicado a manejo de redes. Existen administradores calificados para realizar este trabajo de manera natural pero hay un alto porcentaje de administradores que no están aptos para enfrentar este proceso debido a su preparación y al poco o nulo acceso a la información por lo que es importante ofrecer una guía que les sirva como ayuda para poder tener operativo un dominio y sus servicios básicos en el menor tiempo posible.

Para dar respuesta a este problema es necesario trabajar en los servicios que se ofrecen normalmente en una empresa, utilizando software confiable para cada aplicación y los sistemas operativos disponibles en el país.

Objetivo general

Proponer una guía para implementar dominios y un grupo de servicios básicos necesarios, empleando herramientas de software libre y gratis, que garanticen el correcto funcionamiento y seguridad de una red de computadoras en el ámbito empresarial.

Objetivos específicos

Para el cumplimiento de este objetivo se ha definido un conjunto de objetivos específicos que se relacionan a continuación.

a) Definir el sistema operativo a utilizar y los servicios básicos necesarios para una empresa.
b) Analizar variantes de creación de dominios utilizando software libre gratis.
c) Implementar los servidores por medio de máquinas virtuales, realizando la simulación del sistema completo y comprobando el correcto funcionamiento de los servicios.

Preguntas de investigación

1) ¿Qué tipos de sistema operativos deben utilizarse de acuerdo a las necesidades y el hardware disponible en la empresa?
2) ¿Qué servicios de red mínimos se necesitan para comenzar la migración a software libre?
3) ¿Qué variante de implementación del dominio es la adecuada teniendo en cuenta principalmente la experiencia de los administradores?
4) ¿Cómo se garantiza un nivel mínimo adecuado de seguridad?

Justificación y viabilidad de la investigación

Este trabajo es necesario dada la situación general en el país y especialmente en la provincia con el proceso de migración al software libre.

Para realizar este trabajo se necesita montar varios sistemas y probarlos antes de instalar los servidores de producción, esto puede hacerse utilizando máquinas virtuales con las configuraciones deseadas en la empresa para poder monitorear el comportamiento y determinar si cumple con los requerimientos.

Hipótesis de investigación

Con los equipos disponibles generalmente en la empresa destinados a la administración es posible lograr una red propia con un ambiente de trabajo heterogéneo que satisface los requerimientos de la empresa.

DISEÑO DE LA TESIS

Este trabajo está estructurado en tres capítulos, a continuación se presenta un resumen de los mismos:

En el Capítulo I se hace referencia al desarrollo de Linux y se ofrece una definición de los servicios básicos que se ofrecen regularmente en una red.

El Capítulo II aborda propuestas de implementación de los servicios que garanticen la interoperabilidad en un ambiente heterogéneo utilizando OpenLDAP como centro vital de organización y se realiza la caracterización de los servicios con diferentes herramientas.

Además define las aplicaciones que se necesitan instalar, la distribución de los servicios en los servidores y la seguridad de las mismas.

En el Capítulo III se hace un análisis de los resultados de la encuesta aplicada a varios administradores de red. Además muestra cómo se hace la integración de sistemas heterogéneos en el dominio y se valora el proceso de migración. También muestra en forma de ejemplo el servicio de correo electrónico funcionando.

En los Anexos se encuentran algunas guías para implementar los dominios se exponen los detalles de algunas aplicaciones y sus correspondientes archivos de configuración.

CAPÍTULO I: SERVICIOS BASICOS DE REDES

1.1 La administración de redes de computadoras

La administración de redes se ha convertido en un aspecto crítico, especialmente en redes de computadores con sistemas operativos heterogéneos, situación en la que se encuentran actualmente la mayoría de las empresas cubanas enfrascadas en el proceso de migración.

Se define como **administración** al monitoreo, control y coordinación de los recursos de la computadora, los recursos usados en la conexión y comunicación de las mismas, y las aplicaciones usadas en esas computadoras. [1]

El modelo de administración más utilizado en la pequeña y mediana empresa es el de **administración jerárquica o centralizada**. En este modelo la administración es realizada desde un solo punto, conocido como nodo de administración.

La administración se realiza desde sistemas operativos llamados servidores que en el caso de ser propietarios son muy costosos como los sistemas de Microsoft pero el mundo Linux ha desarrollado distribuciones gratuitas que en estos momento tienen un grado adecuado de robustez, funcionalidad y adaptabilidad a varios entornos que los ha convertido en la principal alternativa para sistemas propietarios como Unix y los sistemas operativos de Microsoft, IBM, Hewlett-Packard, etc. convirtiéndose así en su segunda década de existencia en una opción viable como plataforma para servidores de aplicaciones.

1.2 Estudio No. 1 Titulado: “Tendencias de la adopción de Linux en el 2012

Según informe ***Titulado “Tendencias de la adopción de Linux en el 2012***: publicado en enero del año 2012, por *Linux Foundation* la situación actual ofrece un panorama aún más prometedor para Linux (una copia del informe completo se puede descargar desde el sitio de la *Linux Foundation*) [2] debido a que cada vez se incorpora más el Linux en misiones críticas como es el mantener un dominio y ofrecer servicios confiables en las grandes empresas.

La encuesta de *la Linux Foundation* se llevó a cabo en colaboración con *Yeoman Technology Group*. Aunque se recibieron respuestas de casi 1.900 personas, el informe se centra en los datos de las empresas más grandes del mundo y las organizaciones de gobierno, representadas por 428 encuestados en organizaciones con ingresos anuales de US$ 500 millones o más, y con más de 500 empleados.

De las numerosas distribuciones de Linux, Ubuntu es actualmente una de las más famosas, por la manera en que trabaja y por haber sabido combinar flexibilidad, estabilidad, usabilidad y solidez. Está basada en Debían y esto le da ventaja por la gran cantidad de paquetes disponibles. Con el paso de los años se ha convertido en el Sistema Operativo libre más usado, han ganado experiencia y se encuentra en una etapa de madurez que les ha permitido experimentar con éxito en el campo de los servidores. Marcan muchas pautas y su influencia en otras distribuciones es innegable.

1.3 Servicios básicos.

Independientemente de las dimensiones y requerimientos de una empresa, su red debe proporcionar un conjunto de servicios básicos. Por ejemplo, tanto la gran empresa como la PYME (Pequeña Y Mediana Empresa), necesitan de un grupo de servicios mínimos (básicos) que posibiliten la conectividad dentro y fuera de la red local, el control de los recursos y el acceso al correo e internet.

En este grupo de servicios tenemos:

a. Servicios de Infraestructura: DNS, DHCP
b. Servicios de Directorio: Samba y LDAP integrados.
c. Servicio de correo electrónico.
d. Servicio de acceso a internet.

1.3.1 Servidor DNS (Domain Name System)

Domain Name System (Sistema de Nombre de Dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres

inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de aplicaciones de cada dominio (Vea figura 1.1). [3]

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio HTTP de softlib.uclv.edu.cu es 10.12.1.103, la mayoría de la gente llega a este equipo especificando http://softlib.uclv.edu.cu y no la dirección IP. Además de ser fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

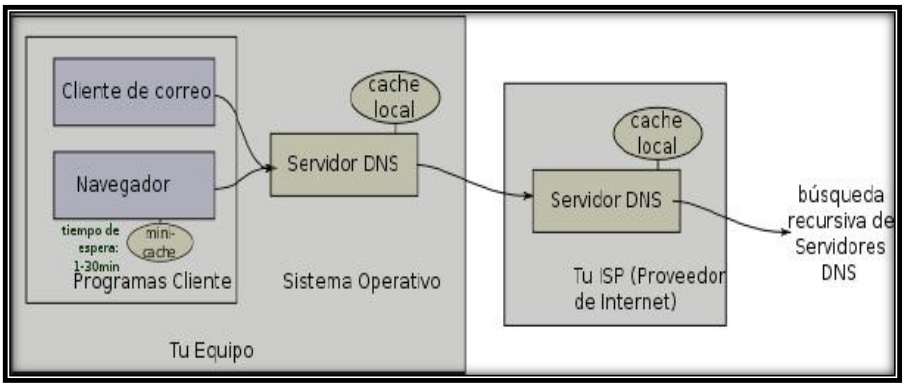


Figura 1.1: Servidor DNS

Roles de Servidor de DNS:

La tarea principal del servidor DNS es obtener el número IP de un ordenador o dominio a partir de su nombre. A continuación se muestra los tres roles fundamentales del servidor DNS:

- Resolución de nombres.
- Resolución inversa de direcciones.
- Resolución de servidores de correo y otros servicios.

Existen varios tipos de servidores de DNS como Bind, PowerDNS, djbdns y todos trabajan sobre el puerto 53 protocolo TCP/UDP.

Existen cuatro formas de implementar un servidor DNS:

- **Maestro:** Es el servidor responsable para determinada zona DNS y se encarga de la resolución de nombres dentro de esa zona donde es la autoridad.
- **Esclavo:** Este tipo de servidor sirve como espejo de un servidor DNS Maestro, recibe sus actualizaciones del maestro y se utiliza para aliviar la carga de trabajo de los servidores maestros.
- **Caché:** Este tipo de servidor se utiliza dentro de una red local, cuando se hace una consulta a un servidor DNS Caché y no contiene la resolución envía una petición a un DNS Maestro y la resolución quedará guardada en el caché del DNS local hasta que expire el tiempo de vida.
- **Reenvío:** Reenvía las peticiones a una lista específica de servidores DNS para la resolución de nombres.

Un servidor DNS puede ser de varios tipos configurados en el mismo servidor DNS.

1.3.2 Servidor DHCP

Un servidor *Dynamic Host Configuration Protocol* (DHCP) asigna dinámicamente las direcciones IP y otras configuraciones de una red determinada a otros ordenadores clientes que están conectados a la red. Esto simplifica la administración de la red y hace que la conexión de nuevos equipos a la red sea más fácil y menos propensa a errores. Todas las direcciones IP de todos los equipos se almacenan en una base de datos que reside en un servidor (Vea figura 1.2). [4]

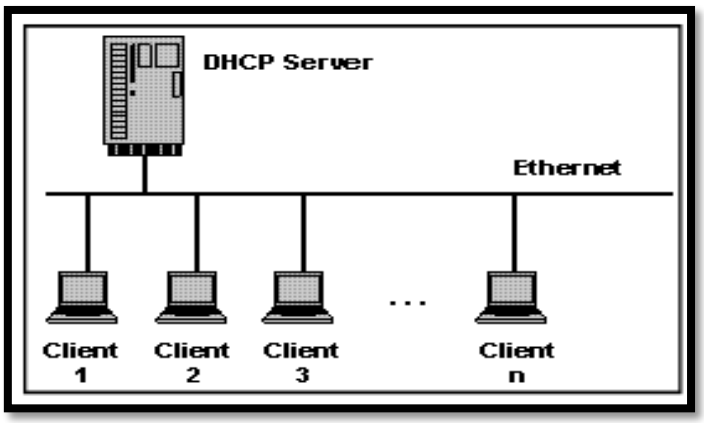


Figura 1.2: Red con servidor DHCP

Un servidor DHCP puede proporcionar los ajustes de configuración utilizando dos métodos:

- **Rango de Direcciones**:
  Este método se basa en la definición de un grupo de las direcciones IP para los clientes DHCP (también llamado IP address pool) que suministran sus propiedades de configuración de forma dinámica según lo soliciten los ordenadores clientes. Cuando un cliente DHCP ya no está en la red durante un periodo determinado, la configuración vence y la dirección IP se libera del pool para su uso por otros clientes DHCP.

- **Dirección MAC**:
  Este método se basa en utilizar el protocolo DHCP para identificar la dirección de hardware única de cada tarjeta de red conectada a la red y luego asignarle una configuración fija, cada vez que el cliente realiza una petición al servidor DHCP recibe la misma asignación.

1.3.3 Servicio de Directorio

Un **servicio de directorio** es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red.

Además, los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos.

El servicio de directorio proporciona la interfaz de acceso a los datos que se contienen en unos o más espacios de nombre de directorio. La interfaz del servicio de directorio es la encargada de gestionar la autenticación de los accesos al servicio de forma segura, actuando como autoridad central para el acceso a los recursos de sistema que manejan los datos del directorio. Como base de datos, un servicio del directorio está altamente optimizado para lecturas y proporciona alternativas avanzadas de búsqueda en los diferentes atributos que se puedan asociar a los objetos de un directorio. Los datos que se almacenan en el directorio son definidos por un esquema extensible y modificable. Los servicios de directorio utilizan un modelo distribuido para almacenar su información y esa información generalmente está replicada entre los servidores que forman el directorio. [5]

1.3.3.1 Desarrollos de servicios de directorio

La gran mayoría de implementaciones están basadas en el estándar X.500, que posteriormente fue la base de LDAP, pero utilizando la pila TCP/IP en vez de usar el modelo OSI, adquiriendo especial relevancia en internet.

Existen numerosas formas de implementación de servicios de directorio de diferentes compañías. Algunos son: [6]

- NIS *Network Information Service* protocolo, nombrado originalmente como Páginas Amarillas, implementación de Sun Microsystems en un servicio de directorio para redes de entorno UNIX. (Sun, a principios del 2000, se unió a iPlanet, alianza de Netscape y desarrolló la base de LDAP, servicio de directorio que formó parte de Sun ONE, la empresa que es ahora Sun Java Enterprise).

- eDirectory, desarrollado por Novell, es un servicio de directorio que soporta múltiples arquitecturas incluyendo Windows, NetWare, Linux, e incluyendo algunas distribuciones de Unix. Se ha utilizado durante tiempo para la administración de usuarios, gestión de configuraciones y gestión de software. eDirectory se ha desarrollado como componente central en una gama más amplia de productos para la gestión de identidad. Fue conocido previamente como servicios de directorio de Novell.

- Servidor de directorio de Red Hat: Red Hat lanzó un servicio de directorio, que adquirió de "*Netscape Security Solutions* de AOL", el cual funcionaba como producto comercial, bajo Red Hat Enterprise Linux denominado como servidor de directorio de Red Hat, como parte del núcleo de Fedora.

- Active Directory (AD): El servicio del directorio de Microsoft, es el directorio que se incluye en las versiones de los sistemas operativos Windows Server 2000 y sus sucesores. AD es una implementación propietaria (creada por Microsoft) de los Servicios de Directorio, y proporciona una manera de compartir información entre recursos y usuarios de la red. Además de proporcionar una fuente centralizada para esa información, AD también funciona como autoridad de seguridad centralizada de Autenticación para la red siendo el más avanzado en estos momentos.

  AD combina capacidades que tradicionalmente se hallaban en sistemas separados y especializados de directorio, como integración simplificada, gestión y seguridad de los recursos de la red.

- 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.

1.3.4 Servidor de Correo Electrónico

El servicio de correo electrónico consta de tres agentes o componentes bien diferenciadas (Vea figura 1.3). Estos son:

1.3.4.1 MUA (Mail User Agent)

MUA es un programa que permite leer y escribir correos. Suelen tener muchas funcionalidades que superan la estricta lectura y composición de mensajes, como el mantenimiento de libretas de direcciones, gestión de anexos (*attachments*), gestión de múltiples carpetas para organizar el correo, filtros de correo para borrarlo, responderlo, o redirigirlo a carpetas determinadas, todo ello automáticamente y en función de las características del mensaje, etc. Algunos nombres habituales de MUAs son: mail, elm, pine, kmail (entorno KDE), Netscape Messenger, Microsoft Outlook Express, Qualcomm Eudora (en Windows), PegasusMail (en Windows) etc.

1.3.4.2 MTA (Mail Transport Agent)

Es un programa encargado de recoger mensajes y enviarlos, comunicando para ello con otros MTA según sea preciso. Lo normal es que funcione como servicio (es decir, de modo continuo, esperando peticiones de los MUAs o de otros MTAs y atendiéndolas). El MTA más famoso y utilizado es Sendmail; otros MTAs son Postfix, QMail etc. Además, productos de groupware como Microsoft Exchange, Lotus Domino Server, Novell Groupwise o Netscape Messaging Server incluyen MTAs.

1.3.4.3 MDA (Mail Delivery Agent)

Se encarga de copiar los mensajes desde el servidor de correo hasta el buzón de usuario. MDA es el encargado de realizar la entrega de correos a los MUA. Algunos de los más usados son: Qpopper, Courier, Cyrus, Maildrop (Unix) y Dovecot.

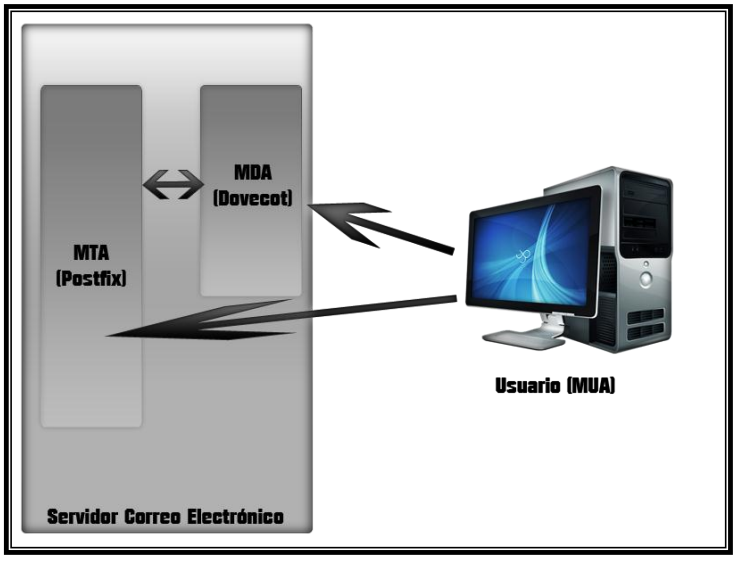


Figura 1.3: Los tres componentes del servicio de correo

1.3.4.4 Protocolos de Correo Electrónico

1.3.4.4.1 Protocolo SMTP

Simple Mail Transfer Protocol (SMTP) en español, Protocolo Simple de Transferencia de Correo, es un protocolo de red de la capa de aplicación, basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres. Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo. El número va dirigido a un procesado automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea. En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión.

1.3.4.4.2 Protocolo POP

Post Office Transport Protocol (POP), se utiliza para obtener/descargar los mensajes guardados en el servidor al usuario. POP3 está diseñado para recibir correo, no para enviarlo; le permite a los usuarios con conexiones intermitentes o muy lentas (tales como las conexiones por módem), descargar su correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados. La mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de manera tal que, un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta. En contraste, el protocolo IMAP permite los modos de operación conectado y desconectado.

Los clientes de correo electrónico que utilizan IMAP dejan por lo general los mensajes en el servidor hasta que el usuario los elimina directamente. Esto y otros factores hacen que la operación de IMAP permita a múltiples clientes acceder al mismo buzón de correo. La mayoría de los clientes de correo electrónico soportan POP3 o IMAP; sin embargo, solo unos cuantos proveedores de internet ofrecen IMAP como valor agregado de sus servicios. [7]

1.3.4.4.3 Protocolo IMAP

Internet Message Access Protocol, o su acrónimo IMAP, es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP, que es el otro protocolo empleado para obtener correo desde un servidor. Por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP. IMAP, tiene la misma finalidad que POP aunque funciona de forma diferente; de este protocolo se pueden observar algunas ventajas, como tiempos de respuesta más rápidos, acceso remoto a los mensajes, accesos simultáneos a múltiples clientes, vigilancia en el estado del mensaje, agilidad en las búsquedas, entre otras ventajas sobre el protocolo POP.

1.3.4.5 Funcionamiento de los Servidores de Correo Electrónico

Un servidor de correo electrónico debe constar en realidad de dos servidores el SMTP encargado de enviar y recibir mensajes, y un servidor POP/IMAP, que será el que permite a los usuarios obtener sus mensajes; para esto los usuarios se sirven de clientes, es decir, programas que implementan un protocolo POP/IMAP (Vea figura 1.4), los que en algunas ocasiones se ejecutan en la máquina del usuario (como son los casos de Evolution y Outlook). Sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del usuario; es el caso de los clientes vía web. [8]

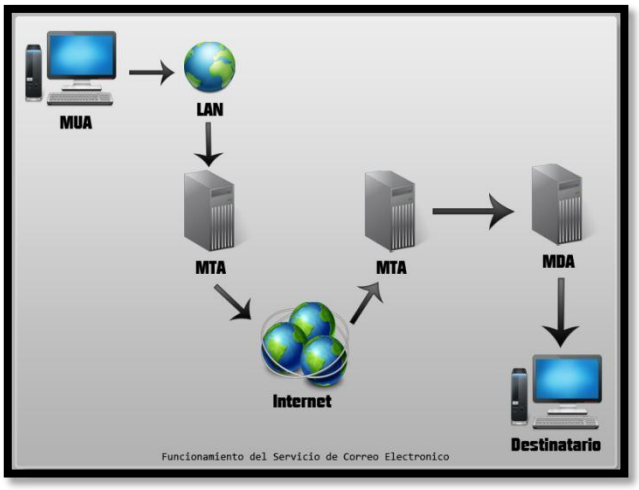


Figura 1.4: Proceso en el envió de un correo Electrónico

1.3.4.6 Aspectos a tener en cuenta al instalar un servidor de correo electrónico:

- ✓ Volumen de correos que van a gestionarse.
- ✓ Configurar otros servicios como:
  - DNS: Es esencial definir los registros MX para definir cuál es el servidor SMTP.
  - Definir reglas en el firewall (permitir el tráfico en MDA/MTA).
- ✓ Crear buzones de correo siguiendo determinadas políticas (nombre de la cuenta).
- ✓ Disponer de una máquina de *backup.*

1.3.5 Servidor de acceso a internet (Proxy)

El término en ingles «Proxy» tiene un significado muy general y al mismo tiempo ambiguo, aunque invariablemente se considera un sinónimo del concepto de «Intermediario». Se suele traducir, en el sentido estricto, como delegado o apoderado.

Un **Servidor Intermediario** se define como un dispositivo o software que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red (Vea figura 1.5). [9, 10] Durante el proceso ocurre lo siguiente:

- Cliente se conecta a un Servidor Proxy.
- Cliente solicita una conexión, archivo u otro recurso, disponible en otro servidor.
- Servidor Intermediario proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.
    - En algunos casos el Servidor Intermediario puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los Servidores Proxy generalmente trabajan simultáneamente como muro cortafuegos, operando en el Nivel de Red actuando como filtro de paquetes, como en el caso de iptables, o bien operando en el Nivel de Aplicación, controlando diversos servicios, como es el caso de TCP Wrapper. Dependiendo del contexto, el muro cortafuegos también se conoce como BPD o Border Protection Device o simplemente filtro de paquetes.

Una aplicación común de los Servidores Proxy es funcionar como caché de contenido de Red (principalmente HTTP), proporcionando en la proximidad de los clientes, un caché de páginas y archivos disponibles a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un **URL** (*Uniform Resource Locator*), el Servidor Intermediario busca el resultado del URL dentro del caché. Si éste es encontrado, el Servidor Intermediario responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el Servidor Intermediario lo traerá desde un servidor remoto, entregándolo al cliente

que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de respuestas a solicitudes (hits) (ejemplos: **LRU**, **LFUDA** y **GDSF**).

Los Servidores Proxy para contenido de Red (Web Proxies) también pueden actuar como filtros del contenido servido, aplicando políticas de censura de acuerdo a criterios arbitrarios.

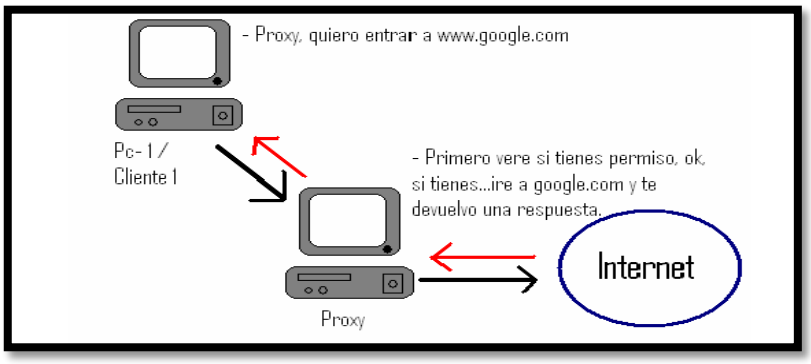


Figura 1.5: Como funciona el proxy

1.3.5.1 Ventajas de un servidor proxy: Un Proxy hace posible:

- **Control**: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- **Ahorro**. Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
- **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

- **Anonimato**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos.

1.4 Zentyal, servidor Linux para pequeñas y medianas empresas

Zentyal (anteriormente conocido como **eBox Platform**) es un servidor de red unificada de código abierto (o una plataforma de red unificada) para las pequeñas y medianas empresas (PYMEs). Zentyal puede actuar gestionando la infraestructura de red, como puerta de enlace a Internet (Gateway), gestionando las amenazas de seguridad (UTM), como servidor de oficina, como servidor de comunicaciones unificadas o una combinación de estas. Además, Zentyal incluye un marco de desarrollo para facilitar el desarrollo de nuevos servicios basados en Unix.

El código fuente del proyecto está disponible bajo los términos de la Licencia Pública General de GNU, así como bajo varias licencias privativas. La empresa española eBox Technologies S.L. es el propietario y patrocinador de Zentyal y posee el copyright del código fuente.

Zentyal (eBox Platform) empezó como un proyecto colaborativo entre dos empresas y fue publicado como un proyecto de código abierto por primera vez en 2005. El 16 de noviembre de 2006 Zentyal (eBox Platform) fue oficialmente aprobado como proyecto NEOTEC, recibiendo fondos públicos del CDTI (organización pública española bajo el Ministerio de Industria, Comercio y Turismo) para completar el desarrollo de la versión 1.0. Zentyal (eBox Platform) fue incluido por primera vez en Ubuntu en 2007, en el Gutsy Gibbon Tribe 3, la tercera versión alfa de Ubuntu 7.10. La primera versión candidata a definitiva de Zentyal (eBox Platform 1.0), fue publicada en 2008. Actualmente se encuentra en la versión 3.0. [11]

1.4.1 Las PYMEs y las TICs

Alrededor del **99% de las empresas del mundo** son pymes, y generan más de la mitad del PIB mundial. Las pymes buscan continuamente fórmulas para **reducir costes** y **aumentar su productividad**, especialmente en tiempos de crisis como el actual. Sin embargo, suelen operar bajo **presupuestos muy escasos** y con una **fuerza laboral limitada**. Estas circunstancias hacen muy difícil ofrecer soluciones adaptadas a las pymes que les aporten

importantes beneficios, manteniendo al mismo tiempo las inversiones necesarias y los costes operacionales dentro de su presupuesto.

Por lo general, las soluciones corporativas disponibles en el mercado se han desarrollado pensando en las grandes corporaciones, por lo que requieren inversiones considerables en tiempo y recursos y demandan un alto nivel de conocimientos técnicos.

En el mercado de los servidores, esto ha significado que hasta ahora las pymes han dispuesto de pocas opciones donde elegir, consistentes por lo general en soluciones sobredimensionadas a sus necesidades reales, complejas de gestionar y con elevados costes de licencias.

En este contexto parece razonable considerar a **Linux** como una alternativa más que interesante como servidor para pymes, puesto que técnicamente ha demostrado una **calidad** y nivel funcional muy elevados y su **precio** de entrada es muy competitivo. Sin embargo, la presencia de *Linux* en entornos de pyme es testimonial y su crecimiento relativamente reducido. ¿Cómo es posible explicar estos datos?

Creemos que la razón es sencilla: para que un servidor de empresa se adapte a un entorno de pyme necesita que sus distintos componentes estén bien integrados entre sí y que sean sencillos de administrar. Así mismo, los proveedores de servicios TIC para pymes también precisan de soluciones que requieran poco tiempo en despliegue y mantenimiento para poder ser competitivos, y las tradicionales distribuciones de Linux para servidor no cumplen con estas premisas.

1.4.2 Zentyal servidor Linux para PYMEs

Zentyal [11] se desarrolló con el objetivo de **acercar Linux a las pymes** y permitirles aprovechar todo su potencial como servidor de empresa. Es la alternativa en código abierto a los productos de Microsoft para infraestructura TIC en las pymes (Windows Small Business Server, Windows Server, Microsoft Exchange, Microsoft Forefront...) y está basado en la popular distribución *Ubuntu*. Zentyal permite a profesionales TIC administrar todos los servicios de una red informática, tales como el acceso a Internet, la seguridad de la red, la compartición de recursos, la infraestructura de la red o las comunicaciones, de forma sencilla y a través de **una única plataforma**.

Durante su desarrollo se hizo un especial énfasis en la usabilidad, creando una **interfaz intuitiva** que incluye únicamente aquellas funcionalidades de uso más frecuente, aunque también dispone de los medios necesarios para realizar toda clase de configuraciones avanzadas. Otra de las características importantes de Zentyal es que todas sus funcionalidades están estrechamente integradas entre sí, **automatizando la mayoría de las tareas** y ahorrando tiempo en la administración de sistemas. (Vea figura 1.6)

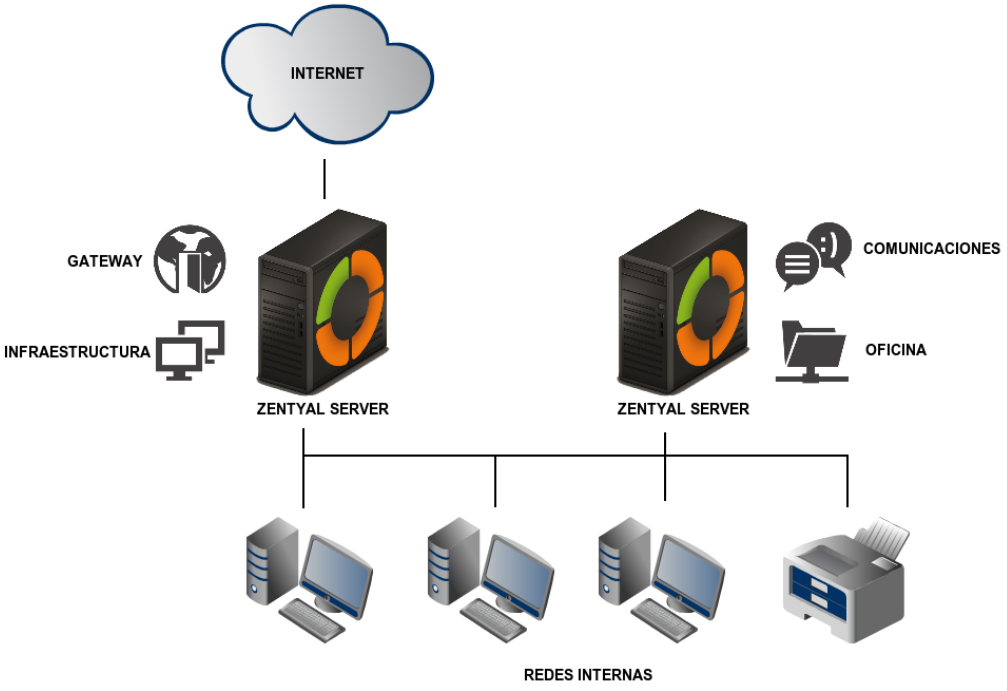


Figura 1.6: Ejemplo de un despliegue con Zentyal en diferentes roles

Teniendo en cuenta que el 42% de los fallos de seguridad y el 80% de los cortes de servicio en una empresa se deben a errores humanos en la configuración y administración de los mismos [12], el resultado es una solución no sólo más **sencilla** de manejar sino también más **segura y fiable**. En resumen, además de ofrecer importantes ahorros, Zentyal mejora la seguridad y disponibilidad de los servicios en la empresa.

El desarrollo de Zentyal se inició en el año 2004 con el nombre de *eBox Platform* y actualmente es una solución consolidada de reconocido prestigio que integra **más de 30 herramientas** de código abierto para la administración de sistemas y redes en una sola tecnología. Zentyal está incluido en *Ubuntu* desde el año 2007, desde el año 2012 las

ediciones comerciales están oficialmente respaldadas por Canonical - la empresa detrás del desarrollo y comercialización de Ubuntu.

Hoy en día hay ya decenas de miles de instalaciones activas de Zentyal, principalmente en América y Europa, aunque su uso está extendido a prácticamente todos los países, siendo Estados Unidos, Alemania, España, Brasil y Rusia los que cuentan con más instalaciones. Zentyal se usa principalmente en pymes, pero **también en otros entornos** como centros educativos, administraciones públicas, hospitales o incluso en instituciones de alto prestigio como la propia *NASA*.

El desarrollo del servidor Zentyal está financiado por Zentyal S.L. Zentyal es un servidor Linux completo que se puede usar de forma gratuita sin soporte técnico y actualizaciones, o con soporte completo por una cuota mensual muy asequible (Vea figura 1.7). Las ediciones comerciales están dirigidas a dos tipos de clientes claramente diferenciados. Por un lado la **Edición Small Business** está dirigida a pequeñas empresas con una infraestructura TIC relativamente sencilla y la *Edición Enterprise* está dirigida a pequeñas y medianas empresas.

Las ediciones comerciales del servidor Zentyal dan acceso a los siguientes servicios y herramientas:

- **Soporte técnico completo** por el Equipo de Soporte de Zentyal
- **Soporte oficial de Ubuntu/Canonical**
- **Actualizaciones de software y de seguridad**
- **Plataforma de monitorización y gestión remota** de servidores y escritorios
- **Recuperación de desastres**
- **Proxy HTTPS**
- **Múltiples administradores del servidor**

Así mismo Zentyal S.L. ofrece los siguientes servicios comerciales en la nube que pueden ser usados integrados a las ediciones comerciales del servidor Zentyal o de forma independiente:

- **Correo electrónico en la nube**
- **Compartición corporativa de ficheros**

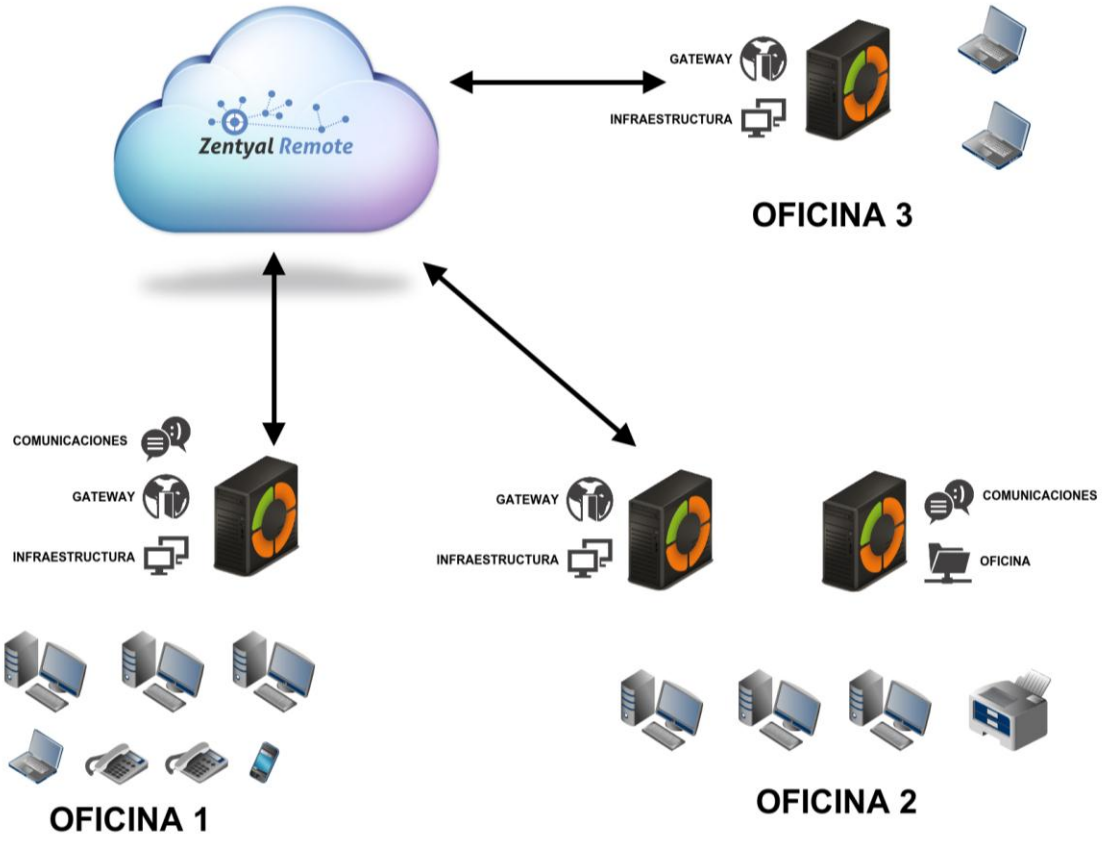


Figura 1.7: Una infraestructura de red profesional con un coste mensual asequible

1.4.3 Requisitos de hardware

Zentyal funciona sobre hardware estándar arquitectura x86 (32-bit) o x86_64 (64-bit). Sin embargo, es conveniente asegurarse de que Ubuntu Precise 12.04 LTS (Kernel 3.2.0) es compatible con el equipo que se vaya a utilizar. Se debería poder obtener esta información directamente del fabricante. De no ser así, se puede consultar en la lista de compatibilidad de hardware de Ubuntu Linux [13], en la lista de servidores certificados para Ubuntu 12.04 LTS o buscando en Google.

Los requerimientos de hardware para un servidor Zentyal dependen de los módulos que se instalen, de cuántos usuarios utilizan los servicios y de sus hábitos de uso.

Algunos módulos tienen bajos requerimientos, como Cortafuegos, DHCP o DNS, pero otros como el Filtrado de correo o el Antivirus necesitan más memoria RAM y CPU. Los módulos

de Proxy y Compartición de ficheros mejoran su rendimiento con discos rápidos debido a su intensivo uso de E/S.

Para un servidor de uso general con los patrones de uso normales, los requerimientos siguientes serían los mínimos recomendados:

Perfil de Zentyal	Usuarios	CPU	Memoria	Disco	Tarjetas de red
Puerta de acceso	<50	P4 o superior	2G	80G	2 ó más
	50 ó más	Xeon Dual core o superior	4G	160G	2 ó más
Infraestructura	<50	P4 o superior	1G	80G	1
	50 ó más	P4 o superior	2G	160G	1
Oficina	<50	P4 o superior	1G	250G	1
	50 ó más	Xeon Dual core o superior	2G	500G	1
Comunicaciones	<100	Xeon Dual core o equivalente	4G	250G	1
	100 ó más	Xeon Dual core o equivalente	8G	500G	1

Tabla de requisitos Hardware

Si se combina más de un perfil se deberían aumentar los requerimientos. Si se está desplegando Zentyal en un entorno con más de 100 usuarios, debería hacerse un análisis más detallado, incluyendo patrones de uso, tras un benchmarking y considerando estrategias de alta disponibilidad.

1.5 Conclusiones parciales del capítulo

En este capítulo hemos presentado algunos servicios de redes que consideramos básicos, necesarios y minimales. Básicos porque son la base de muchos otros servicios. Necesarios porque garantizan la conectividad y consistencia de la red y minimales porque son el conjunto mínimo de servicios que garantiza la conectividad dentro de la LAN y el acceso a correo electrónico e internet como forma imprescindibles de comunicación y colaboración para la empresa moderna. Se hace un resumen de cada servicio y sus características más relevantes. Hemos presentado a Zentyal como un posible sustituto de los servidores Windows para las PYMEs que ofrece un ambiente de trabajo gráfico al que están acostumbrados la mayoría de los administradores y con un alto nivel de integración en sus aplicaciones tratando de emular el comportamiento de los servidores de Microsoft.

CAPÍTULO II: IMPLEMENTACIÓN DE LOS SERVICIOS EN MÁQUINAS VIRTUALES

2.1 Introducción

Muchos países, Cuba entre ellos, han adoptado el uso de las distribuciones Linux, específicamente Debian y Ubuntu, debido a su estabilidad y la disponibilidad de sus repositorios, para facilitar la migración hacia software libre. Por este motivo, en este trabajo se ha seleccionado como sistema operativo a la versión de Linux, **Ubuntu Server 12.04 LTS**.

El trabajo en la red con el sistema Ubuntu junto con clientes Windows implica la oferta e integración de los servicios comunes a los entornos Windows. Estos servicios ayudan en la compartición de datos e información entre los equipos y usuarios implicados en la red, y pueden clasificarse en tres grandes categorías de funcionalidades:

- Compartir impresoras y archivos.
- Servicios de Directorio.
- Autentificación y acceso.

Afortunadamente, un sistema Ubuntu puede proporcionar tales facilidades a clientes Windows y compartir recursos de red con ellos. Una de las principales piezas de software que incluye su sistema Ubuntu para trabajar con redes Windows es el paquete de herramientas y aplicaciones de servidor Samba (SMB).

2.2 Ubuntu Server 12.04 LTS

Ubuntu es un sistema operativo mantenido por Canonical y la comunidad de desarrolladores. Utiliza un núcleo Linux, y su origen está basado en Debian. Ubuntu está orientado al usuario novel y promedio, con un fuerte enfoque en la facilidad de uso y mejorar la experiencia de usuario. Está compuesto de múltiples programas normalmente distribuidos bajo una licencia libre o de código abierto. Las estadísticas web sugieren que el porcentaje de mercado de Ubuntu dentro de "distribuciones Linux" es de aproximadamente 49%, y con una tendencia a subir como servidor web. Y un importante incremento activo de 20 millones de usuarios a fines de 2011. [14]

Para realizar este trabajo se usa como sistema operativo la versión de Linux **Ubuntu Server 12.04 LTS**.

Ya que uno de los servicios básicos más importantes es el servicio de directorio, es necesario contar al menos con un servidor que sirva como controlador principal de dominio (PDC). Es recomendable tener al menos otro servidor que sirva como respaldo (*backup*) del PDC, a este se le denomina controlador secundario del dominio (BDC).

PDC (*Primary Domain Controller*)

Para establecer un dominio, se precisa al menos de un sistema como controlador principal que es el encargado de mantener la base de datos de cuentas de usuario, recursos del dominio, así como de las listas de control de acceso. Es el servidor más importante al tener la copia del directorio donde pueden realizarse escrituras.

BDC (*Backup Domain Controller*)

Por cuestiones de seguridad y rendimiento es aconsejable tener al menos otro servidor que sirva de *backup* del PDC. Este servidor llamado *Backup Domain Controller* mantiene una copia del árbol de directorio del dominio de solo lectura. El concepto de Controlador secundario o *backup* fue eliminado en el ambiente Windows a partir del lanzamiento del SO Windows Server 2003, pero aún se mantiene con las actuales implementaciones de Samba en el ambiente Linux.

2.3 Herramientas utilizadas para la virtualización de los servidores

En el trabajo se utilizó *ORACLE VirtualBox versión 4.1.14* (Vea figuras 2.1 y 2.2). Los servidores fueron virtualizados considerando 800 MB de memoria RAM y discos de 20 GB lo que fue suficiente para la implementación con fines de probar y mostrar los servicios. Para un ambiente de producción se recomienda como mínimo que los servidores sean máquinas con al menos 1 GB de memoria RAM y el tamaño de los discos debe ser lo mayor posible.

En la medida de sus posibilidades se sugiere que las empresas dispongan de los computadores con mejores características de hardware que tengan para estos roles.

Figura 2.1: Virtual Box versión 4.1.14

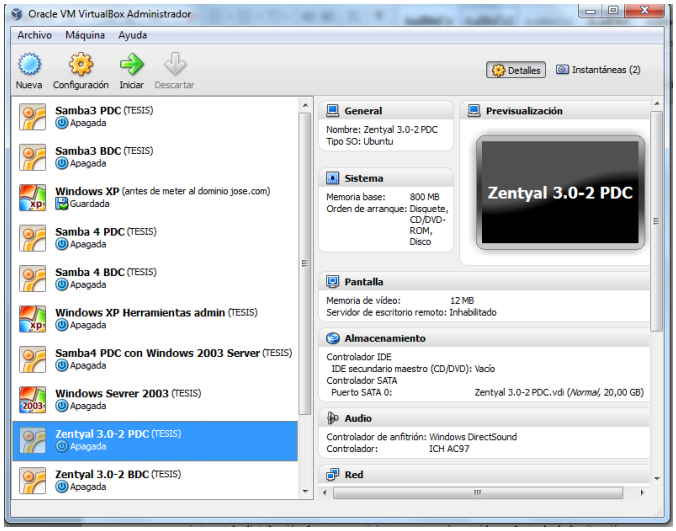


Figura 2.2: Servidores instalados en el Virtual Box

2.4 Distribución de servicios básicos sobre servidores PDC y BDC con Zentyal 3.0.2

Primeramente se instala el sistema operativo deseado para el servidor, en este caso Zentyal 3.0.2. En este trabajo asumimos que solo hay disponibles dos servidores por lo que proponemos utilizar el PDC para la instalación del dominio y los servicios y usar el BDC como respaldo de los servicios básicos de directorio.

Como servicios básicos de cualquier red empresarial están los servicios de correo y de acceso a internet, la distribución de estos servicios en uno o más servidores depende de la situación real de la empresa donde se desee su instalación, dependiendo en gran medida de los recursos materiales y económicos con lo que cuente la empresa. Es decir, depende del equipamiento en existencia y/o el respaldo monetario que se tenga. En nuestro caso estos servicios serán instalados en el servidor primario.

2.5 Zentyal 3.0.2

Zentyal está concebido para ser instalado en una máquina (real o virtual) de forma, en principio, exclusiva. Esto no impide que se puedan instalar otros servicios o aplicaciones adicionales, no gestionados a través de la interfaz de Zentyal, que deberán ser instalados y configurados manualmente.

Funciona sobre la distribución *Ubuntu* en su versión para servidores, usando siempre las ediciones LTS (*Long Term Support*), cuyo soporte es mayor: cinco años en lugar de tres.

La instalación puede realizarse de dos maneras diferentes: usando el instalador de Zentyal (opción recomendada), o instalando a partir de una instalación de *Ubuntu Server Edition*.

En el segundo caso es necesario añadir los repositorios oficiales de Zentyal y proceder a la instalación de aquellos módulos que se deseen.

Sin embargo, en el primer caso se facilita la instalación y despliegue de Zentyal ya que todas las dependencias se encuentran en un sólo CD o USB y además se incluye un entorno gráfico que permite usar la interfaz web desde el propio servidor.

La documentación oficial de *Ubuntu* incluye una breve introducción a la instalación y configuración de Zentyal. [15]

2.5.1 El instalador de Zentyal

El instalador de Zentyal está basado en el instalador de *Ubuntu Server* así que el proceso de instalación resultará muy familiar a los usuarios de dicha distribución.

En primer lugar seleccionaremos el lenguaje de la instalación, para este ejemplo usaremos *Ingles*.

Podemos instalar utilizando la opción por omisión que elimina todo el contenido del disco duro y crea las particiones necesarias para Zentyal usando *LVM (Logical Volume Manager)* o podemos seleccionar la opción *expert mode* que permite realizar un particionado personalizado. La mayoría de los usuarios deberían elegir la opción por omisión a no ser que estén instalando en un servidor con RAID por software o quieran hacer un particionado más específico a sus necesidades concretas.

En el siguiente paso elegiremos el lenguaje que usará la interfaz de nuestro sistema una vez instalado, para ello nos pregunta por el país donde nos localizamos, en este caso use Estados Unidos.

Podemos usar la detección automática de la distribución del teclado, que hará unas cuantas preguntas para asegurarse del modelo que estamos usando o podemos seleccionarlo manualmente escogiendo *No*.

En caso de que dispongamos de más de una interfaz de red, el sistema nos preguntará cuál usar durante la instalación (por ejemplo para descargar actualizaciones).

Después elegiremos un nombre para nuestro servidor; este nombre es importante para la identificación de la máquina dentro de la red. El servicio de *DNS* registrará automáticamente este nombre, *Samba* también lo usará de identificador como podremos comprobar más adelante.

Para continuar, habrá que indicar el nombre de usuario o *login* usado para identificarse ante el sistema. Este usuario tendrá privilegios de administración y además será el utilizado para acceder a la interfaz de Zentyal.

En el siguiente paso se pide la contraseña para el usuario. Cabe destacar que este usuario con esta contraseña podrá acceder tanto al sistema (mediante SSH o *login* local) como a la interfaz web de Zentyal, por lo que debe tener una contraseña segura (más de 7 caracteres incluyendo letras, cifras y símbolos de puntuación).

En el siguiente paso, se define la zona horaria, que se autoconfigurará dependiendo del país de origen que hayamos seleccionado anteriormente, pero se puede modificar en caso de que sea errónea. Para hacer coincidir la zona horaria después de terminado el proceso de instalación podemos acceder a *System ‣ General* y hacer las modificaciones necesarias (Vea figura 2.3).

Figura 2.3: Configuración de la zona horaria

La instalación del sistema base puede durar unos 20 minutos aproximadamente, dependiendo del servidor en cada caso, después se extrae el disco de instalación y se reinicia el sistema.

El sistema arrancará un interfaz gráfica con un navegador que permite acceder a la interfaz de administración, y, aunque tras este primer reinicio el sistema haya iniciado la sesión de usuario automáticamente, de aquí en adelante, necesitará autenticarse antes de hacer login en

el sistema (Vea figura 2.4). El primer arranque tomará algo más de tiempo, ya que necesita configurar algunos paquetes básicos de software.

Figura 2.4: Entorno gráfico con la interfaz de administración

Para comenzar a configurar los perfiles o módulos de Zentyal, usaremos el usuario y contraseña indicados durante la instalación. Cualquier otro usuario que añadamos posteriormente al grupo *sudo* podrá acceder al interfaz de Zentyal al igual que tendrá privilegios de superusuario en el sistema.

2.5.2 Configuración inicial

Una vez autenticado por primera vez en la interfaz web comienza un asistente de configuración, en primer lugar podremos seleccionar qué funcionalidades queremos incluir en nuestro sistema.

Para simplificar nuestra selección, en la parte superior de la interfaz contamos con unos perfiles prediseñados. (Vea figura 2.5)

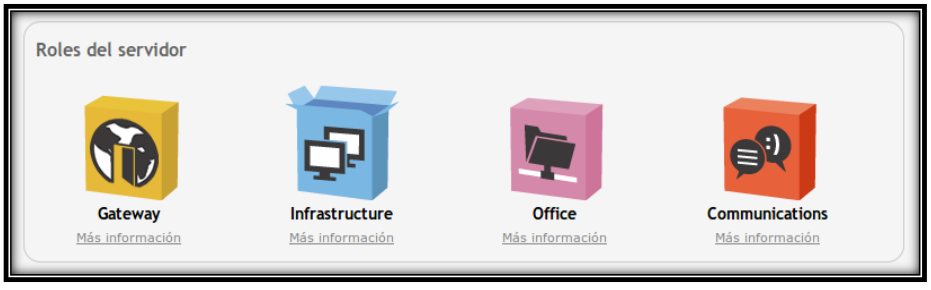


Figura 2.5: Perfiles instalables

Perfiles de Zentyal que podemos instalar:

Zentyal Gateway: Zentyal actúa como la puerta de enlace de la red local ofreciendo un acceso a Internet seguro y controlado. Zentyal protege la red local contra ataques externos, intrusiones, amenazas a la seguridad interna y posibilita la interconexión segura entre redes locales a través de Internet u otra red externa.

Zentyal Infrastructure: Zentyal gestiona la infraestructura de la red local con los servicios básicos: DHCP, DNS, NTP, servidor HTTP, etc.

Zentyal Office: Zentyal actúa como servidor de recursos compartidos de la red local: ficheros, impresoras, calendarios, contactos, perfiles de usuarios y grupos, etc.

Zentyal Unified Communications: Zentyal se convierte en el centro de comunicaciones de la empresa, incluyendo correo, mensajería instantánea y Voz IP.

Podemos seleccionar varios perfiles para hacer que Zentyal tenga, de forma simultánea, diferentes roles en la red.

También podemos instalar un conjunto manual de servicios simplemente seleccionando sus respectivos iconos sin necesidad de adaptarlos a los perfiles, o bien, instalar un perfil más unos determinados paquetes que también les interesen.

Proponemos los módulos *DHCP Service*, *DNS Service*, *File Sharing and Domain*, *HTTP Proxy*, *Mail Service*, *Network Configuration*, *Users and Groups*, *Web Mail Service* y *Web Server* para el servidor primario, y *Network Configuration*, *DNS Service* y *File Sharing and Domain* para el servidor segundario. Los *wizards* que aparecerán en nuestra instalación dependen de los paquetes que hayamos escogido en este paso.

Al terminar la selección, se instalarán también los paquetes adicionales necesarios y además si hay algún complemento recomendado se preguntará si lo queremos instalar. Esta selección no es definitiva, ya que posteriormente podremos instalar y desinstalar el resto de módulos de Zentyal a través de la gestión de software.

El sistema comenzará con el proceso de instalación de los módulos requeridos, mostrando una barra de progreso donde además podemos leer una breve introducción sobre las funcionalidades y servicios adicionales disponibles en Zentyal Server y los paquetes comerciales asociados.

Una vez terminado el proceso de instalación el asistente configurará los nuevos módulos realizando algunas preguntas. Cuando instalemos módulos de Zentyal más adelante, pueden llevar asociados *wizards* de configuración similares.

En primer lugar se solicitará información sobre la configuración de red, definiendo para cada interfaz de red si es *interna* o *externa*, es decir, si va a ser utilizada para conectarse a Internet u otras redes externas, o bien, si está conectada a la red local. Se aplicarán políticas estrictas en el cortafuego para todo el tráfico entrante a través de interfaces de red externas. En nuestro caso solo tenemos la interfaz de red *eth0* y la configuramos de tipo *interna.*

Posteriormente, podemos configurar el método y parámetros de configuración (DHCP, estática, IP asociada, etc.). De nuevo, si nos equivocamos en cualquiera de estos parámetros no es crítico dado que los podremos modificar desde el interfaz de Zentyal en cualquier otro momento.

En nuestro caso usamos la configuración estática (Vea figura 2.6).

Figura 2.6: Seleccionar modo de las interfaces de red

A continuación, tendremos que elegir el dominio asociado a nuestro servidor y el dominio del servidor de correo (Vea figura 2.7 y 2.8) respectivamente, si hemos configurado nuestra(s) interfaz externa por DHCP, es posible que el campo aparezca ya rellenado. Como hemos comentado anteriormente, nuestro *hostname* se registrará como un *host* perteneciente a este dominio. El dominio de autenticación para los usuarios tomará también este identificador. Más adelante podremos configurar otros dominios y su configuración asociada, pero éste es el único que vendrá preconfigurado para que nuestros clientes de *LAN* encuentren los servicios de autenticación necesarios.

Figura 2.7: Configurar dominio local del servidor

Figura 2.8: Configurar dominio del servidor de correo

Una vez hayan sido respondidas estas cuestiones, se procederá a la configuración de cada uno de los módulos instalados. El instalador nos avisará cuando se haya terminado el proceso y podamos acceder al *Dashboard*.

Vea (Primeros pasos con Zentyal) de la documentación oficial [16]

2.5.3 Servicio de resolución de nombres de dominio (DNS)

La configuración de DNS es vital para el funcionamiento de la autenticación en redes locales (implementada con Kerberos a partir de Zentyal 3.0), los clientes de la red consultan el dominio local, sus registros SRV y TXT para encontrar los servidores de tickets de autenticación. Como hemos comentado anteriormente, este dominio viene preconfigurado para resolver los servicios Kerberos a partir de la instalación.

Es importante no confundir el *cliente* de DNS de Zentyal, que se encuentra en *Red -> DNS*, con el *servidor* de DNS de Zentyal en *Infrastructure -> DNS*. Si el servidor DNS está habilitado, el cliente DNS lo usará siempre. En caso de que Zentyal no disponga de servidor

DNS podremos consultar servidores externos. El servidor DNS, a su vez, puede ser configurado para reenviar las consultas para las que no tenga respuesta a otros servidores DNS externos.

Bind [17] es el servidor DNS más comúnmente usado en Internet, originalmente creado en la Universidad de California, Berkeley y en la actualidad mantenido por el *Internet Systems Consortium*. La versión Bind 9, reescrita desde cero para soportar las últimas funcionalidades del protocolo DNS, es la usada por el módulo de DNS de Zentyal.

Vea *Propuesta de servicios básicos de redes para una Empresa basada en software libre*, año 2012, página 36 Capítulo II: Implementación de los servicios en máquinas virtuales epígrafe 2.5 Servidor DNS (Bind9).

2.5.3.1 Proxy DNS transparente

El **proxy DNS transparente** nos permite forzar el uso de nuestro servidor DNS sin tener que cambiar la configuración de los clientes. Cuando esta opción está activada (Vea figura 2.9) todas las peticiones DNS que pasen por Zentyal son redirigidas al servidor DNS de Zentyal que se encargará de responder. Los clientes deberán usar Zentyal como puerta de enlace para asegurarnos que sus peticiones DNS sean redirigidas. Para habilitar esta opción es necesario tener activado el módulo de **cortafuegos**.

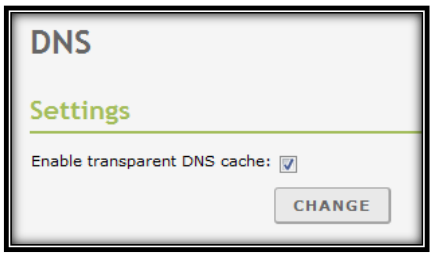


Figura 2.9: Proxy DNS transparente

2.5.3.2 Redirectores DNS

Los **redirectores** o *forwarders* son servidores DNS a los que nuestro servidor reenviará las consultas. El servidor buscará en primer lugar en su cache local, compuesta de los dominios registrados en la máquina y anteriores consultas cacheadas; en caso de no tener respuesta registrada, acudirá a los redirectores. Por ejemplo, la primera vez que consultemos

www.google.com, suponiendo que no tenemos el dominio *google.com* registrado en nuestro servidor, el servidor de DNS de Zentyal consultará a los redirectores y almacenará la respuesta en el cache.

En caso de no tener ningún redirector configurado, el servidor DNS de Zentyal usará los servidores raíz DNS para resolver consultas no almacenadas.

2.5.3.3 Configuración de un servidor DNS autoritario con Zentyal

Además de DNS *caché*, Zentyal puede funcionar como servidor DNS autoritario para un listado de dominios que configuremos. Como servidor autoritario responderá a consultas sobre estos dominios realizadas tanto desde redes internas como desde redes externas, para que no solamente los clientes locales, sino cualquiera puedan resolver estos dominios configurados. Como servidor *caché* responderá a consultas sobre cualquier dominio solamente desde redes internas.

La configuración de este módulo se realiza a través del menú *DNS*, dónde podremos añadir cuantos dominios y subdominios deseemos.

Podemos observar el dominio "local", que se configuró durante la instalación o en el *wizard* de DNS más adelante. Uno de los registros TXT de este dominio contiene el *realm* (concepto similar a dominio) de autenticación de Kerberos. En sus registros de servicios (SRV) podremos encontrar también información sobre los *host* y puertos necesarios para la autenticación de los usuarios. De nuevo, si decidimos eliminar este dominio, sería conveniente replicar esta información en el nuevo. Podemos tener cualquier número de dominios simultáneamente, no causará ningún problema a los mecanismos de autorización mencionados.

Para configurar un nuevo dominio, desplegaremos el formulario pulsando *Añadir nuevo*. Desde éste se configurará el *Nombre del dominio*. (Vea figura 2.10)

Figura 2.10: Añadiendo un dominio

Dentro del dominio nos encontramos con diferentes registros que podemos configurar, en primer lugar las *Direcciones IP del dominio*. Un caso típico es agregar todas las direcciones IP de Zentyal en las interfaces de red locales como direcciones IP del dominio.

Una vez creado un dominio, podemos definir cuantos nombres (registros A) queramos dentro de él mediante la tabla *Nombres de máquinas*. Zentyal configurará automáticamente la resolución inversa. Además para cada uno de los nombres podremos definir cuantos *Alias* queramos. De nuevo, podemos asociar más de una dirección IP a nuestro nombre de máquina, lo cual nos puede servir para que los clientes sepan balancear entre diferentes servidores, por ejemplo dos servidores de *LDAP* replicados con la misma información. (Vea figura 2.11)

Figura 2.11: Añadiendo un host

Normalmente, los nombres apuntan a la máquina dónde está funcionando el servicio y los alias a los servicios alojados en ella. Por ejemplo, la máquina *amy.example.com* tiene los alias *smtp.example.com* y *mail.example.com* para los servicios de mail y la máquina *rick.example.com* tiene los alias *www.example.com* o *store.example.com* entre otros, para los servicios web.

Adicionalmente, podemos definir los servidores de correo encargados de recibir los mensajes para cada dominio. Dentro de *Intercambiadores de correo* elegiremos un servidor del listado definido en *Nombres* o uno externo. Mediante *Preferencias*, determinamos a cuál de estos

servidores le intentarán entregar los mensajes otros servidores. Si el de más preferencia falla lo reintentarán con el siguiente.

También podemos configurar los registros *NS* para cada dominio mediante la tabla *Servidores de nombres*.

Vea (Servicio de resolución de nombres de dominio (DNS)) [18]

2.5.4 Servicio de configuración de red (DHCP)

Para configurar el servicio de DHCP, Zentyal usa *ISC DHCP Software* [19], el estándar más comúnmente usado en sistemas Linux. Este servicio usa el protocolo de transporte UDP, puerto 68 en la parte del cliente y puerto 67 en el servidor.

Vea *Propuesta de servicios básicos de redes para una Empresa basada en software libre*, año 2012, página 37 Capítulo II: Implementación de los servicios en máquinas virtuales epígrafe 2.6 Servidor DHCP.

2.5.4.1 Configuración de un servidor DHCP con Zentyal

El servicio DHCP necesita una interfaz configurada estáticamente sobre la cual se despliega el servicio. Esta interfaz deberá además ser interna. Desde el menú *DHCP* podemos encontrar una lista de interfaces sobre las que podremos ofrecer el servicio. En nuestro caso usaremos la interfaz *eth0* que ya habíamos configurado como interna.

Una vez hagamos clic en la configuración de una de estas interfaces, se nos mostrará un formulario con los siguientes parámetros y se pueden configurar en la pestaña de *Opciones personalizadas*:

Puerta de enlace predeterminada: Es la puerta de enlace que va a emplear el cliente para comunicarse con destinos que no están en su red local, como podría ser Internet. Su valor puede ser *Zentyal*, una puerta de enlace ya configurada en el apartado *Red ‣ Routers* o una *Dirección IP personalizada*.

Dominio de búsqueda: En una red cuyas máquinas estuvieran nombradas bajo el mismo subdominio, se podría configurar este como el dominio de búsqueda. De esta forma, cuando

se intente resolver un nombre de dominio sin éxito (por ejemplo *host*), se intentará de nuevo añadiéndole el dominio de búsqueda al final (*host.zentyal.lan*).

Servidor de nombres primario: Especifica el servidor DNS que usará el cliente en primer lugar cuando tenga que resolver un nombre de dominio. Su valor puede ser *Zentyal DNS local* o la dirección IP de otro servidor DNS. Si queremos que se consulte el propio servidor DNS de Zentyal, hay que tener en cuenta que el módulo **DNS** debe estar habilitado.

Servidor de nombres secundario: Servidor DNS con el que contactará el cliente si el primario no está disponible. Su valor debe ser una dirección IP de un servidor DNS.

Servidor NTP: Servidor NTP (*Network Time Protocol*) que usará el cliente para sincronizar el reloj de su sistema. Puede ser *Ninguno*, *Zentyal NTP local* o la dirección IP de otro servidor NTP. Si queremos que se consulte el propio servidor NTP de Zentyal, hay que tener el módulo **NTP** habilitado.

Servidor WINS: Servidor WINS (*Windows Internet Name Service*) que el cliente usará para resolver nombres en una red NetBIOS. Este puede ser *Ninguno*, *Zentyal local* u otro *Personalizado*. Si queremos usar Zentyal como servidor WINS, el módulo de **Compartición de ficheros** tiene que estar habilitado.

Debajo de estas opciones, podemos ver los rangos dinámicos de direcciones (Vea figura 2.12) y las asignaciones estáticas. Para que el servicio DHCP funcione, al menos debe haber un rango de direcciones a distribuir o asignaciones estáticas; en caso contrario el servidor DHCP **no** servirá direcciones IP aunque esté escuchando en todas las interfaces de red.

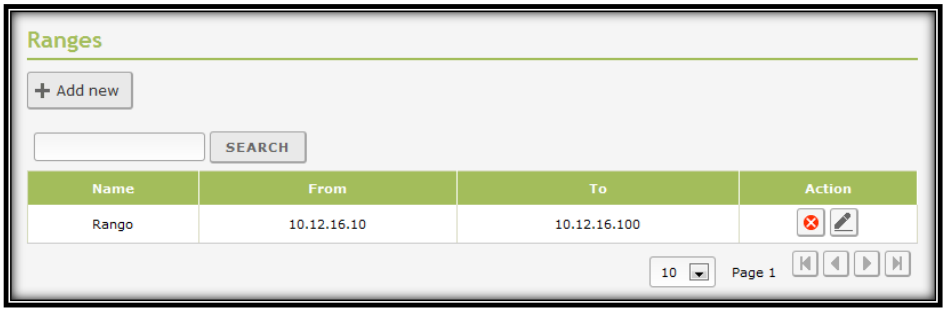


Figura 2.12: Configuración de los rangos de DHCP

Los rangos de direcciones y las direcciones estáticas disponibles para asignar desde una determinada interfaz vienen determinados por la dirección estática asignada a dicha interfaz.

Cualquier dirección IP libre de la subred correspondiente puede utilizarse en rangos o asignaciones estáticas.

Para añadir un rango en la sección *Rangos* se introduce un *nombre* con el que identificar el rango y los valores que se quieran asignar dentro del rango que aparece encima.

2.5.4.2 Opciones de DNS dinámico

Las opciones de DNS dinámico permiten asignar nombres de dominio a los clientes DHCP mediante la integración de los módulos de **DHCP** y **DNS**. De esta forma se facilita el reconocimiento de las máquinas presentes en la red por medio de un nombre de dominio único en lugar de por una dirección IP que puede cambiar. (Vea figura 2.13)

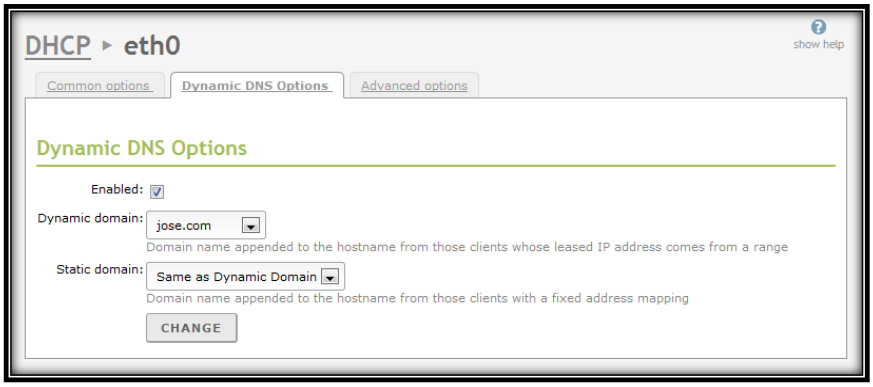


Figura 2.13: Configuración de actualizaciones DNS dinámicas

Para utilizar esta opción, hay que acceder a la pestaña *Opciones de DNS dinámico* y para habilitar esta característica, el módulo DNS debe estar habilitado también. Se debe disponer de un *Dominio dinámico* y un *Dominio estático*, ambos se añadirán a la configuración de DNS automáticamente. El dominio dinámico aloja los nombres de máquinas cuya dirección IP corresponde a una del rango y el nombre asociado es el que envía el cliente DHCP, normalmente el nombre de la máquina, si no envía ninguno usará el patrón *dhcp-<dirección-IP-ofrecida>.<dominio-dinámico>*. Si existe conflictos con alguna asignación estática se sobrescribirá la dirección estática establecida manualmente. Con respecto al dominio estático, el nombre de máquina seguirá este patrón: *<nombre>.<dominio-estático>*. El *nombre* corresponderá con el nombre registrado en el objeto que se usa en la asignación.

Podremos ver los clientes DHCP con asignaciones dinámicas (las estáticas no se mostrarán) gracias a un *widget* que aparecerá en el *Dashboard* (Vea figura 2.14):

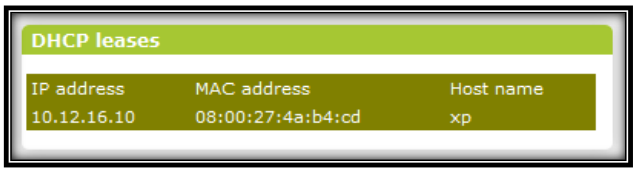


Figura 2.14: Cliente con asignación dinámica activa

Vea (Servicio de configuración de red (DHCP)) de la documentación oficial [20]

2.5.5 Servicio de directorio (LDAP)

Zentyal integra **OpenLDAP** como servicio de directorio, con tecnología *Samba* para implementar la funcionalidad de controlador de dominios *Windows* además para la compartición de ficheros e impresoras.

Vea *Propuesta de servicios básicos de redes para una Empresa basada en software libre*, año 2012, página 38 Capítulo II: Implementación de los servicios en máquinas virtuales epígrafe 2.7 Servidor OpenLDAP.

2.5.5.1 Opciones de configuración de LDAP

Desde el menú *Usuarios y Grupos ‣ Opciones de configuración de LDAP* podemos comprobar cuál es la configuración actual de LDAP y realizar algunos ajustes relacionados con la configuración de autenticación PAM del sistema.

En la parte superior podremos ver la *Información de LDAP* (Vea figura 2.15):

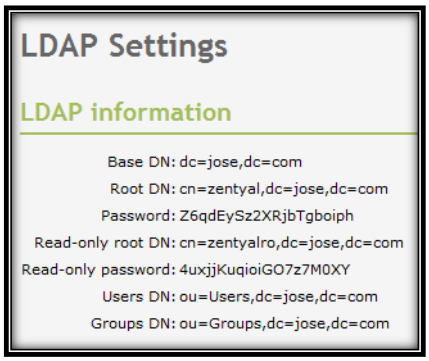


Figura 2.15: Configuración de LDAP en Zentyal

Base DN: Base de los nombres de dominio de este servidor, coincide con el dominio local.

Root DN: Nombre de dominio de la raíz del servidor.

Password: Contraseña que tendrán que usar otros servicios o aplicaciones que quieran utilizar este servidor LDAP. Si se quiere configurar un servidor Zentyal como esclavo de este servidor, esta será la contraseña que habrá de usarse.

Users DN: Nombre de dominio del directorio de usuarios.

Groups DN: Nombre de dominio del directorio de grupos.

En la parte inferior podremos establecer ciertas **Opciones de configuración PAM**

Habilitando PAM permitiremos que los usuarios gestionados por Zentyal puedan ser también utilizados como usuarios normales del sistema, pudiendo iniciar sesiones en el servidor. En este caso no usamos esta configuración.

También podemos especificar desde esta sección el intérprete de comandos predeterminado para los usuarios. Esta opción está inicialmente configurada como *nologin*, evitando que los usuarios puedan iniciar sesiones. Cambiar esta opción no modificará los usuarios ya existentes en el sistema, se aplicará únicamente a los usuarios creados a partir del cambio.

2.5.5.2 Creación de usuarios y grupos

Los usuarios se crean desde el menú *Usuarios y Grupos* ‣ *Usuarios*, donde tendremos que rellenar la siguiente información (Vea figura 2.16):

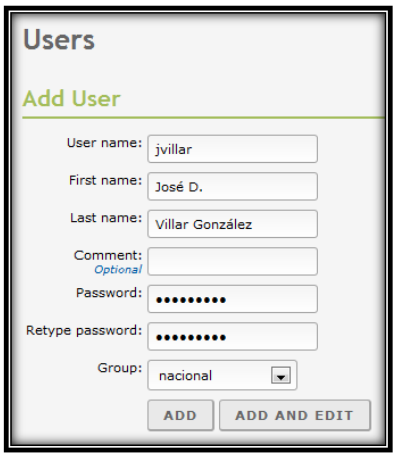


Figura 2.16: Añadir usuario a Zentyal

Nombre de usuario: Nombre que tendrá el usuario en el sistema, que será el nombre que use para identificarse en los procesos de autenticación.

Nombre: Nombre del usuario.

Apellidos: Apellidos del usuario.

Comentario: Información adicional sobre el usuario.

Contraseña: Contraseña que empleará el usuario en los procesos de autenticación. Esta información se tendrá que dar dos veces para evitar introducirla incorrectamente.

Grupo: Es posible añadir el usuario a un grupo en el momento de su creación.

Desde *Usuarios y Grupos ‣ Usuarios* se puede obtener un listado de los usuarios, editarlos o eliminarlos.

Mientras se edita un usuario se pueden cambiar todos los datos anteriores exceptuando el nombre del usuario, además de la información que tiene que ver con aquellos módulos de Zentyal instalados que poseen alguna configuración específica para los usuarios. También se puede modificar la lista de grupos a los que pertenece.

Editando un usuario es posible:

- Activar o desactivar las cuentas de compartición de archivos personales.
- Crear una cuenta de correo electrónico para el usuario y alias para la misma.
- Asignar una extensión telefónica a dicho usuario.
- Activar o desactivar la cuenta de usuario y controlar si dispone de permisos de administración.

Se puede crear un grupo de usuarios desde el menú *Usuarios y Grupos ‣ Grupos*. Un grupo se identifica por su nombre, y puede contener una descripción (Vea figura 2.17).

Figura 2.17: Añadir grupo a Zentyal

A través de *Usuarios y Grupos ‣ Grupos* se pueden ver todos los grupos existentes para poder editarlos o borrarlos.

Editando un grupo, se pueden elegir los usuarios que pertenecen al grupo, además de la información que tiene que ver con aquellos módulos de Zentyal instalados que poseen alguna configuración específica para los grupos de usuarios.

En el ejemplo que proponemos estamos añadiendo el usuario *jvillar* al grupo *nacional* (Vea figura 2.18)

Figura 2.18: Editar grupo

Entre otras cosas con grupos de usuarios es posible:

- Disponer de un directorio compartido entre los usuarios de un grupo.
- Crear colas de llamada por VoIP para el grupo.
- Crear un alias de cuenta de correo que redirija a todos los usuarios de un grupo.

En una configuración *maestro/esclavo*, los campos básicos de usuarios y grupos se editan desde el maestro, mientras que el resto de atributos relacionados con otros módulos instalados en un esclavo dado se editan desde el mismo.

Vea (Servicio de directorio (LDAP)) de la documentación oficial [21]

2.5.6 Servicio de compartición de ficheros y de autenticación

Zentyal usa Samba para implementar SMB/CIFS y gestionar el dominio, Kerberos para los servicios de autenticación.

Vea *Propuesta de servicios básicos de redes para una Empresa basada en software libre*, año 2012, página 42 Capítulo II: Implementación de los servicios en máquinas virtuales epígrafe 2.8 Controlador de dominio (Samba).

2.5.6.1 Configuración de un servidor de ficheros con Zentyal

Los servicios de compartición de ficheros están activos cuando el módulo de **Compartición de ficheros** está activo, sin importar si la función de *Controlador de Dominio* está configurada.

Con Zentyal la compartición de ficheros está integrada con los usuarios y grupos. De tal manera que cada usuario tendrá su directorio personal y cada grupo puede tener un directorio compartido para todos sus usuarios.

El directorio personal de cada usuario en el servidor es compartido automáticamente y sólo puede ser accedido por el correspondiente usuario.

Para configurar los parámetros generales del servicio de compartición de ficheros, ir a *Compartir Ficheros ‣ Configuración general* (Vea figura 2.19).

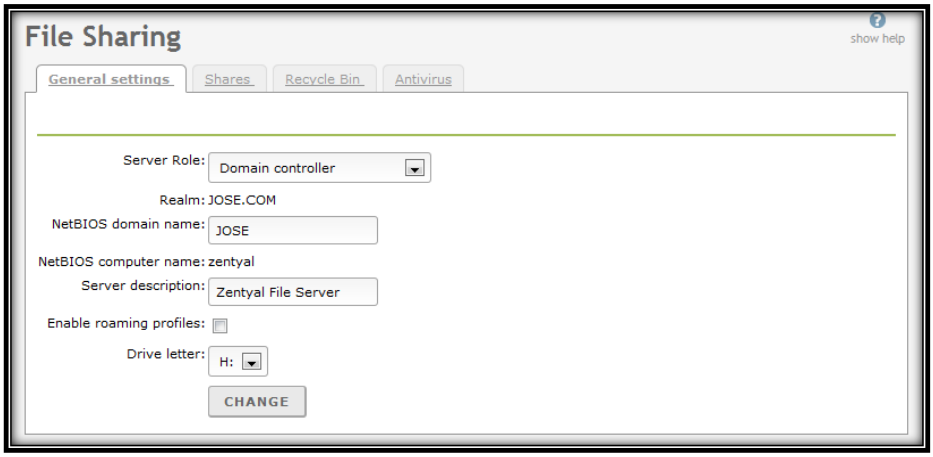


Figura 2.19: Configuración general de la compartición de ficheros

Establecemos el *dominio* donde se trabajará dentro de la red local en *Windows*, y como *nombre NetBIOS* el nombre que identificará al servidor Zentyal dentro de la red *Windows*. Se le puede dar una *descripción* larga para el dominio.

Para crear un directorio compartido, se accede a *Compartir Ficheros* ‣ *Directorios compartidos* y se pulsa *Añadir nuevo* (Vea figura 2.20).

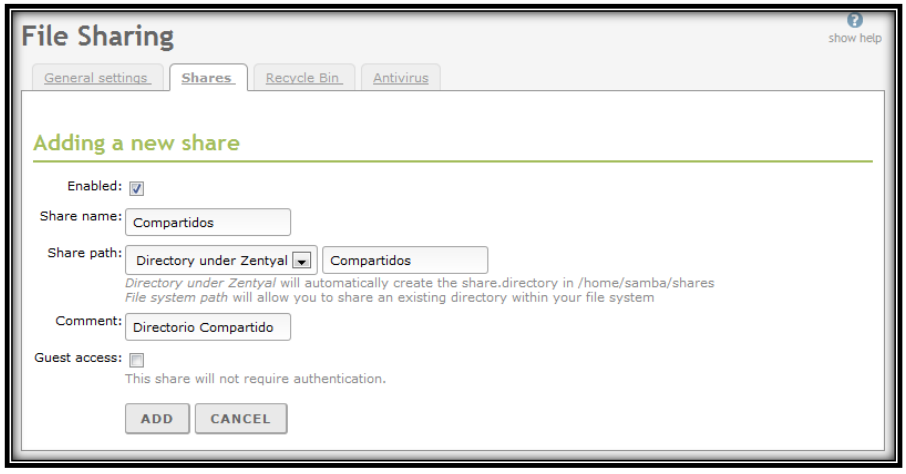


Figura 2.20: Añadir un nuevo recurso compartido

Habilitado: Permite habilitar y deshabilitar el acceso al recurso.

Nombre del directorio compartido: El nombre por el que será conocido el directorio compartido.

Ruta del directorio compartido: Ruta del directorio a compartir. Se puede crear un subdirectorio dentro del directorio de Zentyal */home/samba/shares*, o usar directamente una ruta existente del sistema si se elige *Ruta del sistema de ficheros*.

Comentario: Una descripción más extensa del directorio compartido para facilitar la gestión de los elementos compartidos.

Acceso de invitado: Marcar esta opción hará que este directorio compartido esté disponible sin autenticación. Cualquier otra configuración de acceso o de permisos será ignorada.

2.5.6.2 Configuración de un controlador de dominio con Zentyal

Zentyal puede actuar como controlador de dominio, ya sea como controlador original o como controlador adicional de un dominio *Active Directory* existente.

Si la opción *Perfiles Móviles* está activada, el servidor no sólo realizará la autenticación, sino que también almacenará los perfiles de cada usuario. Estos perfiles contienen toda la información del usuario, como sus preferencias de Windows, sus cuentas de correo de Outlook, o sus documentos. Cuando un usuario inicie sesión, recibirá su perfil del controlador de dominio. De esta manera, el usuario podrá disponer de su entorno de trabajo en cualquier puesto. Hay que tener en cuenta antes de activar esta opción que la información de los usuarios puede ocupar varios *gigabytes*, en el ejemplo que proponemos no usaremos esta configuración. En caso de que se quiera utilizar los *perfiles móviles* es recomendable activar las cuotas. También se puede configurar la *letra del disco* al que se conectará el directorio personal del usuario tras autenticar contra el servidor de autenticación.

En caso que deseemos configurar el servidor como controlador adicional de un dominio *Active Directory* ya creado, habrá que configurar esta opción en la interfaz, junto con otros campos (Vea figura 2.21).

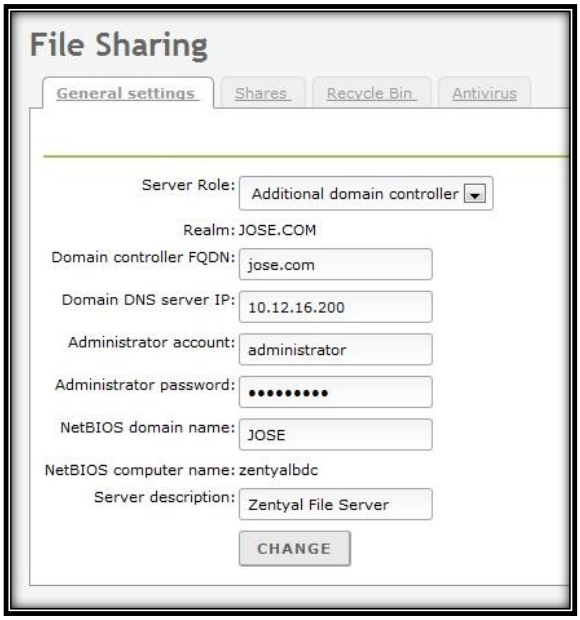


Figura 2.21: Zentyal como controlador adicional de dominio

Nombre *FQDN* del controlador al que nos vamos a unir, dirección IP del servidor DNS que gestiona el dominio, nombre de usuario (en este caso usamos el usuario *administrator* creado por Zentyal, solo es necesario cambiarle la contraseña editando el usuario) y contraseña del administrador del dominio.

Vea (Servicio de compartición de ficheros y de autenticación) de la documentación oficial [22]

2.5.7 Servicio de correo electrónico (SMTP/POP3-IMAP4)

Zentyal usa como MTA para el *envío/recepción* de correos **Postfix**. Así mismo, para el servicio de recepción de correos (POP3, IMAP) Zentyal usa **Dovecot.** Ambos con soporte para comunicación segura con SSL. Por otro lado, para obtener el correo de cuentas externas, Zentyal usa el programa **Fetchmail**.

Vea *Propuesta de servicios básicos de redes para una Empresa basada en software libre*, año 2012, página 58 Capítulo II: Implementación de los servicios en máquinas virtuales epígrafe 2.11 Servidor de correo.

2.5.7.1 Configuración general

En la sección *Correo ‣ General ‣ Opciones del servidor de correo* se pueden configurar los parámetros generales del servicio de correo:

Smarthost al que enviar el correo: Si se establece esta opción, Zentyal no enviará directamente sus mensajes sino que cada mensaje de correo recibido será reenviado al smarthost sin almacenar ninguna copia. En este caso, Zentyal actuará como un intermediario entre el usuario que envía el correo y el servidor que enviará finalmente el mensaje.

En el campo se especifica la dirección IP o nombre de dominio del smarthost. También se puede establecer un puerto añadiendo el texto: [número de puerto] después de la dirección. El puerto por defecto es el estándar SMTP, 25.

Autenticación del smarthost: Determina si el smarthost requiere autenticación y si es así provee un usuario y contraseña.

Nombre del servidor de correo: Determina el nombre de correo del sistema; será usado por el servicio de correo como la dirección local del sistema.

Dirección del postmaster: La dirección del postmaster por defecto es un alias del superusuario (root) pero puede establecerse a cualquier dirección, perteneciente a los dominios virtuales de correo gestionados o no.

Esta cuenta está pensada para tener una manera estándar de contactar con el administrador de correo. Correos de notificación automáticos suelen usar **postmaster** como dirección de respuesta.

Tamaño máximo permitido del buzón de correo: En esta opción se puede indicar un tamaño máximo en MB para los buzones del usuario. Todo el correo que exceda el límite será rechazado y el remitente recibirá una notificación. Esta opción puede sustituirse para cada usuario en la página *Usuarios y Grupos -> Usuarios*.

Tamaño máximo de mensaje aceptado: Señala, si es necesario, el tamaño máximo de mensaje aceptado por el smarthost en MB. Esta opción tendrá efecto sin importar la existencia o no de cualquier límite al tamaño del buzón de los usuarios.

Periodo de expiración para correos borrados: Si esta opción está activada el correo en la carpeta de papelera de los usuarios será borrado cuando su fecha sobrepase el límite de días establecido.

Periodo para correos de spam*:* Esta opción se aplica de la misma manera que la opción anterior pero con respecto a la carpeta de spam de los usuarios.

Vea (Servicio de correo electrónico (SMTP/POP3-IMAP4)) de la documentación oficial [23]

2.5.7.2 Modificando la configuración del correo

Una vez instalado Zentyal con todas las funcionalidades que deseemos incluyendo las de correo, podremos hacer uso de este sin ningún problema, ahora nos interesa controlar los privilegios de los usuarios en el correo, o sea quien tiene derecho a enviar y recibir correo internacional y quien no, y estas opciones Zentyal no las incluye en sus configuraciones, por lo que es necesario hacer algunos cambios en los ficheros de configuración.

Una vez instalado el servicio de correo los archivos de configuración aparecerán en ***/etc/postfix*** pero a estos archivos no debemos hacerle modificaciones ya que cuando reiniciemos el servicio de correo Zentyal reemplaza estos ficheros con unas plantilla ubicadas en ***/usr/share/zentyal/stubs***, por tanto es aquí donde están los archivos que modificaremos, en el caso del correo dentro del directorio ***/mail***.

2.5.7.2.1 Modificando el archivo de configuración principal *main.cf.mas*

Es necesario añadir lo siguiente al final del archivo de configuración */usr/share/zentyal/stubs/mail/main.cf.mas*:

```
smtpd_restriction_classes  =
      inter_in
      inter_out
      nac_in
      nac_out


smtpd_sender_restrictions =
     check_recipient_access hash:/etc/postfix/usuarios_in
```

```
smtpd_recipient_restrictions =
     check_sender_access hash:/etc/postfix/usuarios_out
     permit_mynetworks
     reject_unauth_destination

inter_out  =
   check_recipient_access regexp:/etc/postfix/filtro_inter
   reject
inter_in =
   check_sender_access regexp:/etc/postfix/filtro_inter
   reject
nac_out  =
     check_recipient_access regexp:/etc/postfix/filtro_nac
     reject
nac_in =
     check_sender_access regexp:/etc/postfix/filtro_nac
     reject
```

En la primera parte del contenido añadido declaramos las clases ***inter_in***, ***inter_out***, ***nac_in*** y ***nac_out***, para controlar los niveles de alcance de las cuentas, o sea el derecho de entrada y salida de correos nacionales e internacionales.

Luego cargamos las bases de datos de los usuarios que contienen los niveles de acceso especificando el camino en los valores *check_recipient_access* y *check_sender_access*.

Por último declaramos las ACLs o filtros para las distintas clases.

2.5.7.2.2 Creando filtros para las ACLs

Necesitamos crear los archivos de los filtros para las ACLs (*filtro_nac*, *filtro_inter*). Estos archivos deben crearse directamente en la carpeta de configuración del postfix ubicada en ***/etc/postfix***.

El fichero *filtro_nac* con el siguiente contenido:

```
/\@*\.cu/          RELAY
/^\@/              REJECT 550 El formato de la dirección no es válido.
/\@*/              REJECT Esta cuenta no tiene servicio de correo internacional.
```

De esta forma a quien se le aplique el filtro nacional solo puede enviar o recibir correos nacionales, o sea terminados en .cu

El fichero *filtro_inter* con el siguiente contenido:

```
/^\@/              REJECT 550 El formato de la dirección no es válido.
/\@*/              RELAY
```

De esta forma a quien se le aplique el filtro internacional puede enviar y recibir correos hacia o desde cualquier dirección, solo controlamos que el formato del correo sea válido.

2.5.7.2.3 Definiendo el alcance de cada usuario

Luego de creados los filtros debemos especificar el alcance de cada usuario en nuestro servidor, para ello creamos los archivos (*usuarios_in*, *usuarios_out*) dentro de ***/etc/postfix***

El fichero *usuarios_in* con el siguiente contenido:

```
usuario1@jose.com      inter_in
usuario2@jose.com      nac_in
```

Donde el *usuario1* recibe correos internacionales y el *usuario2* solo nacionales.

El fichero *usuarios_out* con el siguiente contenido:

```
usuario1@jose.com      inter_out
usuario2@jose.com      nac_out
```

Donde el *usuario1* envía correos internacionales y el *usuario2* solo nacionales.

2.5.7.2.4 Generando las bases de datos entendibles por postfix

Por último creemos un fichero llamado *script* dentro de ***/etc/postfix*** que será quien nos generara las bases de datos entendibles por postfix a partir de los ficheros (*filtro_nac*, *filtro_inter*, *usuarios_in*, *usuarios_out*) y por último reiniciará el postfix. Este fichero lo convertimos en ejecutable con el comando *chmod 700 [nombre del script]*, en este caso ***chmod 700 script***, el fichero debe contener lo siguiente:

```
#!/bin/bash
postmap /etc/postfix/filtro_nac
postmap /etc/postfix/filtro_inter
postmap /etc/postfix/usuarios_in
postmap /etc/postfix/usuarios_out
/etc/init.d/zentyal mail restart
exit 0
```

Este fichero debemos ejecutarlos cada vez que realicemos algún cambio ya sea modificando los permisos o añadiendo nuevos usuarios, para correr el script ejecutamos el siguiente comando:

./[nombre del script], en nuestro caso **./script**

2.5.8 Servicio de correo web

Zentyal integra **Roundcube** para implementar el servicio de webmail. Roundcube está desarrollado con las últimas tecnologías web, ofreciendo una experiencia de usuario superior a la de los clientes de webmail tradicionales.

Podemos acceder a las opciones pulsando en la sección *Webmail* del menú izquierdo. Se puede establecer el título que usará el correo *web* para identificarse (Vea figura 2.22). Este título se mostrará en la pantalla de entrada y en los títulos HTML de página.

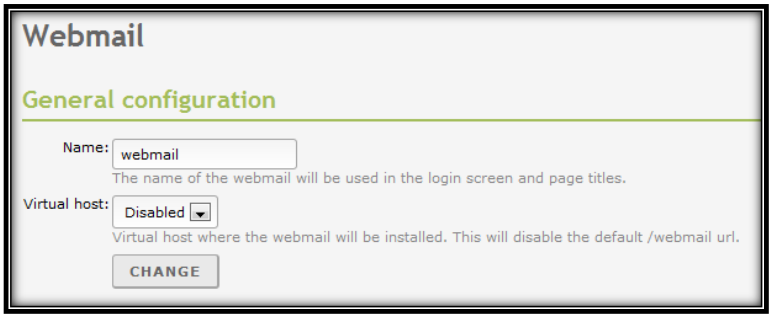


Figura 2.22: Modificar nombre de acceso al servidor web.

Vea (Servicio de correo web) de la documentación oficial [24]

2.5.9 Servicio de Proxy HTTP

Zentyal utiliza Squid para proxy HTTP junto a Dansguardian para el control de contenidos.

Vea *Propuesta de servicios básicos de redes para una Empresa basada en software libre*, año 2012, página 62 Capítulo II: Implementación de los servicios en máquinas virtuales epígrafe 2.12 Squid (Servidor de Proxy).

2.5.9.1 Configuración general del Proxy HTTP con Zentyal

Para configurar el proxy HTTP iremos a *Proxy HTTP ‣ General*. Podremos definir si el proxy funciona en modo Proxy Transparente para forzar la política establecida o si por el contrario requerirá configuración manual. En cualquier caso, en *Puerto* estableceremos dónde escuchará el servidor conexiones entrantes. El puerto preseleccionado es el 3128, otros puertos típicos son el 8000 y el 8080. El proxy de Zentyal únicamente acepta conexiones provenientes de las interfaces de red internas, por tanto, se debe usar una dirección interna en la configuración del navegador. En nuestro caso no usamos la configuración de Proxy Transparente.

El tamaño de la caché define el espacio en disco máximo usado para almacenar temporalmente contenidos web. Se establece en *Tamaño de caché* y corresponde a cada administrador decidir cuál es el tamaño óptimo teniendo en cuenta las características del servidor y el tráfico esperado.

Es posible indicar que dominios no serán almacenados en caché. Por ejemplo, si tenemos servidores web locales, no se acelerará su acceso usando la caché y se desperdiciaría memoria que podría ser usada por elementos de servidores remotos. Si un dominio está exento de la caché, cuando se reciba una petición con destino a dicho dominio se ignorará la caché y se devolverán directamente los datos recibidos desde el servidor sin almacenarlos. Estos dominios se definen en *Excepciones a la caché,* en nuestro caso especificamos el dominio *jose.com*.

A su vez, puede interesarnos que ciertas páginas no se sirvan a través del proxy, sino que se conecte directamente desde el navegador del cliente, ya sea por cuestiones de funcionamiento

incorrecto o de privacidad de los usuarios. En esos casos, podemos añadir una excepción en *Excepciones del Proxy Transparente*.

La característica *Activar Single Sign-On (Kerberos)* sirve para validar el usuario automáticamente usando el ticket de *Kerberos* creado al inicio de sesión, por lo tanto nos puede ser útil si estamos usando proxy *No Transparente*, políticas de acceso por grupos y, por supuesto, un esquema de autorizaciones basado en *Kerberos*, en el ejemplo que proponemos no se usa esta configuración.

Advertencia: Si vamos a usar autenticación automática con Kerberos, al configurar el navegador cliente tendremos que especificar nuestro proxy (el servidor Zentyal) por su nombre en el dominio local, nunca por IP.

El proxy HTTP puede eliminar anuncios de las páginas web. Esto ahorrara ancho de banda y reducirá distracciones e incluso riesgos de seguridad para los usuarios. Para usar esta característica, debemos activar la opción *Bloqueo de Anuncios*.

2.5.9.2 Filtrado de contenidos con Zentyal

Zentyal permite el filtrado de páginas web en base a su contenido. Se pueden definir múltiples perfiles de filtrado en *Proxy HTTP ‣ Perfiles de Filtrado*.

En nuestro caso definimos los perfiles "*nacional*" e "*internacional*" para controlar quien tiene acceso a internet y quien tiene solo acceso a la red nacional.

Accediendo a la *Configuración* de estos perfiles, podremos especificar diversos criterios para ajustar el filtro a nuestros certificados. En la primera pestaña podemos encontrar los *Umbrales de contenido* y el filtro del antivirus. Para que aparezca la opción de antivirus, el módulo *Antivirus* debe estar instalado y activado.

Estos dos filtros son dinámicos, es decir analizarán cualquier página en busca de palabras inapropiadas o virus. El umbral de contenidos puede ser ajustado para ser más o menos estricto, esto influirá en la cantidad de palabras inapropiadas que permitirá antes de rechazar una página. En nuestro caso lo configuramos de forma *Estricta* para los dos perfiles.

En la siguiente pestaña *Reglas de dominios y URLs* podemos decidir de forma estática que dominios estarán permitidos en este perfil. Podemos decidir *Bloquear sitios especificados*

sólo como IP, para evitar que alguien pueda evadir los filtros de dominios aprendiendo las direcciones IP asociadas. Así mismo con la opción *Bloquear dominios y URLs no listados* podemos decidir si la lista de dominios más abajo se comporta como una *blacklist* o una *whitelist*, es decir, si el comportamiento por defecto será aceptar o denegar una página no listada.

Finalmente, en la parte inferior, tenemos la lista de reglas, donde podremos especificar los dominios que queremos aceptar o denegar.

Así para el perfil *nacional* permitimos el dominio *cu* y marcamos la opción *Bloquear dominios y URLs no listados*, garantizando así que los usuarios o grupos a los que se le aplique ese perfil solo puedan navegar en direcciones terminadas en *cu* y el resto quedan prohibidas.

Y para el perfil *internacional* no marcamos la opción *Bloquear dominios y URLs no listado,* de forma tal que los usuarios o grupos a los que se le aplique este perfil tengan acceso a todos los dominios, ahora si queremos llevar el control de algunos sitios, por ejemplo negar *Facebook* solo necesitamos añadir *Facebook.com* a la lista, especificarle la opción *negar* y listo.

Para usar los filtros por *Categorías de dominios* debemos, en primer lugar, cargar una lista de dominios por categorías. Configuraremos la lista de dominios para el Proxy desde *Proxy HTTP ‣ Listas por categorías*.

Una vez hayamos configurado la lista, podemos seleccionar que categoría en concreto deseamos permitir o denegar desde la pestaña *Categorías de dominios* del filtro.

En las dos pestañas restantes podemos decidir los tipos de contenido o ficheros que serán aceptados por este perfil, ya sea por tipo MIME o por extensión de fichero. Los tipos MIME son un identificador de formato en Internet, por ejemplo *application/pdf*.

Contamos con una interfaz similar para las extensiones de ficheros descargados mediante nuestro proxy.

2.5.9.3 Reglas de acceso

Una vez hayamos decidido nuestra configuración general y nuestros perfiles, tendremos que definir reglas de acceso. Por defecto, la sección *Proxy HTTP ‣ Reglas de acceso* contiene una regla permitiendo todo acceso. Al igual que en el *Cortafuegos*, la política por omisión de regla siempre será denegar y la regla que tendrá preferencia en caso de que varias sean aplicables será la que se encuentre más arriba.

Mediante el *Período de tiempo* podemos definir en qué momento se tendrá en consideración esta regla, tanto las horas como los días. Por defecto se aplica en todo momento.

El *Origen* es un parámetro muy flexible, ya que nos permite definir si esta regla se aplicará a los miembros de un *Objeto* de Zentyal o a los usuarios de un determinado *Grupo* (recordemos que las restricciones por grupo sólo están disponibles para el modo de Proxy **no** transparente). La tercera opción es aplicar la regla sobre cualquier tipo de tráfico que atraviese el proxy.

Advertencia: Por limitaciones de Dansguardian no son posibles ciertas combinaciones de reglas basadas en grupo y reglas basadas en objeto. La interfaz de Zentyal avisará al usuario cuando se de uno de estos casos.

De forma similar al *Cortafuegos*, una vez Zentyal haya decidido que el tráfico coincide con una de las reglas definidas, debemos indicarle una *Decisión*, en el caso del Proxy hay tres opciones:

Permitir todo: Permite todo el tráfico sin hacer ninguna comprobación, nos permite aun así, seguir disfrutando de caché de contenidos web y registros de accesos.

Denegar todo: Deniega la conexión web totalmente.

Aplicar perfil de filtrado: Para cada petición, comprobará que los contenidos no incumplen ninguno de los filtros definidos en el perfil, se desarrollarán los perfiles de filtrado en el siguiente apartado.

Antes de definir las nuevas reglas de acceso eliminemos la existente que permitía todo y en todo momento.

2.5.9.3.1 Reglas de acceso nacional e internacional

Para crear la regla de acceso nacional debemos tener definidos los perfiles, en nuestro caso recordemos (*nacional* e *internacional*) y determinados usuarios o grupos a los que les vamos a aplicar estos perfiles y así quedan definidas las reglas. En el ejemplo que proponemos tenemos dos grupos llamados igual a los filtros, o sea (*nacional* e *internacional*).

Solo necesitamos crear una nueva regla *Proxy HTTP ‣ Reglas de acceso,* añadimos una llamada *nacional,* si queremos que esta regla se aplique todo el tiempo dejamos los campos de *Periodo de tiempo* en blanco. Seleccionamos la fuente, en nuestro caso *Grupo de Usuarios* y seleccionamos el grupo *nacional,* en el campo *Decisión* seleccionamos *Aplicar Perfiles de Filtros* y seleccionamos el filtro *nacional,* (recordemos que en nuestro caso el nombre de los grupos y de los perfiles coinciden). Luego añadimos la regla y listo.

De igual forma hacemos en el caso de la regla *Internacional*. Quedando de la siguiente forma, (Vea figura 2.23):

Figura 2.23: Reglas de acceso nacional e internacional

2.6 Samba 3 PDC con Samba 3 BDC controlador de dominio

La configuración del controlador primario y secundario con Samba 3 y OpenLdap se detalla en los anexos. Vea Anexo I Manual de instalación Controlador de Dominio con Samba 3

2.7 Samba 4 PDC con Samba 4 BDC controlador de dominio

La configuración del controlador primario y secundario con Samba 4 se detalla en los anexos.

Vea Anexo II Manual de instalación Controlador de Dominio con Samba 4

2.8 Samba 4 controlador de dominio junto a Windows 2003 Server

Samba 4 también puede usarse con un servidor Windows 2003 Server como respaldo, solo es necesario unir el servidor Windows al dominio de la misma forma que añadimos un cliente con Windows XP Professional (Vea Uniendo Windows XP Professional al dominio)

Una vez hecho esto ejecutamos desde la consola dcpromo y respondemos las preguntas de la siguiente forma:

1. En el tipo de controlador de dominio, seleccionar la opción *Controlador de dominio adicional para un dominio existente.*
2. Luego pedirá el usuario administrador del dominio, la contraseña, y el dominio, aunque este último lo toma por defecto.
3. Después dejar la opción por defecto para todas las preguntas como (*Carpetas de la base de datos y del registro, Volumen del sistema compartido*).
4. Luego pide la *Contraseña de administrador del modo de restauración de servicios de directorios*.
5. Por último muestra un resumen de las principales configuraciones seleccionadas, confirme si todo está como desea y comenzara a producirse la réplica entre servidores.

Una vez lograda la sincronización entre el servidor primario con Samba 4 y el segundario con Windows 2003 Server podremos iniciar sesión en el servidor Windows con el usuario y la contraseña del administrador del dominio y hacer todas las operaciones que deseemos con las herramientas administrativas de Windows.

2.9 Conclusiones parciales del capítulo

- En este capítulo se ha utilizado Ubuntu como sistema operativo para los servidores. Se realizó la instalación y configuración de cada servicio proporcionándose una guía de recomendaciones.
- Se utiliza como plataforma de trabajo para implementar los servidores el ORACLE *VirtualBox versión 4.1.14* que demuestra ser muy eficiente para probar las instalaciones en un ambiente controlado antes de pasarlas a los servidores de producción.
- Se planteó una guía lógica a seguir para la instalación y distribución de los servicios que puede ser muy útil para guiar el trabajo de administradores con poca experiencia en Linux. En esta instalación fueron utilizados servidores que son todos accesibles mediante el repositorio de Ubuntu.
- Después de analizar algunas variantes para la creación de dominios utilizando software libre gratis concluimos:
    - Samba 3 + LDAP: El proceso de instalación resulta engorroso y exige un dominio profundo de Linux.
    - Samba 4: Promete y es más simple la instalación, pero no es estable, algunas cosas aun no funcionan bien, logra una interfaz que es conocida por los administradores pues es similar al directorio activo de Windows.
    - Zentyal: Cuenta con una interfaz gráfica amigable, es intuitiva, fácil de usar, integra un amplio número de servicios de manera bastante simple, es estable y tiene buen soporte de la comunidad internacional.

CAPÍTULO III: ANÁLISIS DE LOS RESULTADOS Y ADMINISTRACIÓN DEL DOMINIO

Como parte de la investigación para la justificación del trabajo realizamos una encuesta (Vea Anexo V Encuesta sobre Administración de Redes) a un grupo de administradores de red con el objetivo de medir:

- Experiencia como administrador de red.
- Conocimiento de la administración de redes.
- Alternativas de superación profesional.
- Sistema operativo que emplean en su desempeño laboral.

Una vez aplicada la encuesta se realizó el análisis de los datos, esto se ve reflejado en la primera parte del capítulo, *Epígrafe 3.1*.

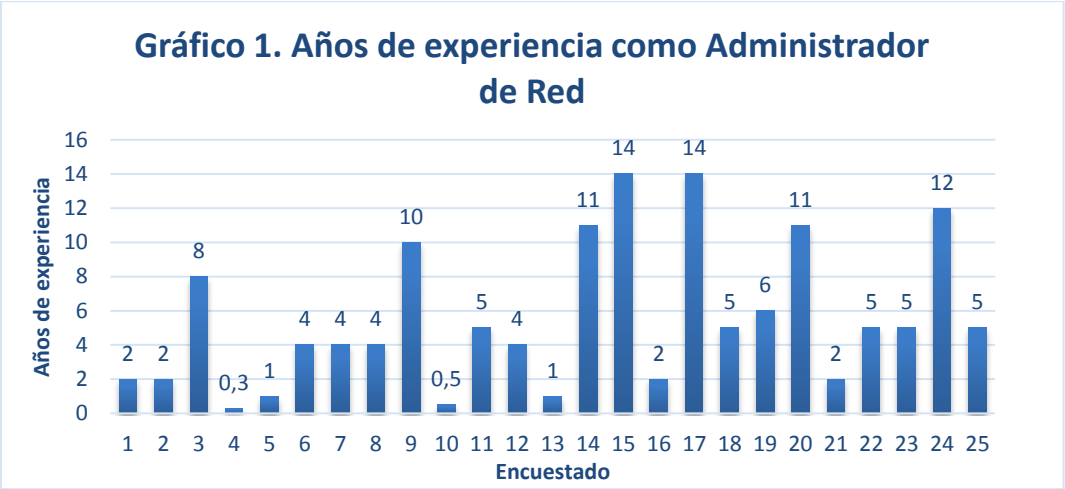
En la segunda parte se explica la adición de clientes Windows y Linux al dominio, proponemos un ejemplo del funcionamiento del servicio de correo y analizamos los errores más comunes en el proceso de migración hacia software libre.

3.1 Resultados de la encuesta “Administración de Redes”

La encuesta se aplicó a un total de 25 personas. Veamos lo siguiente:

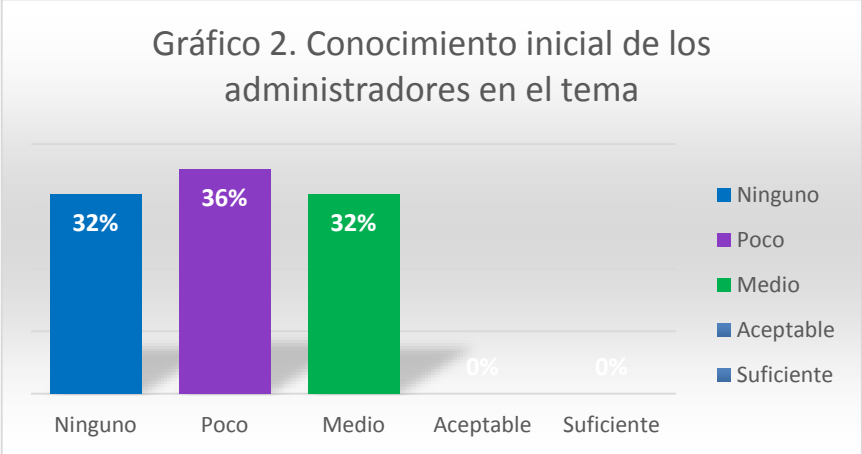
El Gráfico 1 muestra los años trabajados por cada encuestado, nos interesa destacar lo siguiente:

Administrador con menos tiempo de experiencia (en años)	**0,3**
Administrador con más tiempo de experiencia (en años)	14
Promedio de años de trabajo	5,512



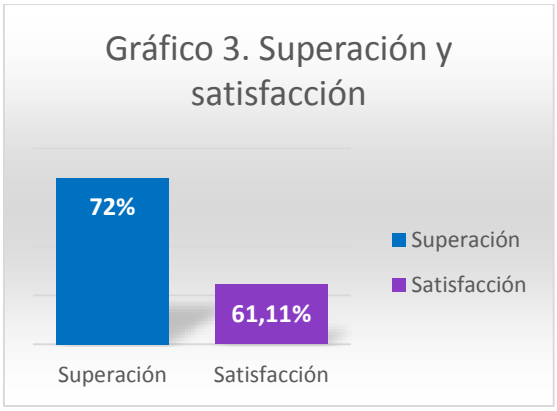
Fuente: Cuestionario "Administración de Redes"

Otro de los aspectos que nos interesaba medir era la experiencia que tenían los administradores cuando comenzaron a ejercer su trabajo, este análisis demostró que el 68% de los administradores no contaban con buena preparación, veamos el Gráfico 2.



Fuente: Cuestionario "Administración de Redes"

El Gráfico 3 muestra cuantos encuestados recibieron superación y de estos cuantos están satisfechos, 18 de los administradores han recibido superación, lo que representa el 72 %, y de este grupo11 están conformes con la superación recibida representando un 61,11%, este análisis demostró que más de la mitad de los administradores han recibido preparación, o sea 18 de 25 un 72%, lo que es bueno, veamos el Gráfico 3.

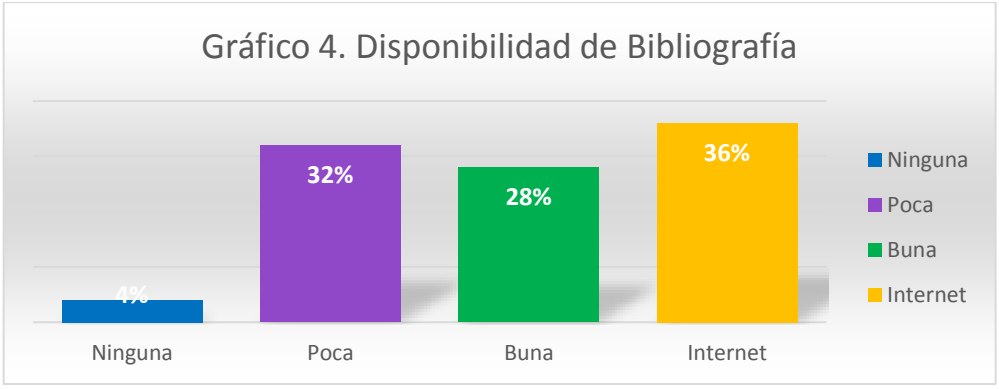


Fuente: Cuestionario "Administración de Redes"

El grafico anterior demostró que existe un grupo de administradores, para ser más precisos 7, representando el 38,89% de los que recibieron superación que no están conformes. Las principales razones de insatisfacción han sido:

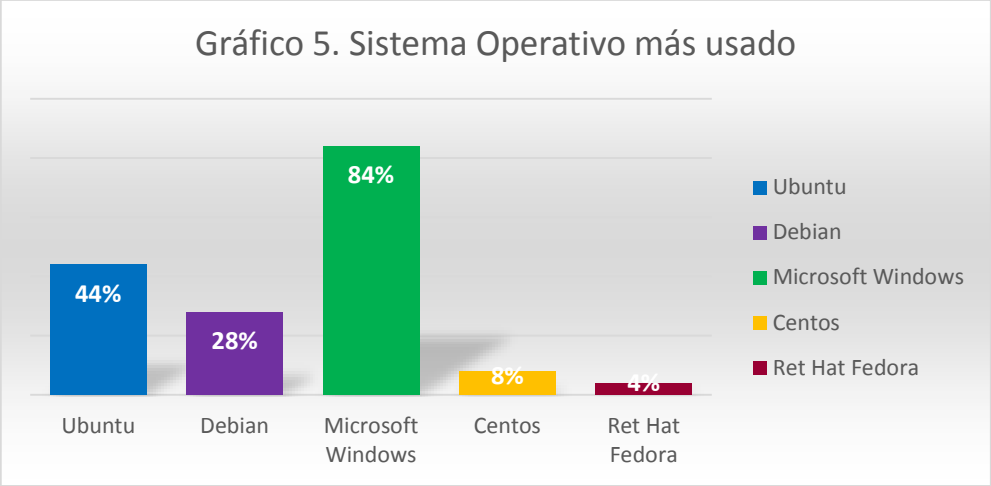
- Los cursos son muy cortos.
- Tienen un nivel medio sobre la profundización de los conocimientos.
- Existen temas que no se tratan (Ejemplo: Seguridad Informática, WiFi).
- Poca actividad práctica.
- Reciben poca preparación.

El Gráfico 4 muestra la disponibilidad de la bibliografía y de internet, este análisis nos revela que el 36% no cuentan con bibliografía necesaria y el 64% no tiene acceso a internet, veamos:



Fuente: Cuestionario "Administración de Redes"

Otro de los aspectos a medir es que sistema operativo es más usado por los administradores y de ellos cuales de software libre, este análisis demostró que de las distribuciones basadas en Linux (Ubuntu y Debian) Ubuntu es la más usada con un 44%, representando11 de los administradores, vea el Gráfico 5.



Fuente: Cuestionario "Administración de Redes"

3.2 Configuración de los terminales clientes

Se consideran en este caso los clientes que actualmente son más utilizados, siendo estos Microsoft Windows XP, Microsoft Windows 7 y clientes Linux. Por la popularidad que ha tomado Ubuntu como máquina de escritorio, en este capítulo se presenta la adición de un Ubuntu Desktop al dominio aunque el proceso es similar para cualquier otra distribución.

Un aspecto importante a garantizar antes de intentar adicionar los clientes al dominio es que la resolución de nombres esté funcionando correctamente y este activada la opción de NetBIOS sobre TCP/IP.

3.2.1 Herramienta gráfica para la administración del directorio OpenLDAP

Existen muchas aplicaciones web que permiten el acceso al directorio LDAP para poder crear y modificar elementos de los cuales PhpLdapAdmin es una de las más utilizadas. Otros posibles exploradores LDAP libres podrían ser LAM (*LDAP Account Manager*) y/o

Jexplorer. PhpLdapAdmin necesita de un servidor web, por lo que en caso de no tener ninguno funcionando durante el proceso de su instalación se instalará automáticamente apache2.

La instalación se hace con: apt-get install phpldapadmin

Por defecto la instalación se hace en */usr/share/phpldapadmin*, puede copiar esta carpeta completa para */var/www* o hacer un enlace simbólico con este directorio para que el servidor web lo muestre.

El archivo de configuración para el phpldapadmin es ***config.php*** y se encuentra dentro del directorio phpldapadmin (Vea Anexo III Configuración de la aplicación PhpLdapAdmin).

3.2.2 Configuración de red de la máquina cliente Windows XP/Seven

Para configurar la red de las máquinas clientes debe asignar al cliente una dirección IP dentro del segmento de red y se configura la red para que el servidor WINS sea el servidor Samba y el DNS apunte al servidor que corre el Bind 9. Se debe habilitar también NetBIOS sobre TCP/IP. Antes de intentar unir el cliente al dominio puede utilizar comandos como *ping* y *nslookup* para comprobar que la resolución de nombres funciona correctamente. Se asume que es conocido como iniciar el asistente para configurar la red. Vea detalles en la figura 3.1.

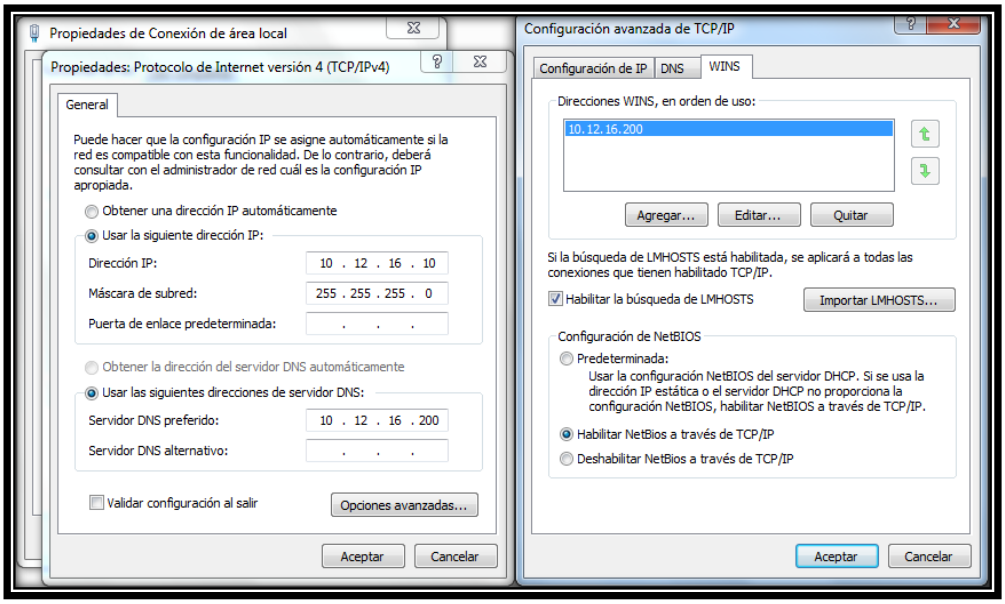


Figura 3.1: Configuración de red de la máquina cliente

3.2.3 Uniendo Windows XP Professional al dominio

Después de haber configurado la red como mostramos anteriormente, para unir clientes Windows al dominio se siguen los pasos siguientes:

Desde el menú “Propiedades del sistema”, se accede a la pestaña “Nombre de equipo” se pulsa sobre el botón “Cambiar”. Por defecto la máquina es parte del grupo de trabajo “GRUPO_TRABAJO” como se ve en la figura 3.2. Se pulsa sobre el *radio botton* con etiqueta “Dominio”, y al activar el campo de texto se pone el nombre corto del dominio (Vea figura 3.3.).

Nota: Es importante señalar que en el caso de Samba 4 se escribe el nombre corto del dominio y en mayúscula, en el ejemplo que proponemos (JOSE) y en el caso de Zentyal se escribe el *FQDN* y en minúscula, sería (jose.com).

A continuación pulse el botón Aceptar, y sale un asistente solicitando las credenciales de un usuario con derechos de agregar clientes al dominio (figura 3.4).

Si se completa con éxito el ingreso al dominio se recibe un mensaje de bienvenida y una solicitud de reinicio del sistema.

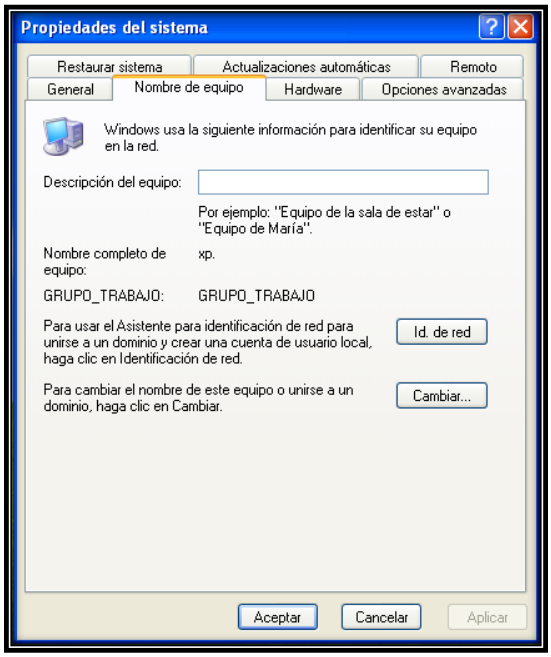


Figura 3.2: Propiedades del sistema Windows XP.

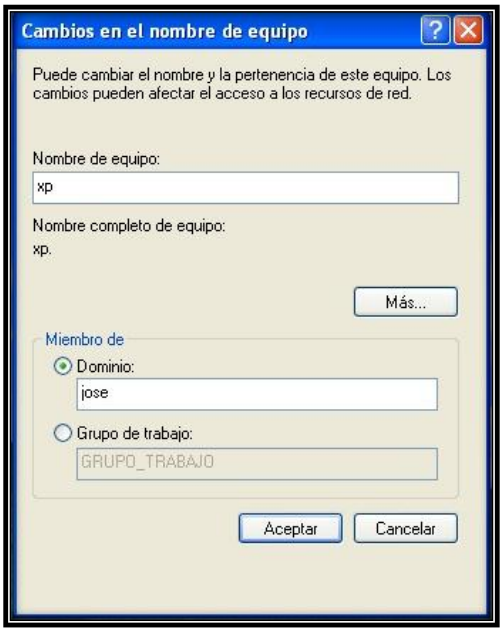


Figura 3.3: Mostrando como añadir una maquina al dominio “JOSE”

Figura 3.4: Petición por usuario administrativo del dominio

3.2.3.1 Iniciar sesión de un usuario del dominio

Al iniciar la máquina cliente debe mostrar en este momento la opción de entrar el dominio. Se puede ingresar al dominio utilizando el nombre de usuario y su contraseña de un usuario del LDAP (figura 3.5). La figura 3.6 muestra una sesión de usuario "jvillar" conectado al dominio.

Figura 3.5: Iniciando sesión con usuario "jvillar" miembro del dominio

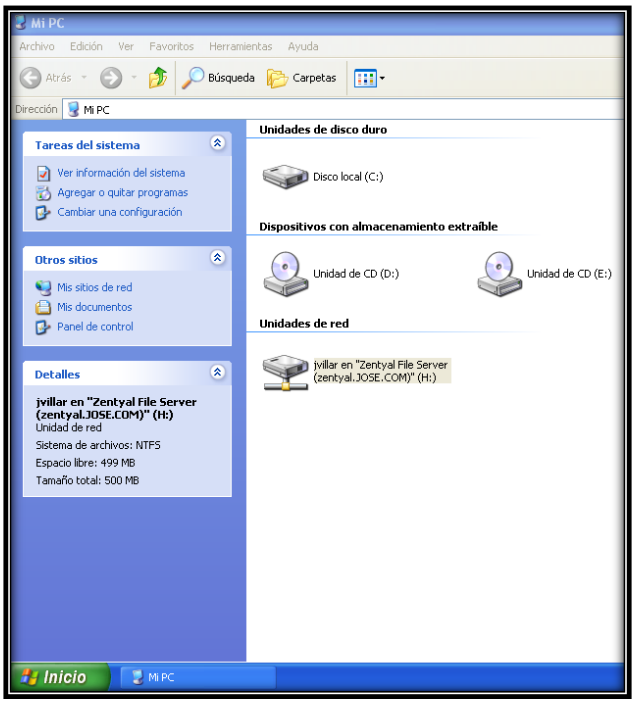


Figura 3.6: Sesión de usuario "jvillar" en el dominio.

3.2.4 Uniendo Windows 7 al dominio

Para unir un cliente de Windows 7 al dominio se deben modificar dos campos del registro. Para ello puede guiarse por la información publicada en https://bugzilla.samba.org/attachment.cgi?id=4988&action=view que debe ser bajado de la red y ejecutado.

A continuación se accede a "*System properties*", desde el apartado "*Advanced system settings"* se selecciona, se accede a la pestaña "*Computer Name"* y de aquí en adelante el proceso es similar al realizado para Windows XP Professional. La comprobación de que el cliente fue añadido con éxito es similar a la realizada con Windows XP.

3.2.5 Uniendo clientes Linux al dominio.

Primero se instala el software necesario para que funcione:

```
apt-get install auth-client-config libpam-ldap libnss-ldap
```

Ahora se deberá responder a las preguntas que se hacen en el proceso de instalación (configuración de auth-client-config) de la siguiente forma:

```
Should debconf manage LDAP configuration? Yes
LDAP server Uniform Resource identifier: LDAP://10.12.16.200/
Distinguished name of the search base: dc=jose,dc=com
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=jose,dc=com
LDAP root account password: dejar vacío
```

A continuación el archivo */etc/ldap.conf* será modificado y se le agregará lo siguiente:

```
host 10.12.16.200
base dc=jose,dc=com
uri ldap://10.12.16.200/
ldap_version 3
```

```
rootbinddn cn=admin,dc=jose,dc=com
port 389
bind_policy soft
pam_password md5
```

Ahora se copiará el archivo */etc/ldap.conf* a */etc/ldap/ldap.conf* con:

```
cp  /etc/ldap.conf  /etc/ldap/ldap.conf
```

Se creará un nuevo arhivo en */etc/auth-client-config/profile.d* con:

```
touch /etc/auth-client-config/profile.d/open_ldap
```

El archivo *open_ldap* debe ser editado y se le agregará la siguiente sintaxis:

```
[open_ldap]
nss_passwd=passwd:          compat ldap
nss_group=group:            compat ldap
nss_netgroup=netgroup:      compat ldap
nss_shadow=shadow:          compat ldap

pam_auth=auth               required        pam_env.so
auth                        sufficient      pam_unix.so    likeauth        nullok
auth                        sufficient      pam_ldap.so    use_first_pass
auth                        required        pam_deny.so
pam_account=account         sufficient      pam_unix.so
account                     sufficient      pam_ldap.so
account                     required        pam_deny.so

pam_password=password       sufficient      pam_unix.so nullok md5 shadow use_authtok
password                    sufficient      pam_ldap.so use_first_pass
password                    required        pam_deny.so
pam_session=session         required        pam_limits.so
session                     required        pam_mkhomedir.so    skel=/etc/skel/
```

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

Se debe realizar una copia de seguridad de */etc/nsswitch.conf*

```
cp  /etc/nsswitch.conf{,.original}
```

Ahora se realizará una copia de seguridad de *pam.d* de la siguiente forma:

```
cd /etc/pam.d/
mkdir bkup
cp * bkup/
```

Finalmente se activa el nuevo perfil de autentificación LDAP ejecutando el siguiente comando:

```
auth-client-config -a -p open_ldap
```

Ahora se debe reiniciar la PC cliente y después de esto debe dejar iniciar una sesión a los usuarios del dominio.

3.3 Correo electrónico

A continuación se muestra un ejemplo básico del servicio de correo electrónico funcionando. Para realizar este ejemplo se utilizó el Roundcube (Vea figura 3.7) desde una máquina ejecutando ORACLE VirtualBox versión 4.1.14 que sirvió como plataforma de prueba.

Figura 3.7: Roundcube mostrando el correo electrónico

Las figuras 3.8 y 3.9 muestran un ejemplo de comunicación entre dos usuarios del dominio, nombrados Manuel Castro (mcastro) y Jose D. Villar González (jvillar) por medio de correo electrónico. En ella se puede ver el envío de un correo con asunto (subject) "***testing mail server***" desde la cuenta de correo de Manuel Castro (mcastro@jose.com) hacia la cuenta de Jose D. Villar (jvillar@prueba.cu). Estas figuras prueban que los tres componentes del correo electrónico están en colaboración y funcionan perfectamente bien.

Figura 3.8: Envió de correo desde usuario Manuel Castro a usuario José D. Villar González.

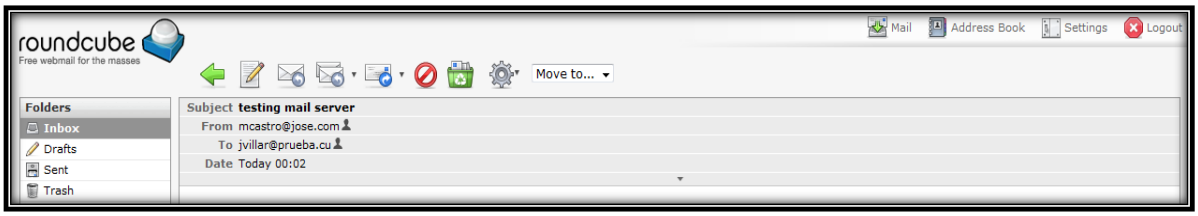


Figura 3.9: Entrada de correo electrónico a usuario José D. Villar González.

3.4 Errores más comunes en el proceso de migración

Actualmente el país ha definido una política de migración hacia software libre, esta política se ha ido aplicando paulatinamente en diferentes sectores dándose como una regularidad que en la mayoría de ellos no se cuenta con personal capacitado en Linux y administración con Linux.

3.4.1 Errores detectados frecuentemente en este proceso:

- Aplicación de directivas que obligan a migrar en determinada etapa sin tener condiciones reales para enfrentar la migración.
- Contratación de personal no calificado en el área de administración de redes para realizar funciones de administrador.

- Ambientes de trabajo sin acceso a internet para los administradores lo que hace casi imposible la autosuperación y le niega el acceso a comunidades de internet que pueden brindar ayuda ante cualquier problema.
- Ausencia de servicios de redes nacionales a los que tengan acceso todas las empresas.

Esto hace que al enfrentar el proceso técnico de migrar se produzcan dificultades como las mostradas en el siguiente tópico.

3.4.2 Dificultades observadas en el proceso de migración.

- Trabajo con repositorios no actualizados.
- No se configuran las actualizaciones de seguridad al no tener acceso a las mismas.
- Grandes pérdidas de tiempo tratando de obtener información disponible en internet pero a la que no tienen acceso.
- Creación de ambientes de redes donde los servidores se migran a Linux pero no se configura dominio por falta de conocimientos sobre el proceso.
- Malas configuraciones de servicios básicos como correo electrónico, DNS, navegación de internet, etc. por no tener la experiencia e información necesaria. En algunos casos simplemente no se oferta el servicio o se oferta un servicio de mala calidad y pésima seguridad.

3.5 Conclusiones parciales del capítulo

A partir del trabajo realizado podemos concluir que:

- ❖ El sistema operativo de distribuciones Linux más usado es Ubuntu.
- ❖ Los servidores son capaces de dar servicio a máquinas Windows y Linux en el dominio.
- ❖ Los servicios y recursos ofrecidos por el servidor se comportan de manera adecuada.
- ❖ El proceso de migración a software libre de los principales servicios de una red no es un procedimiento simple y no está exento de dificultades.

CONCLUSIONES

Como resultado de la encuesta se tiene que Ubuntu, seguido por Debian son los sistemas operativos de distribuciones Linux más utilizados, por lo que sugerimos para la migración **Ubuntu 12.04 LTS** en el cual montamos los servicios de DNS, DHCP, correo e internet. Es necesario destacar que Zentyal tiene como sistema operativo base Ubuntu 12.04 LTS.

Analizamos la creación de dominios usando Samba 3 + LDAP, Samba 4, Samba 4 con Windows 2003 Server y Zentyal 3.0.2, de este estudio concluimos lo siguiente:

1. Samba 3 con LDAP se recomienda para aquellos lugares en que tienen administradores bien experimentados con Linux.
2. Samba 4 no se recomienda hasta que sea estable.
3. Para las PYMEs proponemos Zentyal, por las facilidades gráficas, la integración de un gran número de servicios, su estabilidad y el soporte de la comunidad internacional.

Se implementaron los servidores por medio de máquinas virtuales realizando la simulación del sistema completo y comprobando el correcto funcionamiento de los servicios en todos los casos.

Como resultado general se plantea que este trabajo sirve de guía o manual de ayuda para qué personas con pocos conocimientos de administración puedan enfrentar la tarea de implementar un dominio con software libre y servicios básicos de una manera fácil.

RECOMENDACIONES

- Continuar este trabajo de manera que se perfeccionen las configuraciones de los servicios instalados y se adicionen nuevos servicios.
- Profundizar en el trabajo con Samba 4 que aunque no está disponible actualmente como versión estable se espera su liberación oficial en un corto plazo de tiempo.
- Divulgar este trabajo en centros que están migrando al software libre y no cuentan con administradores experimentados.

REFERENCIAS BIBLIOGRÁFICAS

1. Burgess, M., *Principles of Network and System Administration*. Second Edition ed. 2004.
2. Foundation, L. *Linux está alcanzando nuevos niveles en las empresas, según estudio*. 2012; Available from: http://pro.pcworld.pe/noticias/linux-esta-alcanzando-nuevos-niveles-en-empresas-segun-estudio/.
3. Ubuntu-Documents, O.S.f. *Serverguide Ubuntu 10.04*. 2010.
4. Internet. *Como Instalar y Configurar un Servidor DHCP*. Available from: http://www.guatewireless.org/os/linux/distros/debian/ubuntu/como-instalar-y-configurar-un-servidor-dhcp-en-linux-ubuntu-debian/.
5. Jelmer R. Vernooij, J.H.T., and Gerald Carter, *The Official samba 3.2.x HOWTO and Reference Guide*, 2008.
6. Wikipedia. *Servicio de directorio* 2012; Available from: http://es.wikipedia.org/wiki/Servicio_de_directorio.
7. Wikipedia. *POP3*. Available from: http://es.wikipedia.org/wiki/POP3.
8. Dent, K.D., *Postfix, The Definitive Guide*. 2003: O´Reilly.
9. Wikipedia. *Proxy*. Available from: http://es.wikipedia.org/wiki/Proxy.
10. Wessels, D., *Squid: The Definitive Guide*, 2004, O´Reilly.
11. Zentyal. Available from: http://www.zentyal.com/.
12. Internet. *Estudio fallos de seguridad*. Available from: http://enise.inteco.es/enise2009/images/stories/Ponencias/T25/marcos%20polanco.pdf.
13. Internet. *Lista de compatibilidad de hardware de Ubuntu Linux*. Available from: http://www.ubuntu.com/certification/catalog.
14. Wikipedia. Available from: http://es-wikipedia.org/wiki/Ubuntu#mw-head.

15. Ubuntu. *Zentyal*. Available from: https://help.ubuntu.com/12.04/serverguide/zentyal.html.

16. Zentyal. *Primeros pasos con Zentyal*. Available from: http://doc.zentyal.org/es/firststeps.html.

17. *BIND*. Available from: http://www.isc.org/software/bind.

18. Zentyal. *Servicio de resolución de nombres de dominio (DNS)*. Available from: http://doc.zentyal.org/es/dns.html.

19. *DHCP*. Available from: http://www.isc.org/software/dhcp.

20. Zentyal. *Servicio de configuración de red (DHCP)*. Available from: http://doc.zentyal.org/es/dhcp.html.

21. Zentyal. *Servicio de directorio (LDAP)*. Available from: http://doc.zentyal.org/es/directory.html.

22. Zentyal. *Servicio de compartición de ficheros y de autenticación*. Available from: http://doc.zentyal.org/es/filesharing.html.

23. Zentyal. *Servicio de correo electrónico (SMTP/POP3-IMAP4)*. Available from: http://doc.zentyal.org/es/mail.html.

24. Zentyal. *Servicio de correo web*. Available from: http://doc.zentyal.org/es/webmail.html.

BIBLIOGRAFÍA

BURGESS, M. 2004. Principles of Network and System Administration.

CATER, G. 2003. LDAP System Administration. O´Reilly.

DANTE ORDÍN RAMÍREZ LÓPEZ, C. C. M. 2011. El Cifrado Web (SSL/TLS). Available: http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls.

DENT, K. D. 2003. Postfix, The Definitive Guide, O´Reilly.

DONAHUE, G. A. 2007. Network Warrior. O´Reilly.

H.TERPSTRA, J. 2008. Samba-3 by Example.

HAGEN, W. V. 2007. Ubuntu Linux Bible. Wiley Publishing, Inc.

HUNT, C. Linux Network Servers.

JELMER R. VERNOOIJ, J. H. T., AND GERALD CARTER 2008. The Official samba 3.2.x HOWTO and Reference Guide.

KOETTER, R. H. A. P. 2005. The Book of Postfix State-of -The-Art Message Transaport.

O´REILLY. Available: http://www.oreillynet.com/lpt/a/6849.

SAMS 2000. Maximum Linux Security.

SMITH, R. W. 2001. Linux Samba Server Administration.

SMITH, R. W. 2002. Linux Samba Server Administration. SYBEX Inc.

TANENBAUM, A. S. 2003. Computer Networks.

UBUNTU DOCUMENTATION TEAM, 2010, Ubuntu Server Guide.

UBUNTU DOCUMENTATION TEAM, 2012, Ubuntu Server Guide.

WESSELS, D. 2004. Squid: The Definitive Guide. O´Reilly.

SITIOS WEB CONSULTADOS

- https://launchpad.net/~ubuntu-core-doc
- https://launchpad.net/~ubuntu-server
- https://help.ubuntu.com/community/
- https://code.launchpad.net/serverguide
- https://code.launchpad.net/ubuntu-docs
- http://www.serverworld.net
- http://www.openldap.org
- http://www.zentyal.com
- http://www.serverfault.net
- http://sun.com/software/products/directory_srvr-ee/
- http://www.blogwindows.com/%C2%BFactive-directory-o-ldap-openldap/122/
- http://www.guatewireless.org/os/linux/distros/debian/ubuntu/como-instalar-y-configurar-un-servidor-dhcp-en-linux-ubuntu-debian/
- http://es.tldp.org/COMO-INSFLUG/COMOs/LDAP-Linux-Como/
- https://help.ubuntu.com/11.04/serverguide/C/postfix.html
- http://www.kriptopolis.org/seguridad-en-servidores-windows-vs-linux
- http://www.servidoresdedicados.com/
- http://www.servidoresdedicados.com/linux-windows.asp
- http://www.squid-cache.org/
- https://launchpad.net/ufw
- http://es.wikipedia.org
- http://www.tufuncion.ccom/windows-vs-linux/
- http://www.entmexico.com/hosting/windows-o-linux.html
- http://es.wikipedia.org/wiki/OpenLDAP
- http://es.wikipedia.org/wiki/Proxy
- http://www.samba.org

ANEXOS

Anexo I Manual de instalación Controlador de Dominio con Samba 3

Es muy importante que el administrador de cualquier empresa siga el orden lógico que se muestra a continuación para la instalación de los servidores PDC y BDC. Primeramente se instala el sistema operativo deseado para el servidor, en este caso ***Ubuntu Server 12.04 LTS***, después hay que configurar la red para reflejar una dirección IP estática en el archivo */etc/network/interfaces*. Posteriormente se comprueba la conectividad con el repositorio y se actualiza el sistema operativo.

En el ejemplo que proponemos usamos los siguientes parámetros:

Dominio: jose.com

Servidor primario (PDC): 10.12.16.200

Servidor segundario (BDC): 10.12.16.240

Servidores DNS superiores: 10.12.1.51 y 10.12.1.52

Nombre del servidor de correo: mail con IP 10.12.16.200

Algunos ajustes antes de instalar

Es necesario realizar algunas modificaciones en ambos servidores adaptando a cada uno sus valores como nombre y dirección IP:

- Compruebe que en */etc/hostname* haya algo como lo siguiente, recuerde que debe coincidir con sus datos:

  ```
  PDC.jose.com
  ```

  Note que consiste en *[nombre corto del servidor].[dominio]*

- Compruebe que */etc/hosts* este de la siguiente forma:

  ```
  127.0.0.1       localhost.localdomain       localhost
  10.12.16.200    PDC.jose.com        PDC
  ```

- Reinicie el servicio para que los cambios tengan efecto:

  ```
  root@PDC:~# /etc/init.d/hostname restart
  ```

- Por último compruebe que los comandos hostname y hostname –f devuelven lo mismo que sería *[nombre corto del servidor].[dominio]*, en nuestro caso el resultado de estos comandos sería *PDC.jose.com*

Poniendo los servidores en marcha

- Cree el servidor primario, instale Bind 9:

  root@PDC:~# apt-get install bind9 bind9-doc -y

  Esto instalará los archivos de configuración dentro de ***/etc/bind***

- Después edite el fichero */etc/bind/named.conf.options* para especificar las direcciones IP de los servidores de nombre superiores a los nuestros.

```
options {
    directory "/var/cache/bind";
    forwarders {
        10.12.1.51;
        10.12.1.52;
    };
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
    allow-recursion { localnets; };
}
```

- Especifíquele al Bind 9 todos los dominios de su red mediante el archivo ubicado en */etc/bind/named.conf.local*, la configuración que les mostramos a continuación es para el servidor primario.

```
zone "jose.com" IN {
   type master;
   file "/etc/bind/db.jose.com";
   allow-transfer {10.12.16.240; };
   notify yes;
};
zone "16.12.10.in-addr.arpa" IN {
```

```
    type  master;
    file "/etc/bind/rev.in-addr.arpa";
    allow-transfer {10.12.16.240; };
    notify yes;
};
```

Quedando de la siguiente forma en el servidor segundario:

```
zone "jose.com" IN {
    type slave;
    file "db.jose.com";
    masters {10.12.16.200; };
    allow-notify {10.12.16.200; };
};
zone "16.12.10.in-addr.arpa" IN {
    type slave;
    file "rev.in-addr.arpa";
    masters {10.12.16.200; };
    allow-notify {10.12.16.200; };
};
```

Note los caminos relativos a los archivos de zona, esto se debe a que el directorio de trabajo del Bind 9 por defecto se encuentra en ***/var/cache/bind*** y las salvas de los archivos de zona serán almacenadas allí.

- Ahora cree los archivos de zona en */etc/bind/db.jose.com* (zona directa) y */etc/bind/rev.in-addr.arpa* (zona inversa), haga los cambios para que los nombres coincidan con los valores que usted está usando en el caso de la zona directa. Esto solo se hace en el servidor primario, ya que estos archivos serán transferidos automáticamente mediante la réplica al servidor segundario cuando terminemos la configuración y reiniciemos el Bind 9.

  El archivo de zona directa debe quedar de la siguiente forma:

```
$TTL 60
@       IN      SOA     PDC.jose.com. root.jose.com. (
                        20130101 ; Serial
```

```
                        1w ; Refresh
                        1d ; Retry
                        4w ; Expire
                        1w ) ; Negative Cache TTL
;
@       IN      NS      PDC.jose.com.
@       IN      NS      BDC.jose.com.
@       IN      A       10.12.16.200
@       IN      MX      10 mail.jose.com.

PDC     IN      A       10.12.16.200
BDC     IN      A       10.12.16.240
mail    IN      A       10.12.16.200
```

El archivo de zona inversa:

```
$TTL 604800     ; 1 week
@       IN      SOA     PDC.jose.com. root.jose.com. (
                        20130101 ; Serial
                        1w ; Refresh
                        1d ; Retry
                        4w ; Expire
                        1w ) ; Negative Cache TTL
;
@       IN      NS      PDC.jose.com.
@       IN      NS      BDC.jose.com.
200     IN      PTR     PDC.jose.com.
240     IN      PTR     BDC.jose.com.
200     IN      PTR     mail.jose.com.
```

- Actualice */etc/resolv.conf* para preguntarle al localhost por los servidores de nombre. Recordemos que en **Ubuntu 12.04** *resolv.conf* es un link simbólico a */run/resolvconf/resolv.conf* (para comprobar sudo ls -l /etc/resolv.conf) por lo tanto, debemos borrar el link con el siguiente comando.

root@PDC:~# sudo rm -rf /etc/resolv.conf

- Cree un nuevo fichero:

root@PDC:~# sudo nano /etc/resolv.conf

- Y edítelo para que contenga lo siguiente:

```
nameserver 10.12.16.200
nameserver 10.12.16.240
search jose.com
```

- Reinicie Bind 9

root@PDC:~# /etc/init.d/bind9 restart

- Y chequee que está trabajando:

root@PDC:~# nslookup jose.com
root@PDC:~# dig jose.com
root@PDC:~# dig –x 127.0.0.1
root@PDC:~# host PDC.jose.com

Poniendo los servidores de nombre en un ambiente Chroot

Para incrementar la seguridad, es tiempo de poner a correr los servidores de nombre dentro de una ambiente seguro a fin de que nadie pueda ver el resto de los archivos del sistema.

- Cree el ambiente chroot:

root@PDC:~# mkdir -p /chroot/bind/dev
root@PDC:~# mkdir -p /chroot/bind/etc/bind
root@PDC:~# mkdir -p /chroot/bind/var/run/named
root@PDC:~# mkdir -p /chroot/bind/var/cache/bind

- Copie los archivos de configuración del Bind 9 dentro de la celda chroot:

root@PDC:~# cp /etc/bind/* /chroot/bind/etc/bind

- Cree los dispositivos que el Bind 9 requiere:

root@PDC:~# mknod /chroot/bind/dev/null c 1 3
root@PDC:~# mknod /chroot/bind/dev/random c 1 8

- Establezca los derechos y permisos sobre los archivos.

root@PDC:~# chown -R bind:bind /chroot/bind/etc
root@PDC:~# chown -R bind:bind /chroot/bind/var/run
root@PDC:~# chown -R bind:bind /chroot/bind/var/cache

- Modifique el archivo */etc/default/bind9* para poner Bind 9 a correr dentro de la celda chroot:

```
OPTIONS="-u bind -t /chroot/bind"
RESOLVCONF=yes
```

- Copie la librería OpenSSL dentro de la celda chroot:

root@PDC:~# mkdir -p /chroot/bind/usr/lib/i386-linux-gnu/openssl-1.0.0/engines
root@PDC:~# cp /usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgost.so /chroot/bind/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/

- Detenga AppArmor para modificar el archivo */etc/apparmor.d/usr.sbin.named* e incluya estas líneas al final del archivo y muy importante dentro de las llaves:

root@PDC:~# /etc/init.d/apparmor stop

```
# Additional permissions for a chrooted bind
 /chroot/bind/etc/bind/** r,
 /chroot/bind/var/lib/bind/** rw,
 /chroot/bind/var/lib/bind/ rw,
 /chroot/bind/var/cache/bind/** rw,
 /chroot/bind/var/cache/bind/ rw,
 /chroot/bind/var/run/named/named.pid w,
 /chroot/bind/var/run/named/session.key w,
 # support for resolvconf
 /chroot/bind/var/run/bind/named.options r,

 # Allow access to copies of OpenSSL libraries (Ubuntu 12.04)
```

```
/chroot/bind/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/** rm,
/chroot/bind/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/ rm,
```

- Por último reinicie Apparmor y Bind 9:

```
root@PDC:~# /etc/init.d/apparmor restart
root@PDC:~# /etc/init.d/bind9 restart
```

Chequee ***/var/log/syslog*** y vea los mensajes del Bind 9 al reiniciar, leyendo los archivos de zona, enviando y recibiendo notificaciones. Compruebe que todo funciona correctamente.

Repita lo anterior en el servidor segundario teniendo en cuenta que en este no se configuran los archivos de zonas.

Comandos para comprobar el correcto funcionamiento del DNS

- ✓ nslookup nombre_de_dominio
- ✓ dig nombre_de_dominio
- ✓ dig –x IP_servidordns
- ✓ ping
- ✓ host –t a nombre_del_servidor
- ✓ host –t cname alias_del_servidor
- ✓ named-checkzone

Servidor OpenLDAP

En el ejemplo que proponemos usamos los siguientes parámetros:

Dominio: dc=jose,dc=com

Usuario administrador del LDAP: cn=admin,dc=jose,dc=com

Contraseña: “ok”

Instalando LDAP

- Instale LDAP mediante el siguiente comando:

```
root@PDC:~# sudo apt-get install slapd ldap-utils -y
```

Esto instalará los archivos de configuración dentro de ***/etc/ldap***

- Cree el archivo *log.ldif* con el siguiente contenido:

```
dn: cn=config
changetype: modify
add: olcLogLevel
olcLogLevel: stats
```

- Añada el archivo *log.ldif* al ldap

root@PDC:~# sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f log.ldif

Hasta el momento tenemos el servidor OpenLDAP funcionando, es hora de usarlo para la autenticación de usuarios instalando los siguientes paquetes:

root@PDC:~# sudo apt-get install libnss-ldap -y

- Durante la instalación será necesario responder las preguntas de la siguiente forma:

```
ldap://127.0.0.1
dc=jose,dc=com
3
Yes
No
cn=admin,dc=jose,dc=com
ok (contraseña)
```

Si comete algún error puede solucionarlo ejecutando el comando sudo dpkg-reconfigure ldap-auth-config.

- Ahora configure los perfiles LDAP para NSS (Network Switching Subsystem o Subsistema de Conmutación de Red)

root@PDC:~# sudo auth-client-config -t nss -p lac_ldap

- Finalmente use ldap para la autenticación:

root@PDC:~# sudo pam-auth-update

- Compruebe que el fichero */etc/ldap.conf* contiene lo siguiente:

```
host 127.0.0.1
```

```
base dc=jose,dc=com
uri ldap://127.0.0.1/
rootbinddn cn=admin,dc=jose,dc=com
ldap_version 3
bind_policy soft
```

- Finalmente cree el fichero *indices.ldif* y añada lo siguiente para agilizar las búsquedas en la base de datos ldap:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uid eq,pres,sub
```

- Añádalos con el siguiente comando:

root@PDC:~# sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f indices.ldif

Comandos para comprobar el correcto funcionamiento de OpenLDAP

- ✓ slaptest
- ✓ ldapsearch

Instalando samba

Para este ejemplo hemos usado los siguientes parámetros:

Dominio: dc=jose,dc=com

Usuario administrador del LDAP: cn=admin,dc=jose,dc=com

Contraseña: “ok”

- Instalemos los siguientes paquetes:

root@PDC:~# sudo apt-get install samba samba-doc libpam-smbpass smbclient smbldap-tools -y

- El siguiente paso es copiar el archivo comprimido ldif que contiene los esquemas de samba

root@PDC:~# sudo cp /usr/share/doc/samba-doc/examples/LDAP/samba.ldif.gz ~

- Luego descompactamos el archivo con el siguiente comando:

root@PDC:~# sudo gzip -d ~/samba.ldif.gz

- Agregamos los datos ldif a la base de datos del ldap:

root@PDC:~# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f samba.ldif

- Añadamos algunos índices de samba, para ello crearemos el archivo *smb_indices.ldif* y añadamos lo siguiente:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

- Añadamos estos índices:

root@PDC:~# sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f smb_indices.ldif

- Copiemos los ejemplos de los ficheros de configuración de ***samba-tools*** para trabajar sobre ellos:

root@PDC:~# cp /usr/share/doc/smbldap-tools/examples/{smbldap.conf.gz,smbldap_bind.conf} /etc/smbldap-tools/

- Descompactemos el fichero *smbldap.conf*:

root@PDC:~# gzip -d /etc/smbldap-tools/smbldap.conf.gz

- Editémoslo de la siguiente forma, recuerde que debe coincidir con sus datos:

```
slaveDN="cn=admin,dc=jose,dc=com"
slavePw="ok"
masterDN="cn=admin,dc=jose,dc=com"
masterPw="ok"
```

- Con el siguiente comando obtendremos el SID de samba, lo copiamos y editamos */etc/smbldap-tools/smbldap.conf* comprobando lo siguiente:

root@PDC:~# sudo net getlocalsid
root@PDC:~# nano /etc/smbldap-tools/smbldap.conf

```
SID="S-1-5-21-2252255531-4061614174-2474224977"
sambaDomain="JOSE"
slaveLDAP="127.0.0.1"
masterLDAP="127.0.0.1"
ldapTLS="0"
suffix="dc=jose,dc=com"
userHome="/profiles/%U"
```

- Y reiniciamos OpenLDAP:

root@PDC:~# service slapd restart

- Lo siguiente es configurar samba, copiaremos una platilla del fichero de configuración:

root@PDC:~# cp /usr/share/doc/smbldap-tools/examples/smb.conf.example /etc/samba/

- Editamos el fichero nano */etc/samba/smb.conf.example* de la siguiente forma:

```
[global]
        workgroup = JOSE
        netbios name = PDC
        server string = %h server (Samba Server)
```

```
        wins support = yes
        log level = 1
        log file = /var/log/samba/log.%m
        max log size = 5000
        debug pid = yes
        debug uid = yes
        syslog = 0
        utmp = yes
        security = user
        domain logons = yes
        domain master = yes
        os level = 64
        logon path =
        logon home =
        logon drive =
        logon script =
        passdb backend = ldapsam:"ldap://127.0.0.1/"
        ldap ssl = no
        ldap admin dn = cn=admin,dc=jose,dc=com
        ldap delete dn = no
        ldap password sync = yes
        ;ldap password sync = no
        ;unix password sync = yes
        ;passwd program = /usr/sbin/smbldap-passwd -u '%u'
        ;passwd chat = "Changing *\nNew password*" %n\n "*Retype new password*"
%n\n"
        ldap suffix = dc=jose,dc=com
        ldap user suffix = ou=Users
        ldap group suffix = ou=Groups
        ldap machine suffix = ou=Computers
        ldap idmap suffix = ou=Idmap
        add user script = /usr/sbin/smbldap-useradd -m '%u'
        rename user script = /usr/sbin/smbldap-usermod -r '%unew' '%uold'
        delete user script = /usr/sbin/smbldap-userdel '%u'
```

```
        set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
        add group script = /usr/sbin/smbldap-groupadd -p '%g'
        delete group script = /usr/sbin/smbldap-groupdel '%g'
        add user to group script = /usr/sbin/smbldap-groupmod -m '%u' '%g'
        delete user from group script = /usr/sbin/smbldap-groupmod -x '%u' '%g'
        add machine script = /usr/sbin/smbldap-useradd -w '%u'
[HOMES]
        comment = Home Directories
        browseable = yes
        valid users = %U
        writable = yes
        create mask = 0700
        directory mask = 0700
[NETLOGON]
        comment = Network Logon Service
        path = /var/lib/samba/netlogon
        admin users = root
        guest ok = yes
        browseable = no
[PROFILES]
        path = /var/lib/samba/profiles
        browseable = no
        writeable = yes
        create mask = 0611
        directory mask = 0700
```

- Ahora reemplazemos el archivo de configuración de samba con el que modificamos:

```
root@PDC:~# cp /etc/samba/smb.conf.example /etc/samba/smb.conf
```

- Reiniciamos ldap y samba:

```
root@PDC:~# service slapd restart
root@PDC:~# service smbd restart
root@PDC:~# service nmbd restart
```

- Pongámosle la contraseña de samba al administrador del ldap, recuerde cambiarla para que coincida con la que usted está usando:

root@PDC:~# sudo smbpasswd –w ok

- Ahora creamos la estructura de directorio adecuada para las maquinas Windows en Ldap.

root@PDC:~# sudo smbldap-populate

- Si nos devuelve algún error del PERL (**P**ractical **E**xtraction and **R**eport **L**anguage - *Lenguaje Práctico para la Extracción e Informe)* editemos el archivo */usr/share/perl5/smbldap_tools.pm* y cambiemos lo siguiente:

```
qw(ALRM INT HUP QUIT TERM TSTP TTIN TTOU)
Por
(qw(ALRM INT HUP QUIT TERM TSTP TTIN TTOU))
```

- Ahora crearemos los directorios profiles y netlogon:

root@PDC:~# mkdir -v -m 777 /var/lib/samba/profiles
root@PDC:~# mkdir -v -p -m 777 /var/lib/samba/netlogon

Réplica del LDAP

En el PDC

- Edite el fichero */etc/apparmor.d/usr.sbin.slapd*

root@PDC:~# nano /etc/apparmor.d/usr.sbin.slapd

- Y añada lo siguiente:

```
/var/lib/ldap/accesslog/ r,
/var/lib/ldap/accesslog/** rwk,
```

- Reinicie apparmor

root@PDC:~# sudo -u openldap mkdir /var/lib/ldap/accesslog
root@PDC:~# sudo -u openldap cp /var/lib/ldap/DB_CONFIG /var/lib/ldap/accesslog/

root@PDC:~# sudo /etc/init.d/apparmor reload

- Verifiquemos que en el *provider_sync.ldif* este bien el siguiente parámetro

```
olcRootDN: cn=admin,dc=jose,dc=com
```

- Añadamos el archivo *provider_sync.ldif* con el siguiente contenido (recuerde ajustarlo a los valores que ested este usando):

```
# Add indexes to the frontend db.
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

#Load the syncprov and accesslog modules.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov
-
add: olcModuleLoad
olcModuleLoad: accesslog

# Accesslog database definitions
dn: olcDatabase={2}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap/accesslog
olcSuffix: cn=accesslog
olcRootDN: cn=admin,dc=jose,dc=com
```

```
olcDbIndex: default eq
olcDbIndex: entryCSN,objectClass,reqEnd,reqResult,reqStart

# Accesslog db syncprov.
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE

# syncrepl Provider for primary db
dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE

# accesslog overlay definitions for primary db
dn: olcOverlay=accesslog,olcDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcAccessLogConfig
olcOverlay: accesslog
olcAccessLogDB: cn=accesslog
olcAccessLogOps: writes
olcAccessLogSuccess: TRUE
# scan the accesslog DB every day, and purge entries older than 7 days
olcAccessLogPurge: 07+00:00 01+00:00
```

root@PDC:~# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f provider_sync.ldif

- Por ultimo reiniciemos slapd:

root@PDC:~# sudo /etc/init.d/slapd restart

En el BDC

- Modifiquemos el archivo */etc/samba/smb.conf*, cambiando (wins support = no, domain master= no,)
- Lo siguiente es copiar el SID de samba del servidor primario en el segundario, este dato aparece en el fichero */etc/smbldap-tools/smbldap.conf* en el servidor primario:
- Añadamos el archivo *consumer_sync.ldif* con el siguiente contenido:

```
#Load the syncprov module.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov

# syncrepl specific indices
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID eq
-
add: olcSyncRepl
olcSyncrepl: {0}rid=0  provider=ldap://PDC.jose.com:389 bindmethod=simple
 binddn="cn=admin,dc=jose,dc=com"
 credentials=ok
 searchbase="dc=jose,dc=com"
 logbase="cn=accesslog"
  logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
 schemachecking=on
 type=refreshAndPersist
 retry="60 +"
 syncdata=accesslog
```

```
-
add: olcUpdateRef
olcUpdateRef: ldap:// PDC.jose.com
```

root@BDC:~# sudo ldapadd -c -Y EXTERNAL -H ldapi:/// -f consumer_sync.ldif

- Reiniciemos el servidor segundario:

root@BDC:~# shutdown -r now

TLS (Transport Layer Security)

- Usaremos los siguientes paquetes:

root@PDC:~# sudo apt-get install gnutls-bin -y

- Creando una llave privada para el Certificado de Autoridad

root@PDC:~# sudo sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"

- Creando la plantilla */etc/ssl/ca.info* para definir el Certificado de Autoridad

```
cn = Jose Company
ca
cert_signing_key
```

- Creando certificados:

```
root@PDC:~# sudo certtool --generate-self-signed \
--load-privkey /etc/ssl/private/cakey.pem \
--témplate /etc/ssl/ca.info \
--otile /etc/ssl/certs/cacert.pem
```

- Haciendo una llave privada para el servidor:

```
root@PDC:~# sudo certtool --generate-privkey \
--bits 1024 \
--outfile /etc/ssl/private/ldap01_slapd_key.pem
```

- Crearemos el fichero */etc/ssl/ldap01.info* con lo siguiente:

```
organization = Jose Company
cn = ldap01.jose.com
tls_www_server
encryption_key
signing_key
expiration_days = 3650
```

- Creando el certificado para el servidor:

```
root@PDC:~# sudo certtool --generate-certificate \
--load-privkey /etc/ssl/private/ldap01_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/ldap01.info \
--outfile /etc/ssl/certs/ldap01_slapd_cert.pem
```

- Crearemos el fichero *certinfo.ldif* con lo siguiente:

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap01_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap01_slapd_key.pem
```

- Añadámoslo con el siguiente comando:

```
root@PDC:~# sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/ssl/certinfo.ldif
```

- Ajustando permisos:

```
root@PDC:~# sudo adduser openldap ssl-cert
root@PDC:~# sudo chgrp ssl-cert /etc/ssl/private/ldap01_slapd_key.pem
root@PDC:~# sudo chmod g+r /etc/ssl/private/ldap01_slapd_key.pem
```

root@PDC:~# sudo chmod o-r /etc/ssl/private/ldap01_slapd_key.pem

- Reiniciamos OpenLDAP:

root@PDC:~# sudo service slapd restart

Replica y TLS

- En el Proveedor crearemos el siguiente directorio:

root@PDC:~# mkdir ldap02-ssl
root@PDC:~# cd ldap02-ssl
sudo certtool --generate-privkey \
--bits 1024 \
--outfile ldap02_slapd_key.pem

- Crearemos el archivo *ldap2.info* con lo siguiente:

```
organization = Jose Company
cn = ldap02.jose.com
tls_www_server
encryption_key
signing_key
expiration_days = 3650
```

- Es tiempo de crear el certificado del Consumidor:

root@PDC:~# sudo certtool --generate-certificate \
--load-privkey ldap02_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template ldap02.info \
--outfile ldap02_slapd_cert.pem

- Haremos una copia de los certificados:

root@PDC:~# cp /etc/ssl/certs/cacert.pem

- Ahora es tiempo de transferir el directorio ***ldap02-ssl*** para el Consumidor, usaremos scp (Secure Copy Protocol)

root@PDC:~# cd ..
root@PDC:~# scp -r ldap02-ssl user@consumer:

- Editemos */etc/ldap/ldap.conf* de la siguiente forma:

```
TLS_CERT /etc/ssl/certs/ldap01_slapd_cert.pem
TLS_KEY /etc/ssl/private/ldap01_slapd_key.pem
TLS_CACERT /etc/ssl/certs/cacert.pem
```

- En el Consumidor configuraremos TLS

root@BDC:~# sudo apt-get install ssl-cert
root@BDC:~# sudo adduser openldap ssl-cert
root@BDC:~# cd ldap02-ssl
root@BDC:~# sudo cp ldap02_slapd_cert.pem cacert.pem /etc/ssl/certs
root@BDC:~# sudo cp ldap02_slapd_key.pem /etc/ssl/private
root@BDC:~# cd ..
root@BDC:~# sudo chgrp ssl-cert /etc/ssl/private/ldap02_slapd_key.pem
root@BDC:~# sudo chmod g+r /etc/ssl/private/ldap02_slapd_key.pem
root@BDC:~# sudo chmod o-r /etc/ssl/private/ldap02_slapd_key.pem

- Crearemos el fichero *certinfo.ldif* con lo siguiente:

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap02_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap02_slapd_key.pem
```

- El siguiente paso es añadirlo con el comando:

root@BDC:~# sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f certinfo.ldif

- Añadamos el archivo *consumer_sync_tls.ldif* con el siguiente contenido:

```
dn: olcDatabase={1}hdb,cn=config
replace: olcSyncrepl
olcSyncrepl: {0}rid=0  provider=ldap://PDC.jose.com bindmethod=simple
 binddn="cn=admin,dc=jose,dc=com"
 credentials=ok
 searchbase="dc=jose,dc=com"
 logbase="cn=accesslog"
  logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
 schemachecking=on
 type=refreshAndPersist
 retry="60 +"
 syncdata=accesslog
 starttls=yes
```

root@BDC:~# sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f consumer_sync_tls.ldif

- Editemos */etc/ldap/ldap.conf* de la siguiente forma:

```
TLS_CERT /etc/ssl/certs/ldap02_slapd_cert.pem
TLS_KEY /etc/ssl/private/ldap02_slapd_key.pem
TLS_CACERT /etc/ssl/certs/cacert.pem
```

- Por ultimo reiniciemos LDAP

root@BDC:~# sudo service slapd restart

Para comprobar que todo funciona correctamente chequee **/var/log/syslog**.

- Ppor último instalemos LDAP Account Manager (LAM), herramienta de administración del LDAP (Vea Anexo IV Configuración de la aplicación LDAP Account Manager (LAM))

Anexo II Manual de instalación Controlador de Dominio con Samba 4

La versión que usamos es Ubuntu 12.04.1, asumimos que usted tiene un conocimiento mínimo que le permita configurar Ubuntu a líneas de comando. No explicaremos al detalle.

En el ejemplo que proponemos usamos los siguientes parámetros:

Dominio: jose.com

Rango IP: 10.12.16.0/24

Servidor primario (PDC): 10.12.16.200

Servidor segundario (BDC): 10.12.16.240

Servidor DNS superior: 10.12.1.51

Contraseña: "Josh 2013"

Algunos ajustes antes de instalar

Configure su interfaz de red */etc/network/interfaces* para usar una dirección estática adaptándola a sus valores, el ejemplo que proponemos es para el servidor primario, para el segundario es de igual forma solo cambiando la dirección IP:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
        address         10.12.16.200
        netmask         255.255.255.0
        network         10.12.16.0
        gateway         10.12.16.254
        broadcast       10.12.16.255
        dns-search      jose.com
        dns-nameservers 10.12.16.200 10.12.16.240
```

Compruebe que en */etc/hostname* haya algo como lo siguiente, recuerde que debe coincidir con sus datos:

PDC.jose.com

Note que consiste en *[nombre corto del servidor].[dominio]*

Compruebe que */etc/hosts* este de la siguiente forma:

127.0.0.1 localhost.localdomain localhost

10.12.16.200 PDC.jose.com PDC

Reinicie la red (networking) y el nombre de la máquina (hostname) para que los cambios tengan efecto.

Por último compruebe que los comando hostname y hostname –f devuelven lo mismo que sería *[nombre corto del servidor].[dominio]*, en nuestro caso el resultado de estos comandos sería *PDC.jose.com.* También chequee que */etc/resolv.conf* contenga nuestros servidores de nombre y dominio.

Es importante señalar que estos ajustes se hacen tanto en el servidor primario como en el segundario adaptando a cada uno sus valores.

Instalación en el servidor primario

Instalando Samba 4

Instale el siguiente paquete:

root@PDC:~# apt-get install samba4 –y

La instalación dará un error, pero no nos afecta, solo tendremos que arreglar el paquete editando */var/lib/dpkg/status*, dentro buscamos "Package: samba4″ y reemplazamos "half-configured" con "installed".

Ahora construiremos el Directorio Activo del Dominio, pero primero tendremos que eliminar el archivo de configuración de samba ubicado en */etc/samba/smb.conf*.

root@PDC:~# rm /etc/samba/smb.conf

Para crear el dominio se hace lo siguiente:

root@PDC:~# /usr/share/samba/setup/provision

Estableciendose una sesion interactiva donde nos piden los datos necesarios para la configuración del dominio. También pueden darse esos datos de una vez con la siguiente línea de comando:

```
root@PDC:~# /usr/share/samba/setup/provision --realm=jose.com --domain=JOSE --adminpass='Josh 2013' --server-role=dc
```

El siguiente paso es iniciar Samba:

```
root@PDC:~# rm /etc/samba/smb.conf
```

Para probar la instalación utilizaremos el cliente de Samba 4:

```
root@PDC:~# apt-get install samba4-clients –y
```

Al ejecutar el siguiente comando debe mostrarnos:

```
root@PDC:~# smbclient -L localhost -U%
```

```
Sharename       Type       Comment
---------       ----       -------
netlogon        Disk
sysvol          Disk
IPC$            IPC        IPC Service
```

Servidor DNS Bind

Necesitamos un servidor de nombre en nuestra red para resolver los hosts y servicios en la red. Samba 4 instala por defecto *Bind 9*. Es tiempo ahora de configurarlo.

Edite */etc/bind/named.conf* y añada la siguiente línea al final:

```
include "/var/lib/samba/private/named.conf";
```

Como Ubuntu usa AppArmor para asegurar sus servicios tenemos que garantizar que Bind 9 tiene los permisos para acceder a los archivos provistos por samba, editando el fichero */etc/apparmor.d/usr.sbin.named* añadiendo al final lo siguiente, dentro de los paréntesis:

Si su sistema operativo es de 32 bits:

```
/var/lib/samba/private/** rkw,
```

```
/var/lib/samba/private/dns/** rkw,
/usr/lib/i386-linux-gnu/samba/bind9/** rm,
/usr/lib/i386-linux-gnu/samba/gensec/** rm,
/usr/lib/i386-linux-gnu/ldb/modules/ldb/** rm,
/usr/lib/i386-linux-gnu/samba/ldb/** rm,
```

Si es de 64 bits:

```
/var/lib/samba/private/** rkw,
/var/lib/samba/private/dns/** rkw,
/usr/lib/x86_64-linux-gnu/samba/bind9/** rm,
/usr/lib/x86_64-linux-gnu/samba/gensec/** rm,
/usr/lib/x86_64-linux-gnu/ldb/modules/ldb/** rm,
/usr/lib/x86_64-linux-gnu/samba/ldb/** rm,
```

Cargue la configuración para que tenga efecto:

```
root@PDC:~# /etc/init.d/apparmor reload
```

Ahora es tiempo de reiniciar Bind 9:

```
root@PDC:~# /etc/init.d/bind9 restart
```

Y chequee que está trabajando:

```
root@PDC:~# host -t SRV _ldap._tcp.jose.com
root@PDC:~# host -t SRV _kerberos._tcp.jose.com
root@PDC:~# host -t A PDC.jose.com
```

Permitiremos las actualizaciones dinámicas para el DNS, queremos que los clientes puedan actualizar sus entradas de DNS automáticamente, para lograrlo añada lo siguiente en el fichero */etc/bind/named.conf.options*: (puede que necesite reemplazar *dnssec-validation auto* y comentar el parámetro *listen-on-v6 { any; };*)

```
tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
allow-query { any; };
allow-recursion { any; };
forwarders { 10.12.1.51; };
dnssec-validation no;
```

Si tiene otro Servidor DNS en la red que provee servicio para resolver nombres externos (*www.google.com*), entonces necesitará configurar Bind 9 para usar este DNS para resolver las entradas:

Primero deshabilitar IPv6 editando */etc/default/bind9* para que quede de la siguiente forma:

```
OPTIONS="-4 -u bind"
```

Reiniciemos Bind 9:

```
root@PDC:~# /etc/init.d/bind9 restart
```

Por últimos instale Kerberos

Ejecutamos el siguiente comando:

```
root@PDC:~# apt-get install krb5-user –y
```

Edite el fichero de configuración de kerberos */etc/krb5.conf*, para que quede de la siguiente forma:

Dentro de *realms* debe especificarse los servidores kdc y el que va a funcionar como primario (admins server):

```
[realms]
        JOSE.COM = {
                kdc = PDC.jose.com
                kdc = BDC.jose.com
                admin_server = PDC.jose.com
                default_domain = JOSE.COM
        }
```

Por último dentro de *domain_realm* al final debe especificarse el dominio de la siguiente forma:

```
[domain_realm]
        .mit.edu = ATHENA.MIT.EDU
        mit.edu = ATHENA.MIT.EDU
        .media.mit.edu = MEDIA-LAB.MIT.EDU
        media.mit.edu = MEDIA-LAB.MIT.EDU
```

```
.csail.mit.edu = CSAIL.MIT.EDU
csail.mit.edu = CSAIL.MIT.EDU
.whoi.edu = ATHENA.MIT.EDU
whoi.edu = ATHENA.MIT.EDU
.stanford.edu = stanford.edu
.slac.stanford.edu = SLAC.STANFORD.EDU
.jose.com = JOSE.COM
jose.com = JOSE.COM
```

Compruebe que kerberos funciona ejecutando el siguiente comando:

root@PDC:~# kinit administrator@JOSE.COM

Ya puede unir un cliente al dominio usando el usuario *administrator*.

Instalación en el servidor segundario

Instalando Samba 4

Instale el siguiente paquete:

root@BDC:~# apt-get install samba4 –y

La instalación dará un error, pero no nos afecta, solo tendremos que arreglar el paquete editando */var/lib/dpkg/status***,** dentro buscamos "Package: samba4″ y reemplazamos "half-configured" con "installed".

Ahora eliminaremos el archivo de configuración de samba ubicado en */etc/samba/smb.conf*:

root@BDC:~# rm /etc/samba/smb.conf

Poniendo a prueba la instalación:

root@BDC:~# apt-get install samba4-clients –y

Servidor DNS Bind

Necesitamos un servidor de nombre en la red para resolver los hosts y servicios en la red. Samba 4 instala por defecto *Bind 9*. Ahora configuremoslo.

Edite /etc/bind/named.conf y añada la siguiente línea al final:

```
include "/var/lib/samba/private/named.conf";
```

Como Ubuntu usa AppArmor para asegurar sus servicios tenemos que garantizar que Bind 9 tiene los permisos para acceder a los archivos provistos por samba, editando el fichero */etc/apparmor.d/usr.sbin.named* añadiendo al final lo siguiente, dentro de los paréntesis:

Si su sistema operativo es de 32 bits:

```
/var/lib/samba/private/** rkw,
/var/lib/samba/private/dns/** rkw,
/usr/lib/i386-linux-gnu/samba/bind9/** rm,
/usr/lib/i386-linux-gnu/samba/gensec/** rm,
/usr/lib/i386-linux-gnu/ldb/modules/ldb/** rm,
/usr/lib/i386-linux-gnu/samba/ldb/** rm,
```

Si es de 64 bits:

```
/var/lib/samba/private/** rkw,
/var/lib/samba/private/dns/** rkw,
/usr/lib/x86_64-linux-gnu/samba/bind9/** rm,
/usr/lib/x86_64-linux-gnu/samba/gensec/** rm,
/usr/lib/x86_64-linux-gnu/ldb/modules/ldb/** rm,
/usr/lib/x86_64-linux-gnu/samba/ldb/** rm,
```

Cargue la configuración para que tenga efecto:

```
root@BDC:~# /etc/init.d/apparmor reload
```

Permitiremos las actualizaciones dinámicas para el DNS, para que los clientes puedan actualizar sus entradas de DNS automáticamente añada lo siguiente en el fichero */etc/bind/named.conf.options*: (puede que necesite reemplazar *dnssec-validation auto* y comentar el parámetro *listen-on-v6 { any; };*)

```
tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
allow-query { any; };
allow-recursion { any; };
forwarders { 10.12.1.51; };
dnssec-validation no;
```

Si tiene otro Servidor DNS en la red que provee servicio para resolver nombres externos (*www.google.com*), necesitará configurar a Bind 9 para usar este DNS para resolver las entradas:

Deshabilitar IPv6 editando */etc/default/bind9* para que quede de la siguiente forma:

```
OPTIONS="-4 -u bind"
```

Por últimos instale Kerberos

Ejecutar el siguiente comando, cuando pregunte por *default realm* (área predeterminada) chequee que coincide con su dominio, luego le pide el nombre del servidor (en nuestro caso PDC):

```
root@BDC:~# apt-get install krb5-user –y
```

Edite el fichero de configuración de kerberos */etc/krb5.conf*, de igual forma que en el servidor primario (PDC).

Por último compruebe que kerberos funciona ejecutando el siguiente comando:

```
root@BDC:~# kinit  administrator@JOSE.COM
```

Uniendo el servidor al dominio.

```
root@BDC:~# samba-tool domain join jose.com DC -Uadministrator --realm=jose.com
```

Luego reiniciamos samba

```
root@BDC:~# initctl start samba4
```

Editamos el fichero */etc/samba/smb.conf* dentro del parámetro global añadimos:

```
preferred master = no
log level = 3
```

En el servidor segundario iniciamos samba, lo detenemos y echamos nuevamente a andar

```
root@BDC:~# samba
root@BDC:~# killall samba
root@BDC:~# samba
```

En el servidor primario:

root@PDC:~# samba-tool drs kcc –Uadministrator PDC.jose.com

Por ultimo en el servidor segundario:

root@BDC:~# samba_upgradedns

Algunos comandos para comprobar que todo marcha bien

root@PDC:~# ldbsearch -H /var/lib/samba/private/sam.ldb -b "DC=jose,DC=com" "(objectClass=dnsZone)"

root@PDC:~# samba-tool drs showrepl

Anexo III Configuración de la aplicación PhpLdapAdmin

Si usamos Samba 3 la configuración es la siguiente:

Se edita el archivo *config.php*

```
nano /etc/phpLDAPadmin/config.php
```

Buscar las líneas:

```
$servers->setValue('server','name','My LDAP Server');

$servers->setValue('server','host','127.0.0.1');

$servers->setValue('server','base',array('dc=example,dc=com'));

$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');
```

Cambiarlas para reflejar el dominio del servidor

```
$servers->setValue('server','name','Jose Server');

$servers->setValue('server','host','127.0.0.1');

$servers->setValue('server','base',array('dc=jose,dc=com'));

$servers->setValue('login','bind_id','cn=admin,dc=jose,dc=com');
```

A continuación se reinicia el servicio web con:

```
/etc/init.d/apache2 restart o service apache2 reload
```

Si usamos Samba 4:

Se edita el archivo *config.php*

```
nano /etc/phpLDAPadmin/config.php
```

Buscar las líneas:

```
$servers->setValue('server','name','My LDAP Server');

$servers->setValue('server','host','127.0.0.1');

$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');
```

Cambiarlas para reflejar el dominio del servidor

```
$servers->setValue('server','name','My Samba 4 Server');

$servers->setValue('server','host','ldapi://%2Fvar%2Flib%2Fsamba%2Fprivate%2Fldapi');

$servers->setValue('login','attr','dn');
```

Comentamos la línea

```
#$servers->setValue('server','base',array('dc=example,dc=com'));
```

A continuación se reinicia el servicio web con:

```
/etc/init.d/apache2 restart o service apache2 reload
```

Anexo IV Configuración de la aplicación LDAP Account Manager (LAM)

Una vez instalado con el comando ***sudo apt-get install ldap-account-manager –y*** para acceder a la interfaz abriremos un navegador y escribiremos:

http://localhost/lam (localhost es la dirección IP de la máquina virtual).

Al abrir la pagina del login pulsaremos sobre la opción "*LAM Configuration*". En la siguiente página accedemos a "*Edit general settings*", aquí pedirá la contraseña, por defecto es "*lam*", podemos cambiarla en la opción que se encuentra al final de la página. Una vez hecho esto en el menú anterior seleccione la opción "*Edit server profiles*"

En la pantalla de "*Edit server profiles*" debe comprobar los datos para que coincidan con los del servidor, tanto los referentes a la configuración general como a los de tipo de cuentas. Y al final de la primera página debemos poner los datos del usuario root del LDAP, en este caso "*cn=admin,dc=jose,dc=com*" y su contraseña.

En la segunda pestaña modificar los módulos y tipos de módulos pertenecientes al servidor LDAP. Con la configuración básica es suficiente, pero cuidado con los atributos que hay por defecto, los de LAM son (People, Groups y Machines), habrá que cambiar tanto el nombre del domino como el de los grupos (Users por People, Computers por Machines…). Luego acepte los cambios y vuelva a la ventana inicial del login.

Ahora inicie sesión con el usuario *admin*.

Desde el menú puede ver el árbol de directorios, administrar los usuarios, los grupos, hosts y Dominios SAMBA.

Anexo V Encuesta sobre Administración de Redes

Esta encuesta está dirigida a todas las personas que cumplen la función de administradores de red con el objetivo de identificar el nivel de preparación y desempeño en el tema. Los datos serán tratados con la mayor confidencialidad posible.

1. ¿Cuánto tiempo de experiencia tiene como administrador de red?

   _____

2. Represente, en la siguiente escala, el conocimiento que poseía sobre la administración de redes antes de desempeñar este puesto. (1 significa ninguno y 10 mucho)

   1__ 2__ 3__ 4__ 5__ 6__ 7__ 8__ 9__ 10__

3. En la siguiente escala represente su conocimiento del tema en estos momentos:

   1__ 2__ 3__ 4__ 5__ 6__ 7__ 8__ 9__ 10__

4. ¿Ha tenido la posibilidad de recibir superación en el tema? Mencione por cuales vías:

   Sí __ No __

   _____

5. Si ha sido el caso, ¿está usted satisfecho con la superación recibida? Argumente:

   Sí __ No __

   _____

   _____

6. Posee bibliografía actualizada:

   (1 significa ninguna y 7 mucho)

   1__ 2__ 3__ 4__ 5__ 6__ 7__

7. ¿Qué sistema operativo usted usa para administrar su red?

   Ubuntu__ Debian__ Microsoft Windows__ Otro_____

¡Muchas gracias!

GLOSARIO

BIND Acrónimo de *Berkeley Internet Name Domain,* es el servidor de DNS más comúnmente usado en Internet.

BIOS Acrónimo de *Basic Input Output System* (Sistema Básico de Entrada/Salida). Programa residente normalmente en ROM que controla las interacciones básicas entre el hardware y el software.

DNS *Acrónimo de Domain Name System* (Sistema de Nombres de Dominio). Sistema para traducir los nombres de los ordenadores en direcciones IP numéricas.

FQDN Acrónimo de *Fully Qualified Domain Name*, es el nombre completo de un recurso en el dominio.

FTP *Acrónimo de File Transfer Protocol* (protocolo de transferencia de archivos), un protocolo de Internet que permite que un usuario transfiera archivos hacia y desde otros equipos.

HTML *Hyper Text Markup Language* (Lenguaje de Marcado de Hipertexto). Lenguaje en el que se escriben los documentos que se acceden a través de visualizadores WWW. Admite componentes hipertexto y multimedia.

HTTP Acrónimo de *Hipertext Transfer Protocol* (protocolo de transferencia de hipertexto), es el protocolo en que se basa la tecnología de World Wide Web. Http es el conjunto de reglas que gobiernan el software que transporta los documentos HTML a través de Internet.

LAM Acrónimo *de LDAP Account Manager*.

LAN Acrónimo de *Local Area Network* (red de área local), una red que conecta dos o más equipos que están dentro de un área relativamente pequeña, normalmente en el local de una organización, con el propósito de comunicarlos y compartir archivos.

LDA *Local Delivery Agent,* agente Local empleado para Entregar correo desde el MDA al MUA.

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

MIC *Ministry of Information and Communication* (Ministerio de la Informática y de la Comunicación).

MOM *Acrónimo de Manager of Manager*.

MTA *Mail Transport Agent*, es un programa encargado de recoger mensajes y enviarlos, comunicando con otros MTA según sea preciso.

MUA *Mail User Agent*, es un programa que permite leer y escribir correos.

NIS *Network Information Service* protocolo, nombrado originalmente como Páginas Amarillas.

NSS *Acrónimo de Name Server Switch*.

PAM *Acrónimo de Pluggable Authentication Modules*, es un mecanismo de autenticación flexible que permite abstraer las aplicaciones y otro software del proceso de identificación.

POP *Post Office Transport Protocol*, se utiliza para obtener/descargar los mensajes guardados en el servidor al usuario.

SMTP *Simple Mail Transfer Protocol*, es el protocolo principal del MTA.

SSL *Secure Sockets Layer* (Capa de Conexiones Seguras), es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet.

TCP/IP Acrónimos de Transport Control Protocol and Internet Protcol (protocolo de control de transmisión y protocolo Internet), los dos protocolos que gobiernan la manera en que los equipos y las redes administran el flujo de información que pasa a través de Internet.

TLS *Transport Layer Security*, protocolo basado en SSL.

UNIX Sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas más conocidos como MS-DOS están basadas en este sistema muy extendido para miniordenadores. Internet no se puede comprender en su totalidad sin

conocer el UNIX, ya que las comunicaciones con TCP/IP son una parte fundamental de este sistema operativo.

URL/URI *Universal Resource Locator/Universal Resource Identifier* (Localizador Universal de Recursos/Identificador Universal de Recursos). Sistema unificado de identificación de recursos en la red. Las direcciones se componen de protocolo, FQDN y dirección local del documento dentro del servidor. Este tipo de direcciones permite identificar objetos WWW, Gopher, FTP, News, etc.