TFC - MIGRACIÓN WINDOWS - GNU/LINUX

Jaime Marcos de la Calle

2011-2012 - 1

ÍNDICE

1. INTRODUCCIÓN

1.1. GNU

GNU es el acrónimo de las que significa GNU no es UNIX. Fue creado por Richard Stallman con el objetivo de crear un sistema operativo completamente libre.

El 27 de septiembre de 1983 se anunció públicamente el proyecto por primera vez en el grupo de noticias net.unix-wizards. Al anuncio original, siguieron otros ensayos escritos por Richard Stallman como el "Manifiesto GNU", que establecieron sus motivaciones para realizar el proyecto GNU, entre las que destaca "volver al espíritu de cooperación que prevaleció en los tiempos iniciales de la comunidad de usuarios de computadoras".

UNIX es un Sistema Operativo no libre muy popular, porque está basado en una arquitectura que ha demostrado ser técnicamente estable. El sistema GNU fue diseñado para ser totalmente compatible con UNIX. El hecho de ser compatible con la arquitectura de UNIX implica que GNU esté compuesto de pequeñas piezas individuales de software, muchas de las cuales ya estaban disponibles, como el sistema de edición de textos TeX y el sistema gráfico X Window, que pudieron ser adaptados y reutilizados; otros en cambio tuvieron que ser reescritos.

Para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en Inglés como *copyleft* -'copia permitida'- (en clara oposición a copyright -'derecho de copia'-), y está contenida en la Licencia General Pública de GNU (GPL).

1.2. GPL (GENERAL PUBLIC LICENSE)

La *Licencia Pública General de GNU* o más conocida por su nombre en inglés *GNU General Public License* o simplemente sus siglas del inglés *GNU GPL*, es una licencia creada por la *Free Software Foundation* en 1989 (la primera versión), y está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

La licencia GPL, al ser un documento que cede ciertos derechos al usuario, asume la forma de un contrato, por lo que usualmente se la denomina contrato de licencia o acuerdo de licencia. En los países de tradición anglosajona existe una distinción doctrinal entre licencias y contratos, pero esto no ocurre en los países de tradición civil o continental. Como contrato, la GPL debe cumplir los requisitos legales de formación contractual en cada jurisdicción.

La licencia ha sido reconocida, entre otros, por juzgados en Alemania, particularmente en el caso de una sentencia en un tribunal de Múnich,4 lo que indica positivamente su validez en jurisdicciones de derecho civil.

1.3. FREE SOFTWARE FUNDATION

La *Free Software Foundation (Fundación para el software libre)* es una organización creada en octubre de 1985 por Richard Stallman y otros entusiastas del software libre con el propósito de difundir este movimiento.

La Fundación para el software libre (FSF) se dedica a eliminar las restricciones sobre la copia, redistribución, entendimiento, y modificación de programas de computadoras. Con este objeto, promociona el desarrollo y uso del software libre en todas las áreas de la computación, pero muy particularmente, ayudando a desarrollar el sistema operativo GNU.

En sus inicios, la FSF destinaba sus fondos principalmente a contratar programadores para que escribiesen software libre. A partir de mediados de la década de 1990 existen ya muchas compañías y autores individuales que escriben software libre, por ello los empleados y voluntarios de la FSF han centrado su trabajo fundamentalmente en asuntos legales, organizativos y promocionales en beneficio de la comunidad de usuarios de software libre.

1.4. RICHARD STALLMAN

Richard Matthew Stallman (nacido en Manhattan, Nueva York, 16 de marzo de 1953), con frecuencia abreviado como *"rms",*1 es un programador estadounidense y fundador del movimiento por el software libre en el mundo.

Entre sus logros destacados como programador se incluye la realización del editor de texto GNU Emacs, el compilador GCC y el depurador GDB, bajo la rúbrica del Proyecto GNU. Sin embargo, es principalmente conocido por el establecimiento de un marco de referencia moral, político y legal para el movimiento del software libre, como una alternativa al desarrollo y distribución del software no libre o privativo. Es también inventor del concepto de copyleft(aunque no del término), un método para licenciar software de tal forma que su uso y modificación permanezcan siempre libres y queden en la comunidad.

En 1985 realizó la publicación del Manifiesto GNU, en el cual Stallman declaraba sus intenciones y motivaciones para crear una alternativa libre al sistema operativo Unix, al que denominó GNU (GNU No es Unix). Poco tiempo después fundó la organización sin ánimo de lucro *Free Software Foundation* para coordinar el esfuerzo. Inventó el concepto de *copyleft*, que fue utilizado en la *Licencia Pública General GNU* (conocida generalmente como la "GPL") en1989. La mayor parte del sistema GNU, excepto el núcleo, se completó aproximadamente al mismo tiempo. En 1991,*Linus Torvalds* liberó el núcleo Linux bajo los términos de la GPL, completando un sistema GNU completo y operativo, el sistema operativo GNU/Linux.

1.5. LINUS TORLVALDS

Linus Benedict Torvalds (28 de diciembre de 1969, Helsinki, Finlandia) es un ingeniero de software finlandés, conocido por iniciar y mantener el desarrollo del "kernel" (en español, núcleo) Linux, basándose en el sistema operativo libre Minix creado por Andrew S. Tanenbaum y en algunas herramientas, varias utilidades y los compiladores desarrollados por el proyecto GNU. Actualmente Torvalds es responsable de la coordinación del proyecto. Pertenece a la comunidad sueco-parlante de Finlandia.

En 1988 fue admitido en la Universidad de Helsinki, donde se obtuvo su maestría en Ciencias de la Computación. Ese mismo año el profesor Andrew S. Tanenbaum saca a la luz el

S.O. Minix con propósitos didácticos. Dos años después, en 1990, Torvalds empieza a aprender el lenguaje de programación C en su universidad.

A finales de los años 80 tomó contacto con los computadores IBM, PC y en 1991 adquirió una computadora con procesador modelo 80386 de Intel.

A la edad de 21 años, con 5 años de experiencia programando (en C), ya conocía lo suficiente del sistema operativo Minix como para tomar prestadas algunas ideas y empezar un proyecto personal. Basándose en Design of the Unix Operating System, publicado por Maurice J. Bach en 1986, crearía una implementación que ejecutará cualquier tipo de programa, pero sobre una arquitectura de ordenadores compatibles, IBM/PC.

Este proyecto personal desembocó el 5 de octubre de 1991 con el anuncio2 de la primera versión de Linux capaz de ejecutar BASH (Bourne Again Shell) y el compilador conocido como GCC (GNU Compiler Collection).

En enero de 1992 se adoptó la Licencia Pública General (GPL) para Linux. Ésta añade libertades de uso a Linux totalmente opuestas a las del software propietario, permitiendo su modificación, redistribución, copia y uso ilimitado. Este modelo de licencia facilita lo que es conocido como el modelo de desarrollo de bazar, que ha dado estabilidad y funcionalidad sin precedentes a este sistema operativo.

1.6. GNU/LINUX

GNU/LINUX (más conocido como Linux, simplemente) es un sistema operativo, compatible Unix.

Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado: la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente.

El sistema lo forman el núcleo del sistema (kernel) más un gran número de programas y librerías que hacen posible su utilización.

Linux se distribuye bajo la Licencia Pública General GNU (GPL), por lo tanto, el código fuente tiene que estar siempre accesible.

El sistema ha sido diseñado y programado por multitud de programadores alrededor del mundo. El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de Linus Torvalds, la persona de la que partió la idea de este proyecto, en 1991.

Linus, por aquel entonces un estudiante de informática de la Universidad de Helsinki, empezó (como proyecto de fin de carrera y sin poder imaginar en lo que se llegaría convertir) a programar las primeras líneas de código de este sistema operativo llamado LINUX.

El origen de Linux estuvo inspirado en MINIX, un pequeño sistema Unix desarrollado por Andy Tanenbaum. Las primeras discusiones sobre Linux fueron en el grupo de noticias comp.os.minix, en estas discusiones se hablaba sobre todo del desarrollo de un pequeño sistema Unix para usuarios de Minix que querían más.

Linus nunca anunció la versión 0.01 de Linux (agosto 1991), esta versión no era ni siquiera ejecutable, solamente incluía los principios del núcleo del sistema, estaba escrita en lenguaje ensamblador y asumía que uno tenía acceso a un sistema Minix para su compilación.

El 5 de octubre de 1991, Linus anunció la primera versión "oficial" de Linux, (versión 0.02). Con esta versión Linus pudo ejecutar Bash (GNU Bourne Again Shell) y gcc (El compilador GNU de C) pero no mucho más. En este estado de desarrollo ni se pensaba en los términos soporte, documentación, distribución .....

Después de la versión 0.03, Linus saltó en la numeración hasta la 0.10. Más y más programadores a lo largo y ancho de Internet empezaron a trabajar en el proyecto y después de sucesivas revisiones, Linus incrementó el número de versión hasta la 0.95 (Marzo 1992). Más de un año después (diciembre 1993) el núcleo del sistema estaba en la versión 0.99 y la versión 1.0 llego el 14 de marzo de 1994.

La serie actual del núcleo es la 2.6.x y sigue avanzando día a día con la meta de perfeccionar y mejorar el sistema.

2. JUSTIFICACIÓN DEL TFC

En toda mi carrera profesional no he tenido la oportunidad de trabajar bajo un sistema operativo Linux, sino que siempre he trabajado bajo plataformas Windows, y siempre he tenido la curiosidad y la inquietud de conocer Linux, tanto en servidores como en clientes.

Mis conocimientos iniciales de Linux son de usuario muy básico en desktop, instalación algo de configuración y poco más.

Creo que el futuro irá por cada vez más empezar a utilizar herramientas de software libre, tanto en las empresas como en los hogares, y dado que mi conocimiento sobre la materia es casi nulo y a la opción de este TFC en la carrera encontré muy interesante elegirlo.

Este TFC me aportará sin duda alguna conocimientos sobre las plataformas GNU/Linux a nivel de estructura de un sistema informático de empresa mediana, basado en plataforma GNU/Linux tanto en servidores como en los ordenadores clientes y estoy seguro que será de gran utilidad para mi futuro profesional. Además despertará aún más el interés por conocer más a fondo esta plataforma y realizar en la medida de lo posible laboratorios de configuración de servicios.

3. DESCRIPCIÓN DEL PROYECTO

La empresa Audif S.L. empresa fundada en 1949 y dedicada a ofrecer las mejores soluciones audiológicas a sus clientes (entre ellos particulares, hospitales centros médicos privados...) nos ha encargado el estudio y posterior implantación de una solución informática basada en software libre, consiguiendo reducir los costes actuales y llegar a ser más competitivos.

Actualmente la empresa tiene dos sedes, Barcelona (Central) y Madrid.

La herramienta principal para todos los empleados es un software cliente basado en Java donde se pueden realizar todo lo relacionado con los clientes (facturación, campañas de marketing, citas, audiogramas...) Además todos disponen de una o varias cuentas de correo electrónico para la comunicación tanto interna como externa y el envío de documentos. También disponen en todos los equipos instalado la suite Office. Todos los ordenadores tienen salida a Internet sin ninguna restricción.

Las sedes funcionan de forma independiente, además de tener implementados dos dominios diferentes, cada una dispone de un servidor que hace las funciones de servidor de correo, controlador de dominio, servidor de archivos.

Tienen contratado a una empresa externa un dispositivo físico (en cada sede) que actúa de firewall y que además conecta a través de un túnel de VPN las dos sedes, además de tener también con la misma empresa la gestión del correo electrónico.

Las características de la sede de Barcelona son:

- Despacho de director general.
- Seis despachos de audioprotesistas.
- Despacho de contabilidad.
- Despacho de ORL.
- Tres equipos de secretaría.
- Equipo sala de formación.
- Servidor.

Las características de la sede de Madrid son:

- Despacho de director de sede.
- Tres despachos de audioprotesistas.
- Despacho de contabilidad
- Despacho ORL.
- Tres equipos de secretaría.
- Equipo para publicidad.
- Servidor.

El equipamiento informático disponible en toda la empresa es:

- Trece ordenadores Intel Core i3 con WinXP (Audioprotesistas, ORL y Contabilidad).
- Dos ordenadores Intel Core i5 con WinXP (Directores).
- Ocho ordenadores Intel Core 2 Duo con WinXP (Secretaría, Publicidad y Formación).
- Dos servidores HP DL 160 G6 E5606 con Win 2003 Server.

4. OBJETIVO DEL PROYECTO

El objetivo principal del proyecto es la de diseñar la infraestructura informática de la empresa Audif S.L. teniendo en cuenta las pautas marcadas por la misma, considerando las necesidades indicadas de manera explícita y las derivadas de estas.

Las peticiones principales del cliente son:

- Migración a entorno GNU/Linux todo el sistema.
- Posibilidad de incluir algún equipo bajo plataforma Windows en un futuro.
- Reutilización de lo máximo posible del parqué informático actual.
- Eliminación de la externalización de los servicios de correo electrónico, firewall, VPN.
- Unión de las dos sedes.
- Políticas de seguridad en compartición de archivos de la empresa.
- Política de seguridad en acceso a Internet.
- El cliente está dispuesto a escuchar la opinión del experto en cuanto a cambiar la forma de trabajo, introducir nuevo software... si no supone un coste excesivo.

5. PLANIFICACIÓN PROYECTO

A continuación se detalla la planificación del proyecto con las fechas de cada hito. Se han tenido en cuenta los fines de semana como no laborables, menos en el caso del ID 29 que los servidores se deberán de instalar en un fin de semana para no interrumpir en la actividad diaria de la empresa.

ID	Descripción Tarea	Fecha Inicio	Fecha Fin	Total Días Laborables	% Tarea	% Proyecto
	Elección, Planificación Proyecto	***29/09/11***	***13/10/11***	***11,0***	***14,3***	***14,3***
1	Elección Proyecto	29/09/11	03/10/11	3	3,9	3,90
2	Estudio de las Tareas a Realizar	04/10/11	05/10/11	2	2,6	6,49
3	Establecimiento del Plan de Trabajo	06/10/11	10/10/11	3	3,9	10,39
4	Elaboración Diagrama de Gantt	11/10/11	11/10/11	1	1,3	11,69
5	Elaboración Documento PEC1	12/10/11	13/10/11	2	2,6	14,29
6	Entrega PEC1	13/10/11	13/10/11	0	0,0	14,29
	Etapa de Estudio, Búsqueda y Elección	***14/10/11***	***04/11/11***	***16,0***	***20,8***	***35,1***
7	Estudio de Situación Actual	14/10/11	20/10/11	5	6,5	20,78
8	Estudio y elección de Distribución Linux PC	21/10/11	24/10/11	2	2,6	23,38
9	Estudio y Elección de Distribución Linux Servidor	25/10/11	26/10/11	2	2,6	25,97
10	Estudio Aplicaciones Linux de Sustitución por Actuales	27/10/11	04/11/11	7	9,1	35,06
	Etapa de Preproducción	***07/11/11***	***22/12/11***	***34,0***	***44,2***	***79,2***
	Instalación Servidor Barcelona	***07/11/11***	***23/11/11***	***13***	***16,9***	***51,9***
11	Instalar Distribución GNU/Linux	07/11/11	07/11/11	1	1,3	36,4
12	Instalar servicios LDAP	08/11/11	11/11/11	4	5,2	41,6
13	Instalar Cola de Impresión	14/11/11	14/11/11	1	1,3	42,9
14	Instalar Aplicación Control de Versiones	15/11/11	16/11/11	2	2,6	45,5
15	Entrega PEC2	16/11/11	16/11/11	0	0,0	45,5
16	Instalar Aplicación gestor de Documentación	17/11/11	18/11/11	2	2,6	48,1
17	Instalar y Configurar Servidor de Correo	21/11/11	23/11/11	3	3,9	51,9
	Instalación Servidor Madrid	***24/11/11***	***12/12/11***	***13***	***16,9***	***68,8***
18	Instalar Distribución GNU/Linux	24/11/11	24/11/11	1	1,3	53,2
19	Instalar servicios LDAP	25/11/11	30/11/11	4	5,2	58,4
20	Instalar Cola de Impresión	01/12/11	01/12/11	1	1,3	59,7
21	Instalar Aplicación Control de Versiones	02/12/11	05/12/11	2	2,6	62,3
22	Instalar Aplicación gestor de Documentación	06/12/11	07/12/11	2	2,6	64,9
23	Instalar y Configurar Servidor de Correo	08/12/11	12/12/11	3	3,9	68,8
24	Instalación y Configuración de Servidor Firewall, VPN y proxy Sede Barcelona	13/12/11	16/12/11	4	5,2	74,0
25	Entrega PEC3	14/12/11	14/12/11	0	0,0	74,0
26	Instalación y Configuración de Servidor Firewall, VPN y proxy Sede Madrid	19/12/11	22/12/11	4	5,2	79,2
	Etapa Producción	***23/12/11***	***09/01/12***	***16,0***	***20,8***	***100,0***
26	Instalación Pc's nuevos en entorno GNU/Linux	23/12/11	26/12/11	2	2,6	81,8
27	Migración de actuales Pc's de Windows a GNU/Linux	27/12/11	29/12/11	3	3,9	85,7
28	Apagado de Servidores Actuales Windows	30/12/11	31/12/11	2	2,6	88,3
29	Instalación en Empresa de nuevos Servidores Basados en Linux	30/12/11	01/01/12	3	3,9	92,2
30	Periodo de Pruebas de nueva estructura Informática GNU/Linux	02/01/12	06/01/12	5	6,5	98,7
31	Retirada de Servidores y Pc's antiguos basados en Windows	09/01/12	09/01/12	1	1,3	100,0
32	Entrega PEC4	09/01/12	09/01/12	0	0,0	100,0

Cuadro de fechas de planificación del proyecto

6. DIAGRAMA DE GANTT

A continuación se muestra el diagrama de Gantt. Para una mejor visualización se ha dividido en cuatro subdiagramas, uno por cada etapa del proyecto.

- Etapa de elección y Planificación del proyecto:

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Elección, Planificación Proyecto**	**11 días**	**jue 29/09/11**	**jue 13/10/11**
2	Elección Proyecto	3 días	jue 29/09/11	lun 03/10/11
3	Estudio de las Tareas a Realizar	2 días	mar 04/10/11	mié 05/10/11
4	Establecimiento del Plan de Trabajo	3 días	jue 06/10/11	lun 10/10/11
5	Elaboración Diagrama de Gantt	1 día	mar 11/10/11	mar 11/10/11
6	Elaboración Documento PEC1	2 días	mié 12/10/11	jue 13/10/11
7	Entrega PEC1	0 días	jue 13/10/11	jue 13/10/11

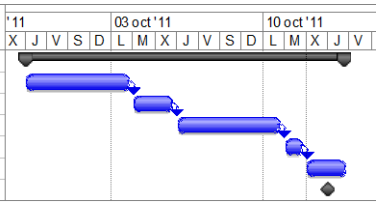


Diagrama Gantt Primera Etapa

- Etapa de estudio, búsqueda y elección software:

Id	Nombre de tarea	Duración	Comienzo	Fin
8	**Etapa de Estudio, Búsqueda y Elección**	**16 días**	**vie 14/10/11**	**vie 04/11/11**
9	Estudio de Situación Actual	5 días	vie 14/10/11	jue 20/10/11
10	Estudio y elección de Distribución Linux PC	2 días	vie 21/10/11	lun 24/10/11
11	Estudio y Elección de Distribución Linux Servidor	2 días	mar 25/10/11	mié 26/10/11
12	Estudio Aplicaciones Linux de Sustitución por Actuales	7 días	jue 27/10/11	vie 04/11/11

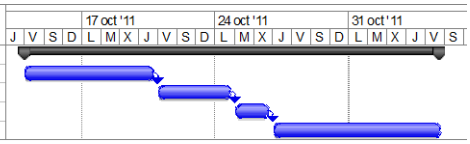


Diagrama Gantt Segunda Etapa

- Etapa Preproducción:

Id	Nombre de tarea	Duración	Comienzo	Fin
13	**Etapa de Preproducción**	**34 días**	**lun 07/11/11**	**jue 22/12/11**
14	**Instalación Servidor PDC (Barcelona)**	**13 días**	**lun 07/11/11**	**mié 23/11/11**
15	Instalar Distribución GNU/Linux	1 día	lun 07/11/11	lun 07/11/11
16	Instalar servicios LDAP	4 días	mar 08/11/11	vie 11/11/11
17	Instalar Cola de Impresión	1 día	lun 14/11/11	lun 14/11/11
18	Instalar Aplicación Control de Versiones	2 días	mar 15/11/11	mié 16/11/11
19	Entrega PEC2	0 días	mié 16/11/11	mié 16/11/11
20	Instalar Aplicación gestor de Documentación	2 días	jue 17/11/11	vie 18/11/11
21	Instalar y Configurar Servidor de Correo	3 días	lun 21/11/11	mié 23/11/11
22	**Instalación Servidor BDC (Madrid)**	**13 días**	**jue 24/11/11**	**lun 12/12/11**
23	Instalar Distribución GNU/Linux	1 día	jue 24/11/11	jue 24/11/11
24	Instalar servicios LDAP	4 días	vie 25/11/11	mié 30/11/11
25	Instalar Cola de Impresión	1 día	jue 01/12/11	jue 01/12/11
26	Instalar Aplicación Control de Versiones	2 días	vie 02/12/11	lun 05/12/11
27	Instalar Aplicación gestor de Documentación	2 días	mar 06/12/11	mié 07/12/11
28	Instalar y Configurar Servidor de Correo	3 días	jue 08/12/11	lun 12/12/11
29	Instalación Servidor Firewall, vpn y proxy Sede Barcelona	4 días	mar 13/12/11	vie 16/12/11
30	Entrega PEC3	0 días	mié 14/12/11	mié 14/12/11
31	Instalación Servidor Firewall, vpn y proxy Sede Madrid	4 días	lun 19/12/11	jue 22/12/11

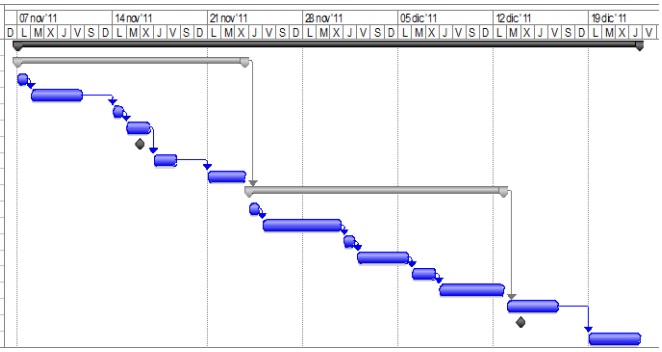


Diagrama Gantt Tercera Etapa

- Etapa Producción:

Id	Nombre de tarea	Duración	Comienzo	Fin
32	**Etapa Producción**	**14 días**	**vie 23/12/11**	**lun 09/01/12**
33	Instalación Pc's nuevos en entorno GNU/Linux	2 días	vie 23/12/11	lun 26/12/11
34	Migración de actuales Pc's de Windows a GNU/Linux	3 días	mar 27/12/11	jue 29/12/11
35	Apagado de Servidores Actuales Windows	2 días	vie 30/12/11	sáb 31/12/11
36	Instalación en Empresa de nuevos Servidores Basados en Linux	3 días	vie 30/12/11	dom 01/01/12
37	Periodo de Pruebas de nueva estructura Informática GNU/Linux	5 días	lun 02/01/12	vie 06/01/12
38	Retirada de Servidores y Pc's antiguos basados en Windows	1 día	lun 09/01/12	lun 09/01/12
39	Entrega PEC4	0 días	lun 09/01/12	lun 09/01/12

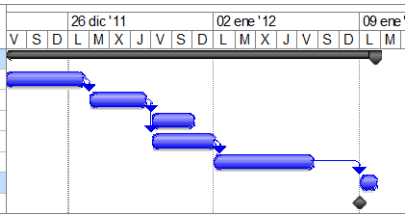


Diagrama Gantt Cuarta Etapa

7. SITUACIÓN ACTUAL

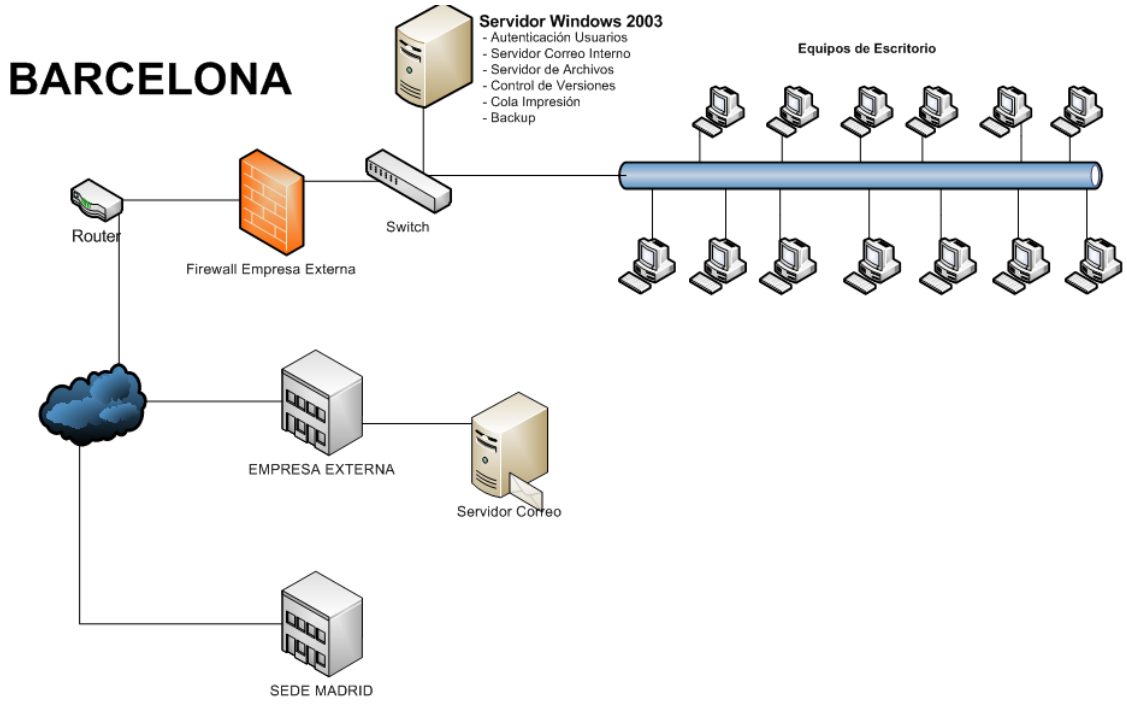
A continuación se recogen los datos generales del equipamiento informático actual y el final.

7.1. ESQUEMA INFORMÁTICO

La sede de Barcelona cuenta con el siguiente hardware:

- Servidor HP DL 160 G6 E5606 con 4GB de RAM y 2 GB de HDD.
- Un ordenador Intel Core i5 con 4 GB de RAM y 4 GB de HDD.
- Ocho ordenadores de escritorio Intel Core i3 con 2 GB de RAM y 1 GB de HDD.
- Cuatro ordenadores de escritorio Intel Core 2 Duo con 1 GB de RAM y 500 MB de HDD.

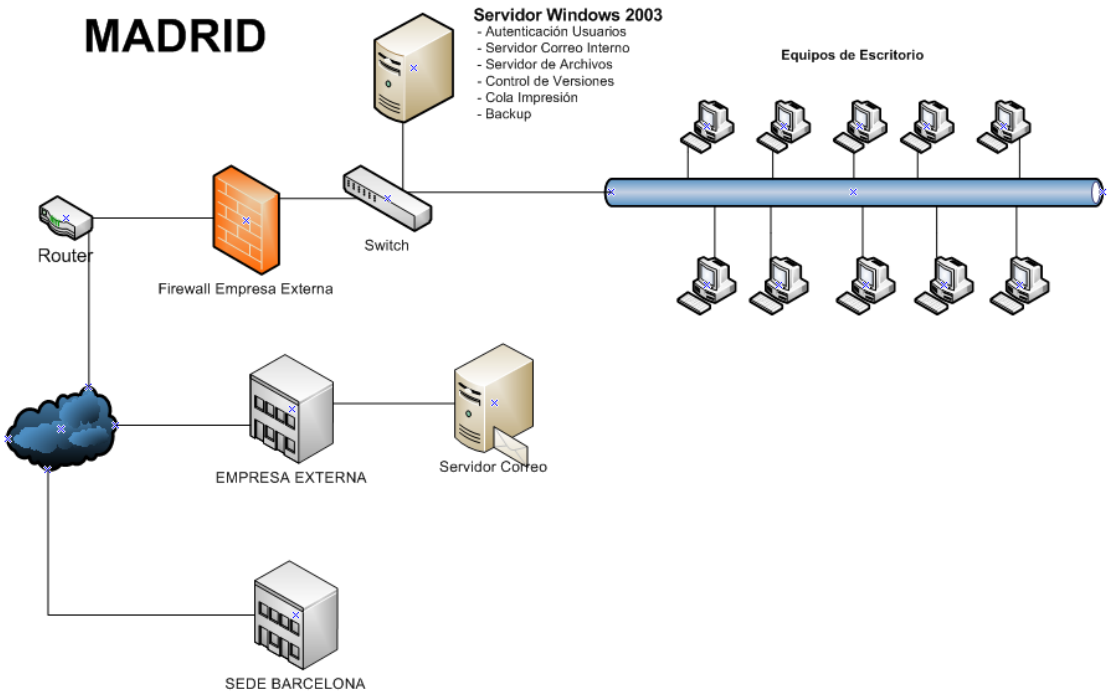
En el siguiente esquema se puede observar la estructura y sistema informático inicial de la sede de Barcelona de la empresa, basado en plataformas Windows:



La sede de Madrid cuenta con el siguiente hardware:

- Servidor HP DL 160 G6 E5606 con 4GB de RAM y 2 GB de HDD.
- Un ordenador Intel Core i5 con 4 GB de RAM y 4 GB de HDD.
- Cinco ordenadores de escritorio Intel Core i3 con 2 GB de RAM y 1 GB de HDD.
- Cuatro ordenadores de escritorio Intel Core 2 Duo con 1 GB de RAM y 500 MB de HDD.

En el siguiente esquema se puede observar la estructura y sistema informático inicial de la sede de Madrid de la empresa, basado en plataformas Windows:



7.2. SOFTWARE

Para la realización de los trabajos diarios los ordenadores de la empresa Audif S.L. tienen instalado el siguiente software:

Servidor	***Clientes***
Windows 2003 Server	Windows XP
Microsoft Exchange	Microsoft Office
Maquina virtual Java	Maquina virtual Java
Microsoft Internet Explorer	Microsoft Internet Explorer
	Nero Bourning Rom

Como sistema operativo en los servidores está instalado Windows 2003 Server Standard Edition, que se utiliza principalmente para la gestión de los dominios, permios de usuarios, compartir archivos, DHCP, DNS y la realización de copias de seguridad.

Además en los servidores se encuentra instalado Microsoft Exchange, configurado para recibir y enviar el correo interno de la empresa sin tener que depender de la empresa externa donde tienen contratado el servicio de correo electrónico.

En los ordenadores personales como sistema operativo se encuentra instalado Windows Xp profesional service pack 3.

Para la realización de documentos de texto, hojas de cálculo y presentaciones cada ordenador personal cuenta con la instalación de la suite Microsoft Office 2003. Dentro de esta suite se encuentra el programa Microsoft Outlook y está configurado, en cada ordenador, para recibir correo electrónico tanto del servidor Exchange de la sede a la que pertenezca, como para recibir correo electrónico exterior desde la empresa externa contratada. Para la realización de copias de datos en almacenamiento externo se encuentra instalado en cada equipo el software Nero Bourning Rom.

Además en todos los ordenadores de la empresa está instalada la máquina virtual de Java, requisito imprescindible para el funcionamiento del software específico que utilizan para hacer las mediciones de audición.

7.3. DISTRIBUCIÓN RED

La distribución actual de la red en la sede de Barcelona es la siguiente:

Red de la sede	192.168.2.0/24
Rango destinado para servidores	192.168.2.240 - 192.168.2.254
Rango destinado a equipos y periféricos	192.168.2.11 - 192.168.2.239
Dominio	barcelona.local

La configuración de red de los equipos de la sede es:

Nombre máquina	Nombre del Dominio	IP
ServerBarcelona	ServerBarcelona.barcelona.local	192.168.2.240
Firewall	----------	192.168.2.241
Francisco	Francisco.barcelona.local	192.168.2.11
Juan	Juan.barcelona.local	192.168.2.12
María	Maria.barcelona.local	192.168.2.13
Pedro	Pedro.barcelona.local	192.168.2.14
Ana	Ana.barcelona.local	192.168.2.15
Ismael	Ismael.barcelona.local	192.168.2.16
Encarna	Encarna.barcelona.local	192.168.2.17
Fernando	Fernando.barcelona.local	192.168.2.18
Teresa	Teresa.barcelona.local	192.168.2.19
Jaime	Jaime.barcelona.local	192.168.2.20
Ricardo	Ricardo.barcelona.local	192.168.2.21
Manuel	Manuel.barcelona.local	192.168.2.22
Alberto	Alberto.barcelona.local	192.168.2.23
Impresora	Impresora.barcelona.local	192.168.2.24

La distribución actual de la red en la sede de Madrid es la siguiente:

Red dela sede	172.26.0.0/24
Rango destinado para servidores	172.26.0.240 - 172.26.0.254
Rango destinado a equipos y periféricos	172.26.0.210 - 172.26.0.239
Dominio	madrid.local

La configuración de red de los equipos de la sede es:

Nombre máquina	Nombre del Dominio	IP
ServerMadrid	ServerMadrid.madrid.local	172.26.0.240
Firewall	----------	172.26.0.241
JuanF	JuanF.madrid.local	172.26.0.11
Teresa	Teresa.madrid.local	172.26.0.12
Rosa	Rosa.madrid.local	172.26.0.13
Juanita	Juanita.madrid.local	172.26.0.14
Bienvenido	Bienvenido.madrid.local	172.26.0.15
Noelia	Noelia.madrid.local	172.26.0.16
Jaime	Jaime.madrid.local	172.26.0.17
Carmen	Carmen.madrid.local	172.26.0.18
Amelia	Amelia.madrid.local	172.26.0.19
Gonzalo	Gonzalo.madrid.local	172.26.0.20
Impresora	Impresora.madrid.local	172.26.0.21

Todos los usuarios de los empleados de la empresa están creados dentro del grupo usuarios del dominio.

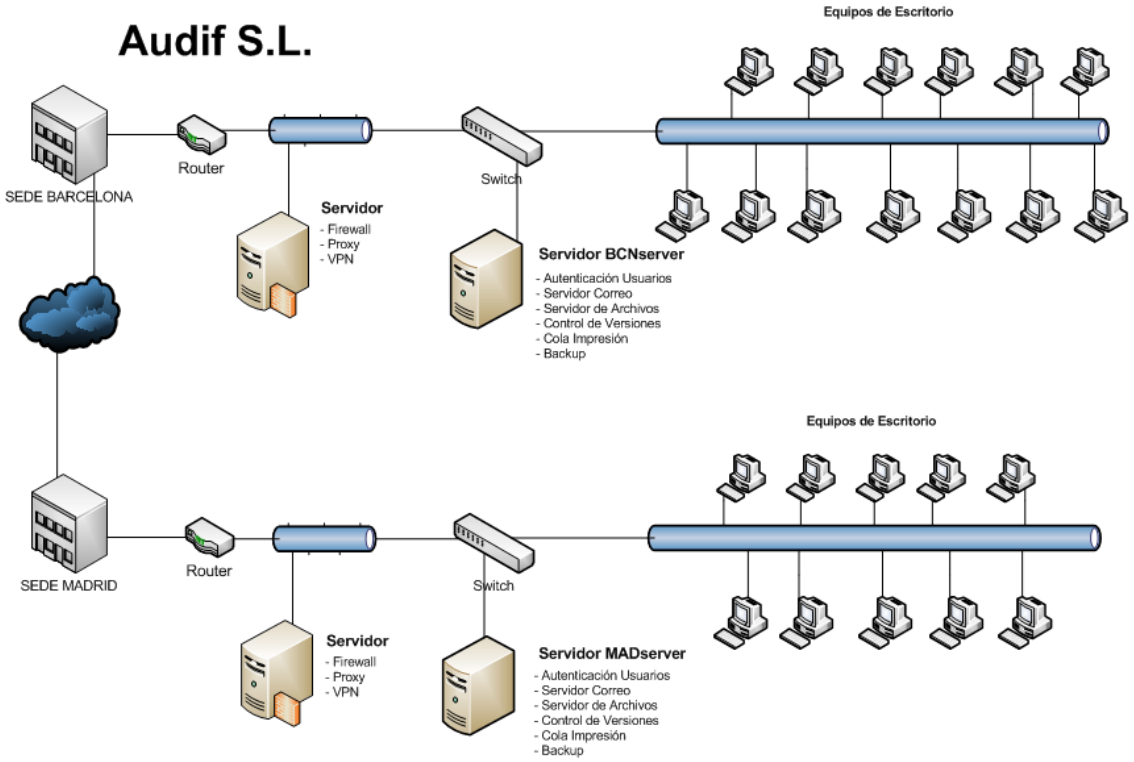
Cada usuario tiene compartido, en su servidor correspondiente, una carpeta con su nombre pública en la que todos tienen permisos de lectura y escritura y otra carpeta con su nombre privada, en la que solamente tiene acceso el propio usuario.

8. SITUACIÓN FINAL

8.1. ESQUEMA INFORMÁTICO

Como ya se ha indicado anteriormente la finalidad del proyecto es crear una estructura informática en la empresa uniendo sus sedes y trabajando bajo plataforma GNU/Linux.

En el siguiente esquema podemos observar la nueva estructura informática de la empresa basada den GNU/Linux :



El hardware actual será reutilizado solo hará falta la compra de dos equipos nuevos para utilizarlos como Servidores de Firewall en cada sede, con unos requisitos mínimos que cualquier equipo actual del mercado los superaría.

8.2. SOFTWARE

En los cuadros siguientes se recogen las alternativas en software libre al software propietario instalado actualmente en la empresa Audif S.L. tanto en los servidores como en los equipos personales:

SERVIDOR	Software Propietario (Instalado Actualmente)	Software Libre (software sustituto)
Dominio	Microsoft Windows 2003 Server	OpenLDAP, Samba
Autenticación Usuarios	Microsoft Windows 2003 Server	OpenLDAP, Samba
Servidor de Archivos	Microsoft Windows 2003 Server	Samba, NFS
Colas de impresión	Microsoft Windows 2003 Server	CUPS
Correo Electrónico	Microsoft Exchange	Postfix, Dovecot, Squirremail, Amavis-new, Spamassain, ClamAV
Copias de seguridad	Microsoft MSBackup	Dump, Restore
Control de Versiones	Ninguno	CVS
Firewall	Ninguno	UFW
Proxy	Ninguno	Squid

CLIENTES	Software Propietario (Instalado Actualmente)	Software Libre (software sustituto)
Correo electrónico	Microsoft Outlook	Squirremail
Editor de texto	Microsoft Word	Libreoffice Writter
Editor de hojas de cálculo	Microsoft Excel	Libreoffice Calc
Editor de presentaciones	Microsoft Power Point	Libreoffice Impress
Grabacion externa	Nero Bourning Rom	Brasero
Explorador internet	Microsoft Internet Explorer	Mozilla firefox

8.3. DISTRIBUCIÓN RED

La distribución de la red de la sede de Barcelona será la siguiente:

Red de la sede	192.168.1.0/24
Rango destinado para servidores	192.168.1.240 - 192.168.1.254
Rango destinado equipos	192.168.1.11 - 192.168.1.200
Rango destinado a periféricos	192.168.1.201 - 192.168.1.239
Dominio	audif.local

La distribución de los equipos en la red de Barcelona será:

Nombre máquina	Nombre del Dominio	IP
BCNserver	bcnserver.audif.local	192.168.1.240
BCNproxy	bcnproxy.audif.local	192.168.1.241
directorbcn	directorbcn.audif.local	192.168.1.11
audioprotesista1bcn	audioprotesista1bcn.audif.local	192.168.1.12
audioprotesista2bcn	audioprotesista2bcn.audif.local	192.168.1.13
audioprotesista3bcn	audioprotesista3bcn.audif.local	192.168.1.14
audioprotesista4bcn	audioprotesista4bcn.audif.local	192.168.1.15
audioprotesista5bcn	audioprotesista5bcn.audif.local	192.168.1.16
audioprotesista6bcn	audioprotesista6bcn.audif.local	192.168.1.17
contabilidadbcn	contabilidadbcn.audif.local	192.168.1.18
orlbcn	orlbcn.audif.local	192.168.1.19
secretaria1bcn	secretaria1bcn.audif.local	192.168.1.20
secretaria2bcn	secretaria2bcn.audif.local	192.168.1.21
secretaria3bcn	secretaria3bcn.audif.local	192.168.1.22
formacionbcn	formacionbcn.audif.local	192.168.1.23
Impresorabcn	Impresorabcn.audif.local	192.168.1.201

La distribución de la red de la sede de Madrid será la siguiente:

Red de la sede	192.168.2.0/24
Rango destinado para servidores	192.168.2.240 - 192.168.2.254
Rango destinado equipos	192.168.2.11 - 192.168.2.200
Rango destinado a periféricos	192.168.2.201 - 192.168.2.239
Dominio	audif.local

La distribución de los equipos en la red de Madrid será:

Nombre máquina	Nombre del Dominio	IP
MADserver	madserver.audif.local	192.168.2.240
MADproxy	madproxy.audif.local	192.168.2.241
directormad	directormad.audif.local	192.168.2.11
audioprotesista1mad	audioprotesista1mad. audif.local	192.168.2.12
audioprotesista2mad	audioprotesista2mad. audif.local	192.168.2.13
audioprotesista3mad	audioprotesista3mad. audif.local	192.168.2.14
contabilidadmad	contabilidadmad. audif.local	192.168.2.15
orlmad	orlmad. audif .local	192.168.2.16
secretaria1mad	secretaria1mad. audif.local	192.168.2.17
secretaria2mad	secretaria2mad. audif.local	192.168.2.18
secretaria3mad	secretaria3mad. audif.local	192.168.2.19
publicidadmad	publicidadmad. audif .local	192.168.2.20
Impresoramad	Impresoramad. audif.local	192.168.2.201

En el nuevo dominio de la empresa se crearán los siguientes grupos de usuarios, donde estarán incluidos todos los usuarios de los empleados de la empresa:

Grupo de Usuarios	Descripción
Administradores	Encargados de mantenimiento y configuración de los equipos, dominio, software… de la empresa
Directores	Directores de las sedes de la empresa
Orl	Empleados del servicio de otorrinolaringología
Audioprotesistas	Empleados del servicio de Audioprótesis
Secretarios	Secretarios de la empresa

9. DISTRIBUCIONES LINUX

En este apartado haré un estudio sobre las distribuciones de GNU/Linux existentes en el mercado, para el servidor y para los equipos de escritorio. Este estudio se hará desde la base que no tengo conocimiento alguno sobre las distribuciones de GNU/Linux existentes.

La información que a continuación se recoge está basada en páginas de Internet oficiales de cada distribución, páginas especialistas y en foros de opinión.

9.1. DISTRIBUCIÓN LINUX SERVIDOR

Las distribuciones más importantes para instalar Linux en un servidor son:

- **Debian:** Creada en 1993 por Ian Murdock, distribución creada únicamente por usuarios, no existe ninguna empresa detrás de esta distribución.
- **Ubuntu:** Distribución con mayor crecimiento en los últimos años y que más se aproxima a lo que los consumidores piden a un sistema operativo. Se basa en Debian y está gestionada por Canonical.
- **Red Hat Enterprise:** es una de las distribuciones más conocidas y más extendidas en cuanto a servidores de Linux. El acceso a soporte y actualizaciones está limitado al pago de unos honorarios.
- **CentOS:** Versión libre de *Red Hat* sin cobro de acceso a actualizaciones.
- **SuSe Enterprise:** distribución de Linux que se basa en *Red Hat* la gestión de paquetes, distribución y modelo de negocio. Desde 2003 pertenece a la empresa Novell.

Para la instalación en Audif S.L. descarto las distribuciones *Red Hat* y *SuSe* Enterprise por ser de pago, son grandes distribuciones pero que para una empresa pequeña no merece la pena pagar por ellas. Con una distribución gratuita para las PYMES es suficiente.

En cuanto a las demás distribuciones existentes de Linux no hay grandes diferencias entre ellas, cualquiera de estas para nuestro caso sería más que suficiente.

Una de las cosas que hay que tener en cuenta para elegir la distribución a instalar en el servidor son los recursos mínimos que necesitan. En la empresa donde van a ser instalados contamos que los dos servidores son equipos relativamente nuevos y que superan con creces los requisitos mínimos de cualquiera de estas distribuciones, por lo que en este caso no hay que preocuparse demasiado en este aspecto, por ejemplo para *Ubuntu Server* los requisitos mínimos son:

- Procesador x86 a 1 GHz.
- Memoria RAM de 1 GB.
- Disco Duro de 15 GB (swap incluida).
- Tarjeta gráfica y monitor capaz de soportar una resolución de 800x600.
- Lector de CD-ROM, puerto USB o tarjeta de red.
- Conexión a Internet puede ser útil.

Navegando por internet, tanto por páginas oficiales como por foros y páginas profesionales he encontrado gran cantidad de documentación muy bien detallada de la versión *Ubuntu Server 10.04 LTS* además de comprobar que es compatible con todas las necesidades de la empresa donde va a ser instalado.

Teniendo en cuenta lo anterior he decidido a instalar en los servidores la distribución de Linux *Ubuntu Server 10.04 LTS.*

9.2. DISTRIBUCIÓN LINUX CLIENTES

Para las distribuciones de Linux en los ordenadores de escritorio las cuestiones más importantes que hay que tener en cuenta son:

- Requisitos mínimos de instalación.
- Compatibilidad con las funcionalidades del servidor y empresa.
- Usuarios están acostumbrados al uso de la interfaz de Microsoft Windows.

Navegando por internet encuentro que los requisitos mínimos para las versiones de escritorio de las distribuciones de Linux no varían demasiado y que cualquiera de ellas se podrían instalar en nuestros equipos.

Las compatibilidades de los requisitos del servidor y de la empresa no son demasiados por lo que cualquiera de ellas podría valernos, aunque en este punto opto más por instalar *Ubuntu Desktop*, para homogenizar versiones en toda la empresa ya que en el servidor hemos optado por la distribución de *Ubuntu*.

En cuanto a la interfaz gráfica, tenemos que tener muy en cuenta que el usuario ha estado desde el principio usando la de Microsoft Windows y que el cambio debe de ser lo mínimo posible. Documentándome por internet he encontrado que entre las versiones más similares a Windows se encuentran *Ubuntu, Mandriva* y *Mint*.

Dado que ya tenemos elegido para el servidor la distribución de *Ubuntu Server 10.04 LTS* y vemos que la versión de escritorio es bastante sencilla para el manejo de los usuarios he optado por instalar en los escritorios la versión *Ubuntu Desktop 10.10*.

10. INSTALACIÓN SERVIDOR BARCELONA.

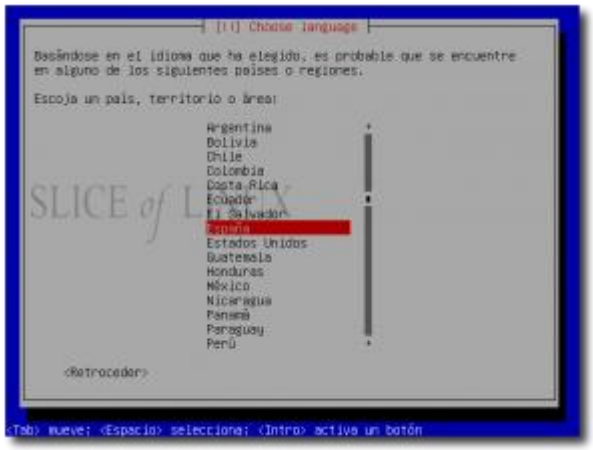
En el siguiente apartado se recoge cómo instalar y configurar desde cero tanto la versión del sistema operativo elegida cómo los programas necesarios para el uso correcto del Servidor en Audif S.L.

10.1. INSTALACIÓN DISTRIBUCIÓN LINUX

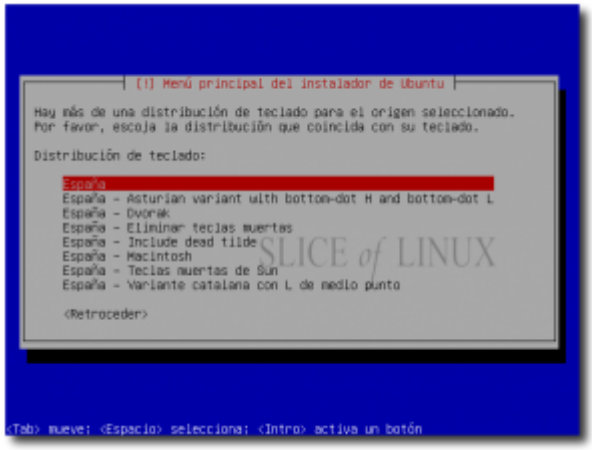
Los pasos a seguir para instalar la versión de Linux Ubuntu server 10.04 LTS son:

1. Bajar la versión de Linux Ubuntu de la página Web http://www.ubuntu.com/server/get-ubuntu/download y grabar el archivo .iso en un CD-ROM.
2. Arrancamos con el CD-ROM donde esté grabada la imagen del paso anterior.
3. Seleccionamos el idioma de la instalación.
4. Seleccionar *Instalar Ubuntu Server*

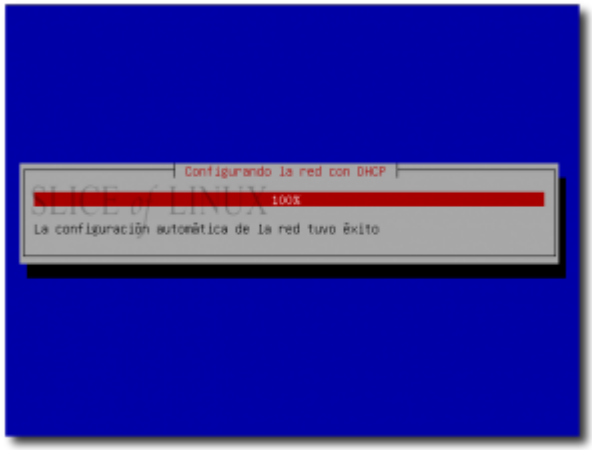
5. Seleccionamos el país.



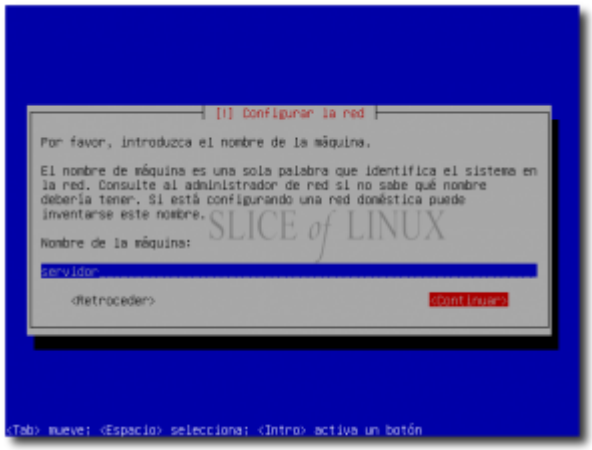
6. Seleccionar que no detecte automáticamente la distribución del teclado, y seleccionar *España.*



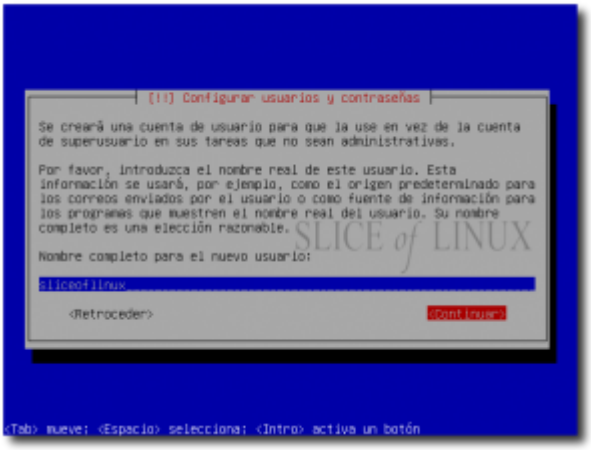
7. El siguiente paso es la configuración de la Red, en este caso al instalar el servidor dentro de una red con DHCP, esta se configura automáticamente.



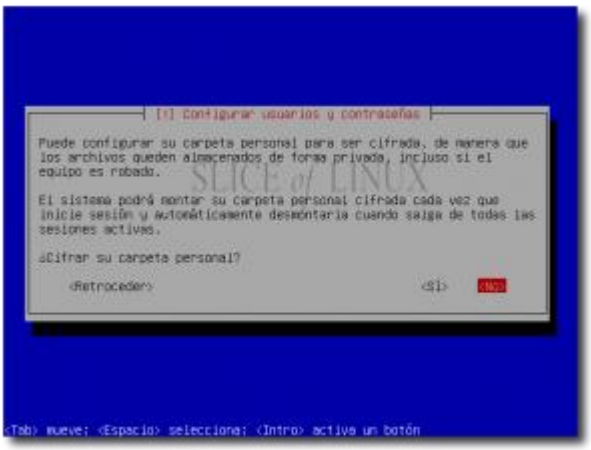
8. Poner el nombre del Servidor (En nuestro caso lo llamaremos BCNserver)



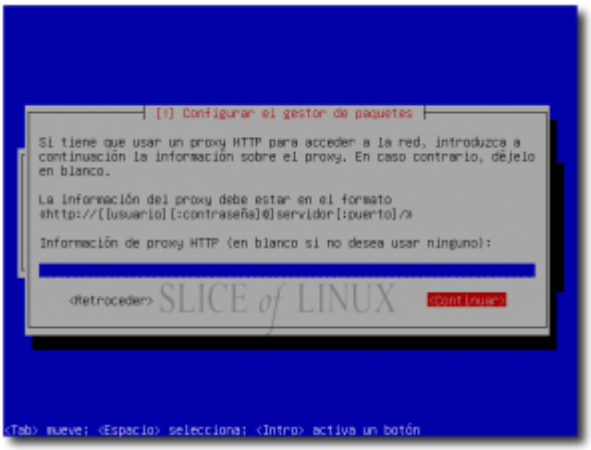
9. Se nos mostrará la zona horaria, si es correcta pulsar *Sí.*
10. Realizar el particionado del disco duro, en este caso se podrá seguir un asistente o bien crearlas manualmente.
11. Crear cuenta de usuario con privilegios de administrador, nombre de usuario y contraseña.



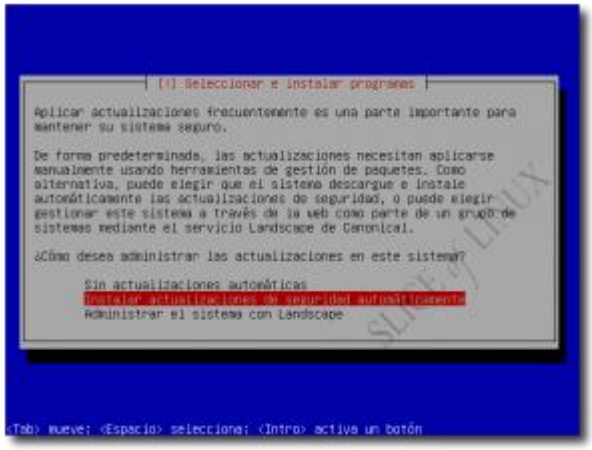
12. Seleccionar si la carpeta personal de la sesión del usuario anteriormente creado la queremos cifrada o no.



13. Configurar el gestor de paquetes, si el servidor está detrás de un proxy habrá que insertarlo. En nuestro caso no tenemos proxy.



14. Configurar el sistema de actualizaciones (Automáticas o manuales)



15. Instalación de servicios. En nuestro caso de momento instalamos solamente el servicio OpenSSH.

16. El último paso es la instalación del cargador de arranque GRUB en el registro principal de arranque.
17. Sacar el CD-ROM de la unidad.

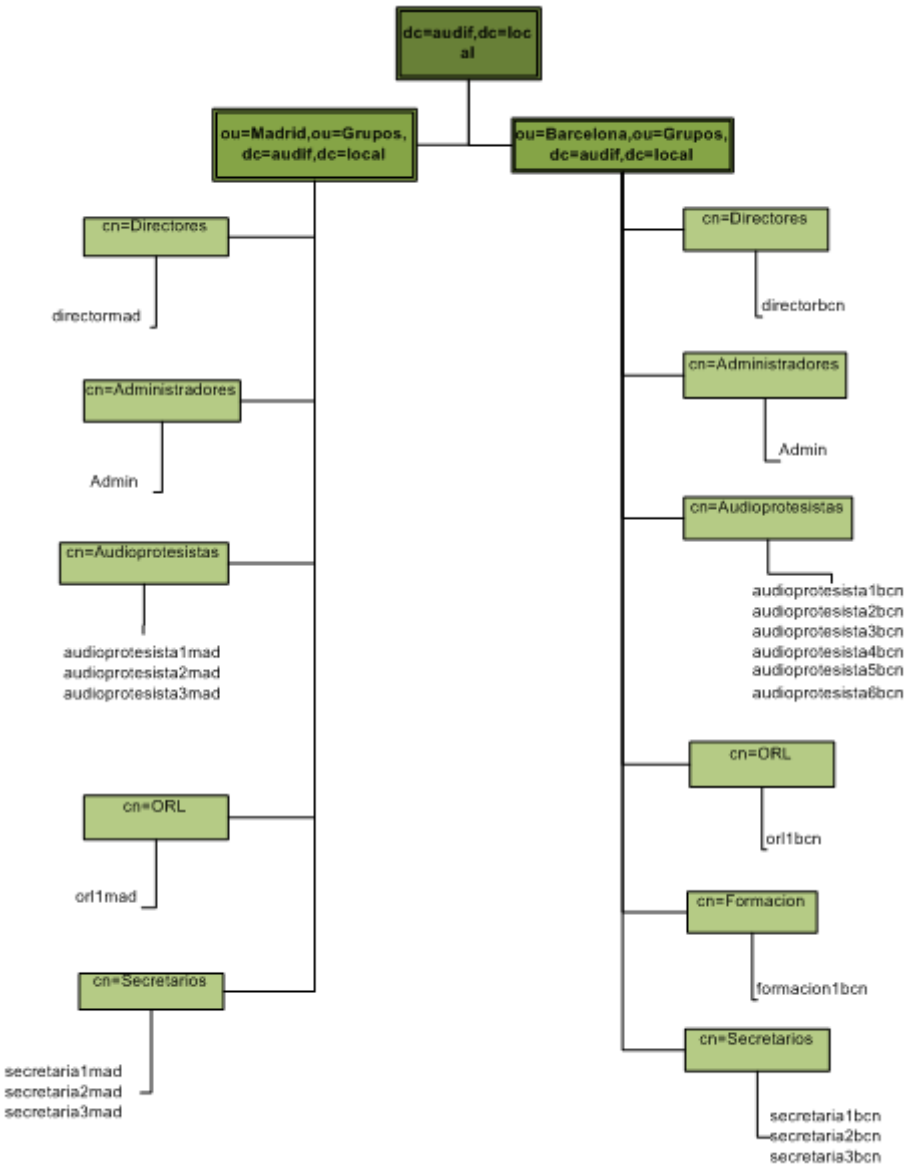
Esta versión de Ubuntu, al estar dedicada exclusivamente para servidores, no tiene ningún entorno gráfico disponible, por lo que cualquier el instalar o configurar cualquier programa podría resultar algo pesado y más costoso.

Por ello y dado que existe la posibilidad de instalar un entorno gráfico para servidores Ubuntu lo instalamos a continuación:

1. Elegir el entorno gráfico a instalar entre los existentes, en nuestro caso el elegido es KDE a modo completo.
2. Introducir el comando para instalar el paquete:
   ```
   jaime@BCNserver:~$ sudo apt-get install kubuntu-desktop
   ```
3. Una vez instalado introducir en el terminal `jaime@BCNserver:~$ startx` y arrancará el interfaz gráfico.

10.2. INSTALACIÓN DE SERVICIOS LDAP

El esquema implantado en el servicio de directorio activo de Audif es el siguiente:



Lo siguiente que hay que instalar en el servidor es OpenLDAP, el dominio slapd y un paquete con utilidades para la gestión del dominio. Para ello seguimos los siguientes pasos:

1. Instalación mediante el siguiente comando:

```
jaime@BCNserver:~$ sudo apt-get install slapd ldap-utils
```

2. Con el siguiente comando se configura el servidor LDAP mediante un asistente.

```
jaime@BCNserver:~$ sudo dpkg-reconfigure slapd
```

   Y las opciones elegidas son:

   - Desea omitir la configuración del servidor OpenLDAP? **NO**
   - DNS Domain Name: **audif.local**
   - Organization Name: **audif.local**
   - Database: **BDB**
   - Desea que se borre la base de datos cuando se purgue el paquete slapd?: **NO**

- Desea mover la base de datos antigua? **SI**
- Contraseña del administrador: **Passw0rd**
- Verificar la contraseña: **Passw0rd**
- Allow LDAPv2 protocol?: **NO**

Para la creación de la estructura organizativa de la empresa utilizo el entorno gráfico phpldapadmin. Esta herramienta es una webfronted que sirve para la gestión de los distintos tipos de cuentas en un directorio LDAP. Está escrito en PHP y se distribuye bajo licencia pública general de GNU.

Para la instalación y configuración de phpldapadmin hay que seguir los siguientes pasos:

1. Instalación de phpldapadmin

```
jaime@BCNserver:~$ sudo aptitude install phpldapadmin
```

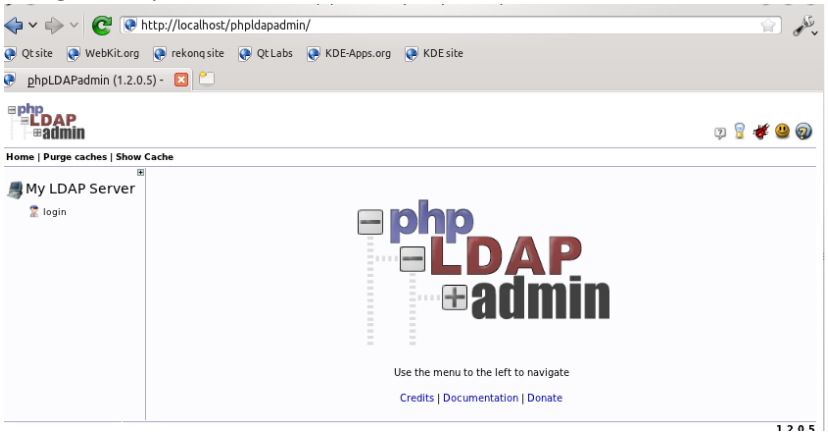
2. Para la configuración de phpldapadmin hay que editar el archivo /etc/phpldapadmin/config.php.
   - Cambiar los valores de defecto de conexión del dominio del servidor por los de nuestro dominio, según se puede observar en la siguiente pantalla.

```
/*********************************************/
/* Define your LDAP servers in this section  */
/*********************************************/

$servers = new Datastore();

/* $servers->NewServer('ldap_pla') must be called before each new LDAP server
   declaration. */
$servers->newServer('ldap_pla');

/* A convenient name that will appear in the tree viewer and throughout
   phpLDAPadmin to identify this LDAP server to users. */
$servers->setValue('server','name','My LDAP Server');

/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com/',
   'ldapi://%2fusr%local%2fvar%2frun%2fldapi'
         (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','127.0.0.1');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=audif,dc=local'));
```

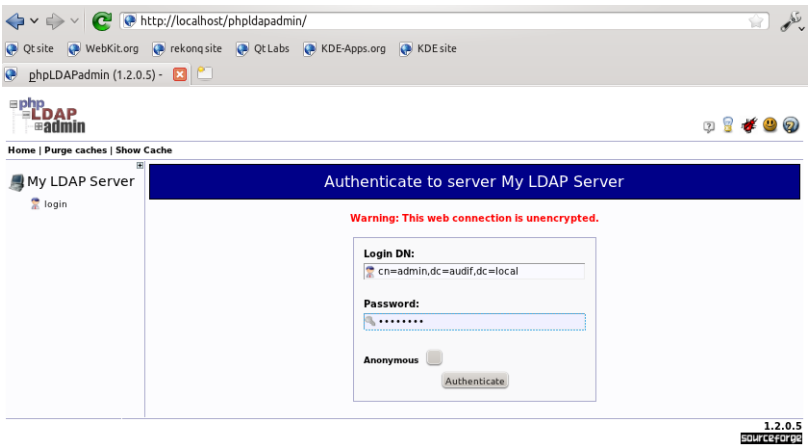
   - Modificar los datos de conexión para entrar en phpldapadmin con los datos de nuestro dominio, como se muestra en la siguiente pantalla.

```
$servers->setValue('server','base',array('dc=audif,dc=local'));

/* Four options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will
      store your login dn and password.
   2. 'session': same as cookie but your login dn and password are stored on the
      web server in a persistent session variable.
   3. 'http': same as session but your login dn and password are retrieved via
      HTTP authentication.
   4. 'config': specify your login dn and password here in this config file. No
      login will be required to use phpLDAPadmin for this server.

   Choose wisely to protect your authentication information appropriately for
   your situation. If you choose 'cookie', your cookie contents will be
   encrypted using blowfish and the secret your specify above as
   session['blowfish']. */
$servers->setValue('login','auth_type','session');

/* The DN of the user for phpLDAPadmin to bind with. For anonymous binds or
   'cookie' or 'session' auth_types, LEAVE THE LOGIN_DN AND LOGIN_PASS BLANK. If
   you specify a login_attr in conjunction with a cookie or session auth_type,
   then you can also specify the bind_id/bind_pass here for searching the
   directory for users (ie, if your LDAP server does not allow anonymous binds. */
$servers->setValue('login','bind_id','cn=admin,dc=audif,dc=local');
#  $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
```

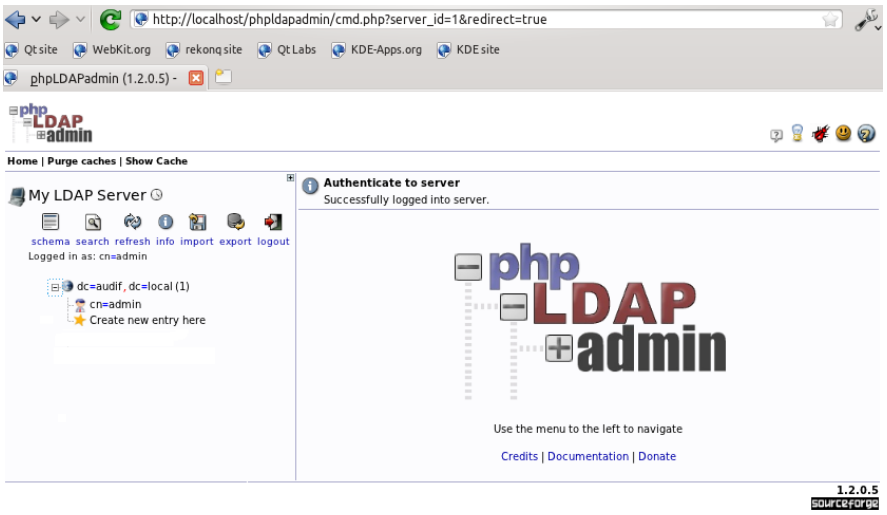
3. Abrir explorador de internet e introducir la ruta: "http://localhost/phpldapadmin" y se mostrará la siguiente pantalla:



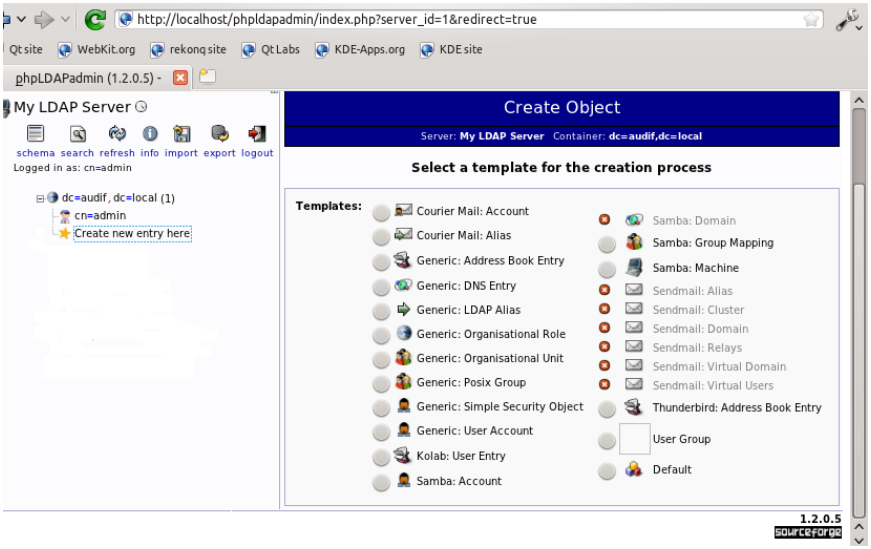
4. Pulsamos sobre login, introducimos la contraseña del usuario admin del dominio y damos a *"Authenticate"*.



5. En la parte izquierda de la pantalla se muestra la estructura actual del directorio ldap. Donde actualmente solo tenemos un usuario llamado *"admin"*

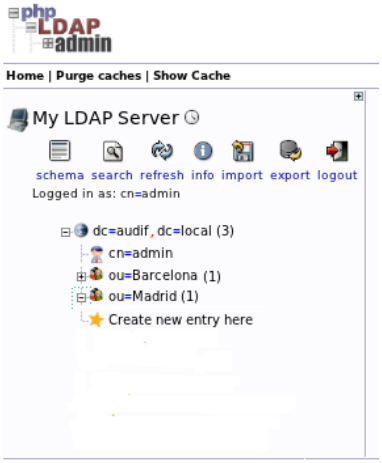


6. El paso siguiente es crear las unidades organizativas (ou) de Barcelona y Madrid, para ello hacemos click en *"create new entry here"* y se muestra la siguiente pantalla.

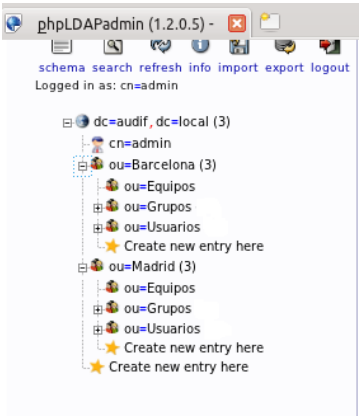


Seleccionamos *"Generic: Organisational Unit"* introducimos el nombre de la unidad organizativa (Barcelona o Madrid), *"create object"* y se mostrará la siguiente pantalla con la información del objeto a introducir.

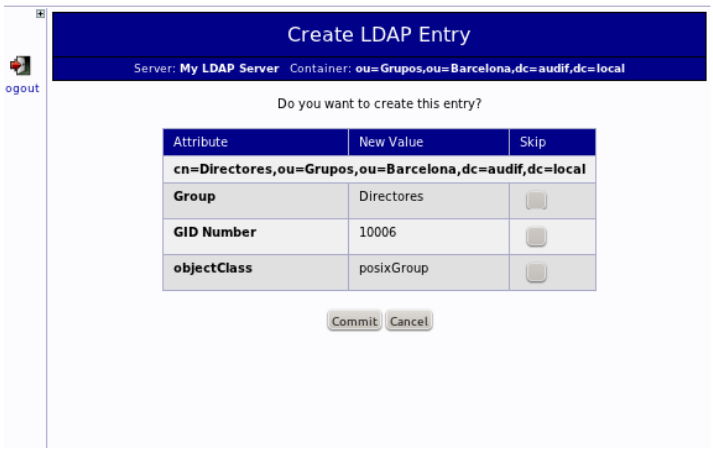
Seleccionamos *"Commit"* y se crea la nueva unidad organizativa. Este proceso hay que repetirlo para la creación de la unidad organizativa *Madrid*. Cómo resultado tendremos la siguiente estructura en el dominio.



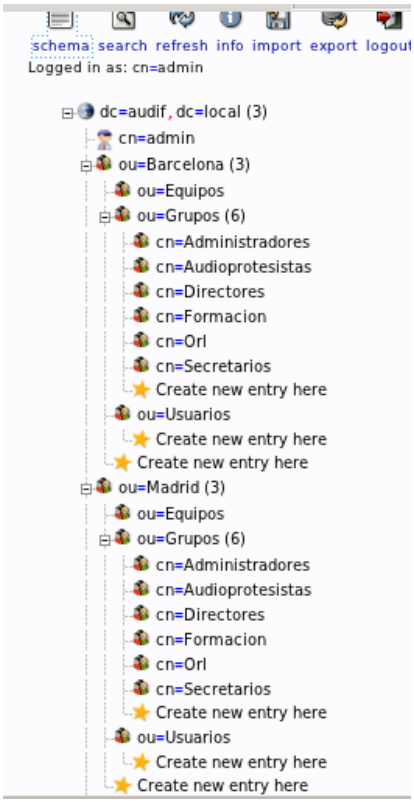
7. El siguiente paso es crear Las unidades organizativas *Equipos, Grupos y Usuarios* dentro de *Barcelona* y *Madrid* de la misma forma que en el paso anterior. Teniendo como resultado la estructura que se muestra en la siguiente pantalla.



8. Seguidamente hay que crear los grupos de usuarios *Administradores, Audioprotesistas, Directores, Formación, Orl* y *Secretarios* dentro de la unidad organizativa *Grupos* de *Barcelona* y de *Madrid.*
   Para ello hacemos click en dicha ou=Grupos de *Barcelona* y en *"Create new entry here"* se mostrará la misma pantalla que en el punto 6, donde en este caso seleccionaremos *"Generic: Posix Group"*. Se introduce el nombre del grupo que queramos añadir y hacemos click sobre *"Create object"* y se mostrará un resumen del objeto a insertar como podemos ver en la siguiente pantalla.

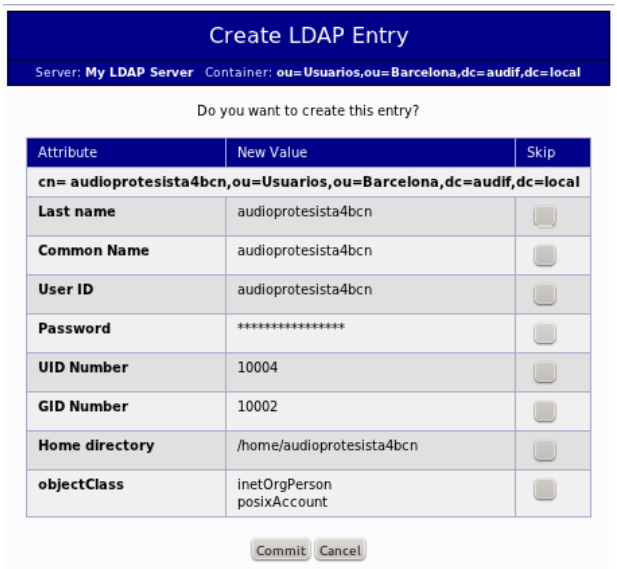


   Finalmente pinchamos sobre el botón *"Commit"* para terminar de crear el objeto.
   Una vez insertados todos los grupos en las diferentes unidades organizativas tenemos como resultado la siguiente estructura del dominio.



9. El siguiente paso es insertar los usuarios en el dominio. Para ello nos situamos dentro de la unidad organizativa llamada ou=Usuarios (primero los creamos en *Barcelona* y después en *Madrid)* pulsamos sobre *"Create new entry here"* aparecerá la pantalla de creación de objetos del punto 6.
   En este caso tenemos que seleccionar la opción *"Generic: User Account"* y se mostrará la siguiente pantalla para su creación.
   Donde los campos de un color pastel son obligatorios rellenar.
   Los campos corresponden con:
   - First name: Nombre propio del usuario.
   - Last name: Apellido del usuario.
   - Common name: Identificador dentro del directorio Ldap.
   - User ID: nombre de la cuenta de usuario.
   - Password: Contraseña de entrada.
   - UID Number: numero de identificador de usuario (Automático).
   - GID Number: grupo del ldap al que pertenece el usuario.
   - Home directory: directorio raiz del usuario.
   - Login shell: shell de inicio de sesión.

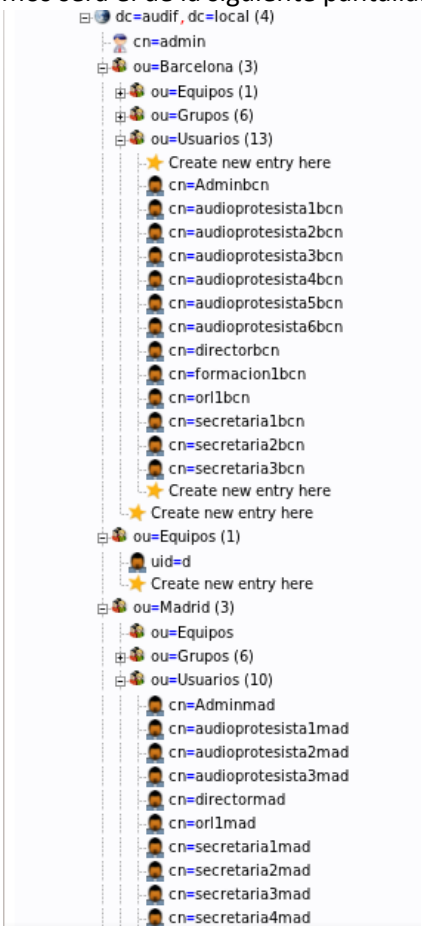
Una vez rellenados todos los datos pulsamos en *"Create Object"* y se muestra la siguiente pantalla con la información del usuario que se va a crear.



Pulsando *Commit* se crea el usuario.

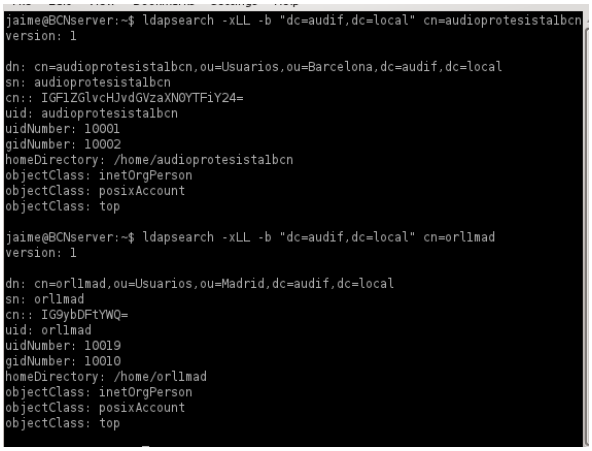
Este proceso tendremos que realizarlo tantas veces como usuarios tiene el dominio, tanto en la unidad organizativa *Barcelona* como en *Madrid.*

El resultado que obtendremos será el de la siguiente pantalla.



En este punto ya tenemos configurado nuestro dominio *"audif.local"* correctamente. Para comprobarlo ejecutamos desde la consola de ubuntu el comando *ldapsearch* y

buscamos dos usuarios por ejemplo *auidoprotesista1bcn* y *orl1mad*, y se mostrará la siguiente pantalla con toda su información.



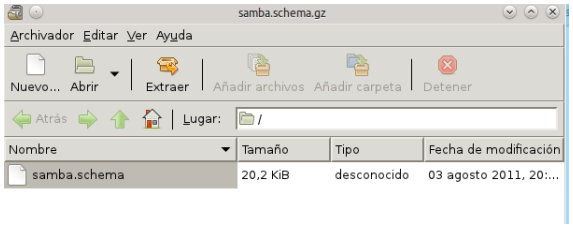
10.3. INSTALACIÓN Y CONFIGURACIÓN SAMBA

Para integrar Samba con LDAP es necesario instalar tres paquetes: Samba, samba-docs y Samba-tools. Con el siguiente comando lo instalamos:

```
jaime@BCNserver:~$ sudo apt-get install Samba samba-docs smbldap-tools
```

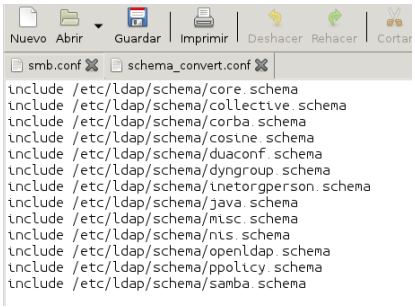
10.3.1. CONFIGURACIÓN DE SAMBA

Es necesario añadir los esquemas samba al directorio LDAP. Estos esquemas se encuentran en el paquete samba-docs, hay que descomprimirlos en /etc/ldap/schema. Gracias al entorno gráfico KDE haciendo doble click sobre el archivo samba.schema.gz que se encuentra en la ruta /usr/share/doc/samba-doc/examples/LDAP/ y se abre la siguiente pantalla.



Pulsamos sobre el icono "Extraer" le indicamos la ruta donde hay que situarlo /etc/ldap/schema/ y nos descomprime el archivo.

A continuación creamos un archivo llamado por ejemplo schema_convert.conf con el siguiente contenido.



Seguidamente creamos un directorio temporal usamos el comando *salpact* para crear el nuevo esquema de LDAP como se indica a continuación.

```
jaime@BCNserver:~$ sudo mkdir /tmp/ldif_out
jaime@BCNserver:~$ sudo slapcat -f schema_convert.conf -F /tmp/ldif_out/ -n0 -s "cn=samba,cn=schema,cn=
config" > /tmp/cn=samba.ldif
```

Si vamos al directorio */tmp/ldif_out/cn=config/cn=schema/* comprobamos que se ha creado un archivo nuevo llamado *cn={12}samba.ldif* que hay que modificarlo para poder terminar la configuración.

Lo abrimos, las tres primeras líneas hay que dejarlas como se muestra a continuación.

```
dn: cn=Samba,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: Samba
```

Y al final del archivo hay que eliminar el siguiente texto.

```
structuralObjectClass: olcSchemaConfig
entryUUID: d4c4c5f4-ba57-1030-8cf0-75dbdc9fea99
creatorsName: cn=config
createTimestamp: 20111214042835Z
entryCSN: 20111214042835.166915Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20111214042835Z
```

Este archivo lo guardamos con el nombre *cn=samba.ldif* y ya lo tenemos preparado para añadir el esquema Samba al directorio LDAP y quede totalmente integrado con este, para ello se procede insertando el siguiente comando:

```
jaime@BCNserver:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/cn=samba.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=Samba,cn=schema,cn=config"
```

Una vez que tenemos el esquema de Samba añadido al directorio LDAP hay que configurar Samba, para ello editamos el archivo */etc/samba/smb.conf* con los parámetros de nuestro dominio LDAP, usuarios y seguridad quedando como resultado el siguiente archivo.

```
[global]
workgroup = audif
server string = %h server (Samba, Ubuntu)
map to guest = Bad User
passdb backend = ldapsam:ldap://localhost
pam password change = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .
username map = /etc/samba/smbusers
unix password sync = Yes
syslog = 0
log file = /var/log/samba/log.%m
max log size = 100
panic action = /usr/share/samba/panic-action %d
security = user
encrypt passwords = yes
usershare allow guests = Yes
# LDAP Settings
passdb backend = ldapsam:ldap://127.0.0.1
ldap suffix = dc=audif,dc=local
ldap user suffix = ou=Barcelona,ou=usuarios;ou=Madrid,ou=usuarios
ldap group suffix = ou=Barcelona,ou=grupos:ou=Madrid,ou=grupos
ldap machine suffix = ou=Barcelona,ou=equipos;ou=Madrid,ou=equipos
ldap idmap suffix = ou=Idmap
ldap admin dn = cn=admin,dc=audif,dc=local
ldap ssl = off
ldap passwd sync = yes
add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%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"
set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

Se reinician los servicios de Samba para que coja la nueva configuración, mediante los comandos.

```
jaime@BCNserver:~$ sudo restart smbd
jaime@BCNserver:~$ sudo restart nmbd
```

Para comprobar que funciona correctamente podemos poner el siguiente comando y vemos que nos devuelve el uid del dominio Samba dentro del LDAP.

```
SID for domain BCNSERVER is: S-1-5-21-1765198653-2688228149-1470090736
jaime@BCNserver:~$
```

Samba necesita conocer del password de LDAP, para ello hay que pasárselo con el siguiente comando.

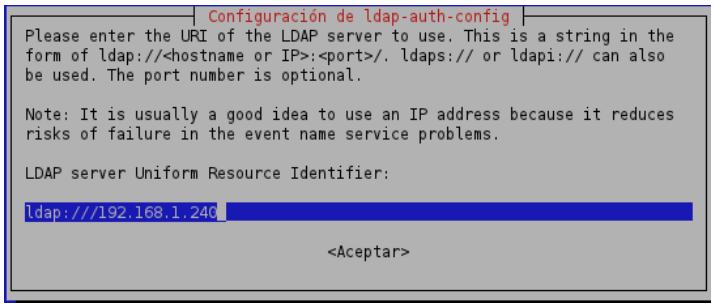
```
jaime@BCNserver:~$ sudo smbpasswd -w Passw0rd
Setting stored password for "cn=admin,dc=audif,dc=local" in secrets.tdb
jaime@BCNserver:~$
```

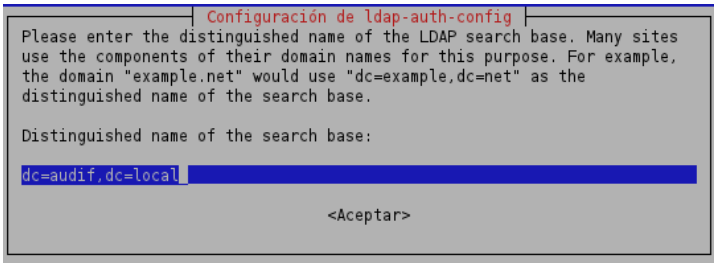
10.4. CONFIGURACIÓN PARA AUTENTICACIÓN DE USUARIOS

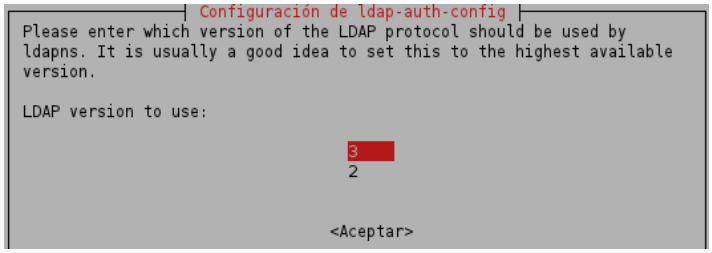
Es necesario instalar el paquete ldap-auth-cliente para que los usuarios del dominio LDAP se puedan autenticar contra él. Se realiza mediante un asistente con el siguiente comando.

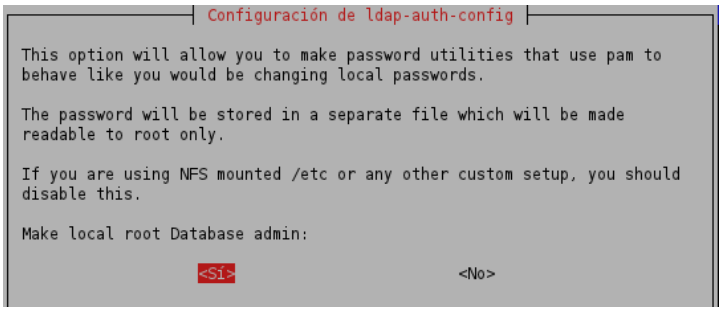
```
jaime@ubuntuBCN:~$ sudo apt-get --yes install ldap-auth-client
```

Salen una serie de pantallas que iremos seleccionando lo siguiente en cada una de ellas.

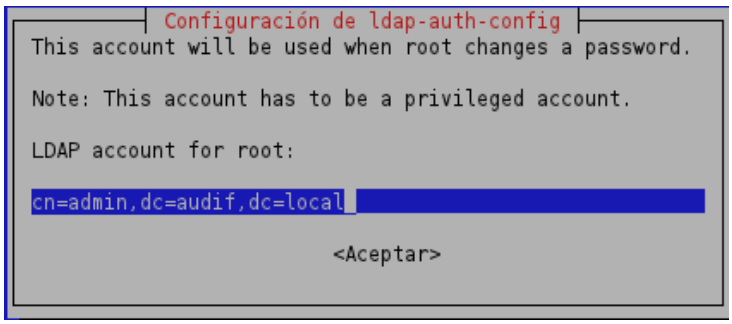

Configuración de ldap-auth-config
Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.
Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.
LDAP server Uniform Resource Identifier:
ldap:///192.168.1.240
<Aceptar>

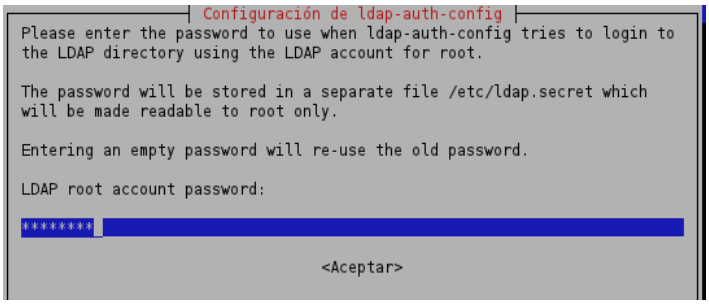

Configuración de ldap-auth-config
Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.
Distinguished name of the search base:
dc=audif,dc=local
<Aceptar>


Configuración de ldap-auth-config
Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.
LDAP version to use:
3
2
<Aceptar>


Configuración de ldap-auth-config
This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.
The password will be stored in a separate file which will be made readable to root only.
If you are using NFS mounted /etc or any other custom setup, you should disable this.
Make local root Database admin:
<Sí>
<No>


Configuración de ldap-auth-config
Choose this option if you are required to login to the database to retrieve entries.
Note: Under a normal setup, this is not needed.
Does the LDAP database require login?
<Sí>
<No>


Configuración de ldap-auth-config
This account will be used when root changes a password.
Note: This account has to be a privileged account.
LDAP account for root:
cn=admin,dc=audif,dc=local
<Aceptar>



En este punto tenemos el servidor de Barcelona implementado al completo para la autenticación de usuarios del dominio LDAP.

10.5. INSTALACIÓN DE COLA DE IMPRESIÓN

Para instalar la cola de impresión en el Servidor seguiremos los siguientes pasos:

1. *sudo apt-get install cups*
2. Para compartir impresoras se añaden al archivo */etc/Samba/smb.conf* lo siguiente:

```
[print$]
Coment = Print Drivers
Path = /var/lib/Samba/printers
browsable = yes
read only = yes
guest ok = yes
[printers]
Comment = Printer
browsable = yes
path = /var/spool/Samba
printable = yes
guest ok = yes
read only = no
create mask = 0755
```

10.5.1. INSTALACIÓN DE IMPRESORA PDF

En la oficina de Barcelona se instalará una impresora de red (en el momento que se disponga de ella), y una impresora pdf para poder imprimir documentos en este formato.

Para ello ejecutamos el siguiente comando.

```
jaime@BCNserver:~$ sudo apt-get install cups-pdf
```

Para que la impresora sea vista por todos los usuarios hay que cambiar los permisos mediante el siguiente comando.

```
jaime@BCNserver:~$ sudo chmod u+s /usr/lib/cups/backend/cups-pdf
```

Ya tenemos la impresora compartida y con los permisos necesarios para poder instalarla en los equipos clientes.

10.6. INSTALACIÓN DE CONTROL DE VERSIONES

Para instalar el control de versiones se ejecuta el siguiente comando:

```
jaime@BCNserver:~$ sudo apt-get install cvs cvsd
```

Es necesario también instalar *xinetd* para poder arrancar y parar el servidor CVS. Para esto ejecutamos el siguiente comando.

```
jaime@BCNserver:~$ sudo apt-get install xinetd
```

Una vez instalados los dos programas hay que configurar *xinted* para inicializar el servidor *CVS*, para esto hay que editar el archivo /etc/xinted.d/cvspserver quedando como en la pantalla siguiente.

```
service cvspserver
{
port = 2401
socket_type= stream
protocol= tcp
user= root
wait= no
type= UNLISTED
server= /usr/bin/cvsd/cvs
server_args= -f --allow-root /var/lib/cvsd/cvs pserver
disable= no
}
```

El directorio de repositorios será: /var/lib/cvsd/cvs

Se ejecuta el comando siguiente.

```
jaime@BCNserver:~$ sudo cvsd-buildroot /var/lib/cvsd/cvs
```

Iniciamos el repositorio con el comando.

```
jaime@BCNserver:~$ sudo cvs -d /var/lib/cvsd/cvs init
```

Reiniciamos el servidor para que se hagan efectivos los cambios de la última configuración.

```
jaime@BCNserver:~$ sudo /etc/init.d/xinetd restart
```

Y ya está listo el repositorio de archivos del servidor, para comprobarlo utilizamos el siguiente comando.

```
jaime@BCNserver:~$ sudo netstat -tap | grep cvs
tcp        0      0 *:cvspserver            *:*                     ESCUCHAR    28621/cvsd
```

10.7. INSTALACIÓN DE GESTIÓN DE DOCUMENTACIÓN

Para la instalación de MoinMoin se utiliza el siguiente comando.

```
jaime@BCNserver:/usr/share/moin$ sudo apt-get install python-moinmoin
```

Se crea nuestra Wiki llamada *"AudifonWiky"* en */usr/share/moin/AudifonWiky/* además le añadimos los archivos y directorios necesarios para que la Wiki se encuentre en su estado inicial, y le añadimos los permisos pertinentes a la carpeta de la Wiki *"AudifonWiky"* mediante los siguientes comandos:

```
jaime@BCNserver:/usr/share/moin$ sudo mkdir AudifonWiky
jaime@BCNserver:/usr/share/moin$ sudo cp -R data AudifonWiky
jaime@BCNserver:/usr/share/moin$ sudo cp -R underlay AudifonWiky
jaime@BCNserver:/usr/share/moin$ sudo cp -R server/moin.cgi AudifonWiky
jaime@BCNserver:/usr/share/moin$ sudo cp server/moin.cgi AudifonWiky
jaime@BCNserver:/usr/share/moin$ sudo chown -R www-data.www-data AudifonWiky
jaime@BCNserver:/usr/share/moin$ sudo chmod -R ug+rwX AudifonWiky
jaime@BCNserver:/usr/share/moin$ sudo chmod -R o-rwx AudifonWiky
```

El siguiente paso es configurar MoinMoin para que encuentre nuestra Wiki *"AudifonWiky"*. Para ello hay que editar el archivo /etc/moin/mywiki.py para que quede de la siguiente forma.

```
# basic options (you normally need to change these)
sitename = u'AudifonWiky' # [Unicode]
interwikiname = u'AudifonWiky' # [Unicode]

# name of entry page / front page [Unicode], choose one of those:

# a) if most wiki content is in a single language
#page_front_page = u"MyStartingPage"

# b) if wiki content is maintained in many languages
page_front_page = u"FrontPage"

data_dir = '/usr/share/moin/AudifonWiky/data/'
data_underlay_dir = '/usr/share/moin/AudifonWiky/underlay/'
```

Además hay que configurar *Apache* para que pueda acceder a la nueva Wiki creada. Para ello hay que modificar el archivo */etc/apache2/sites_avaible/default* y debajo de la etiqueta *<Virtual_Host>* se añaden las siguientes líneas:

```
###moin
        ScriptAlias /AudifonWiky "/usr/share/moin/AudifonWiky/moin.cgi"
        alias /moin_static184 "/usr/share/moin/htdocs/"
        <Directory /usr/share/moin/htdocs>
        Order allow,deny
        allow from all
        </Directory>
###end moin
```

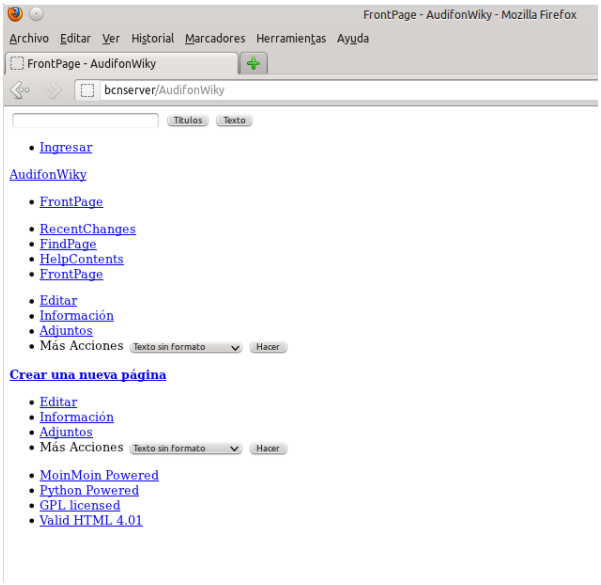
Seguidamente se reinicia el servicio de apache con el comando:

```
jaime@BCNserver:/usr/share/moin$ sudo /etc/init.d/apache2 restart
```

Ya tenemos el servidor Wiki instalado y configurado listo para usar.

10.8. PRUEBAS DE ACCESO AL SERVIDOR DE DOCUMENTACIÓN

Para probar el acceso al servidor de documentación abrimos un navegador de internet y se pone la dirección *http://bcnserver/AudifonWiky* y se mostrará la siguiente pantalla:



Por lo que se comprueba que funciona correctamente.

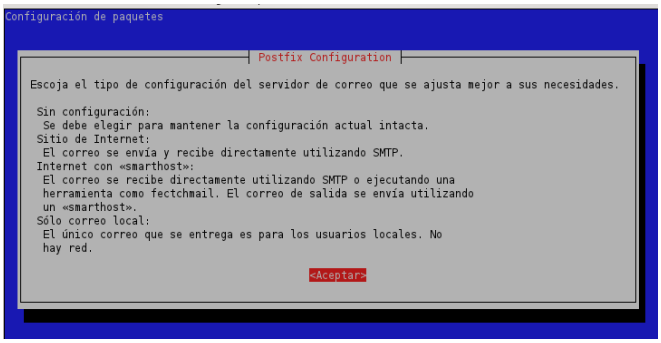
10.9. INSTALACIÓN SERVIDOR DE CORREO

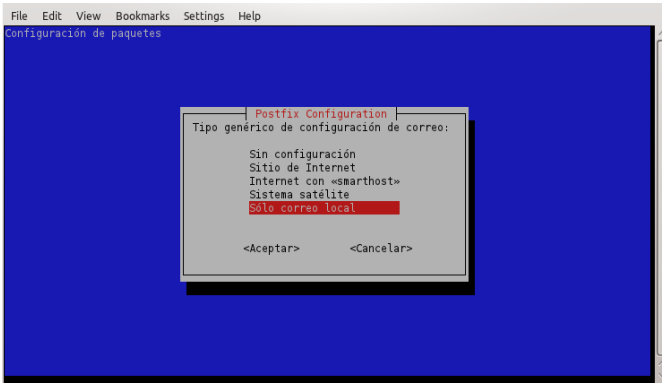
10.9.1. INSTALACIÓN DE SERVIDOR SMTP POSTFIX

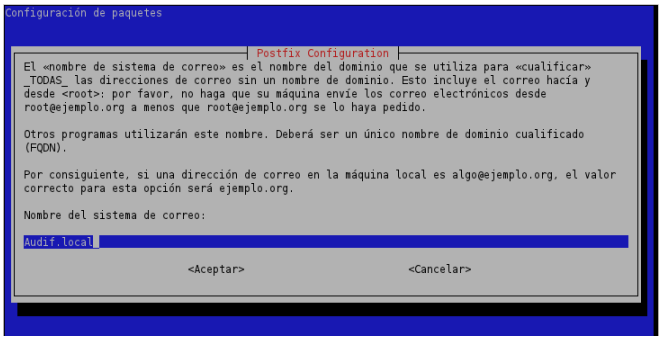
Se instala Postfix con el siguiente comando.

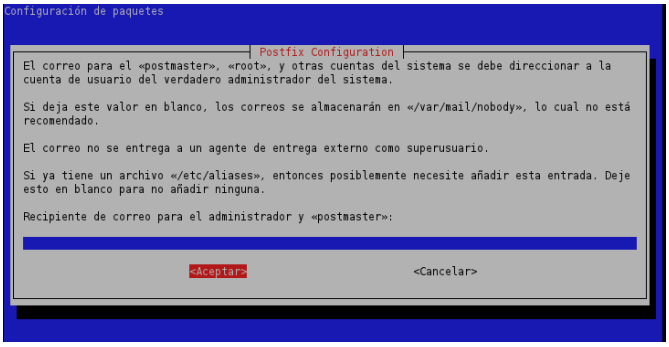
```
jaime@BCNserver:~$ sudo apt-get install postfix
```

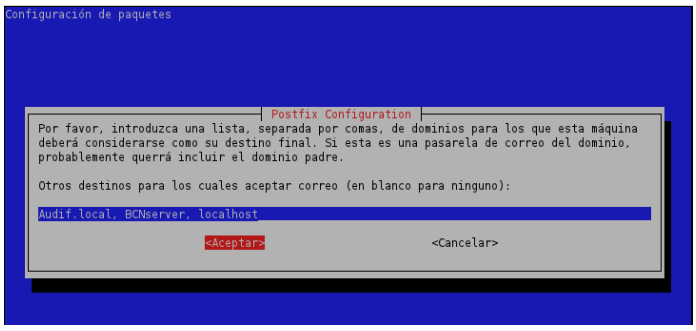
Después se lanzará el asistente de configuración (si no se lanzará hay que forzar el lanzamiento mediante el comando *"sudo dpkg-reconfigure postfix"*) Se contestará de la siguiente forma a las preguntas de configuración.

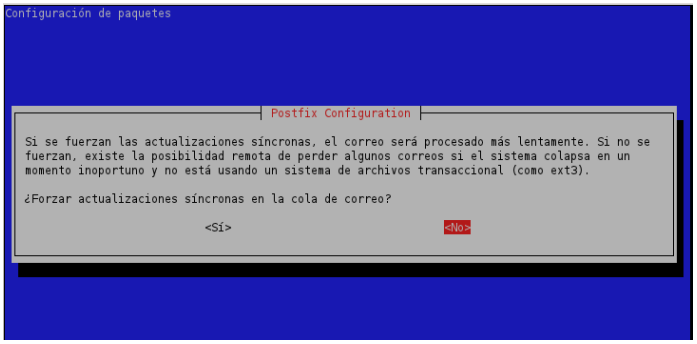


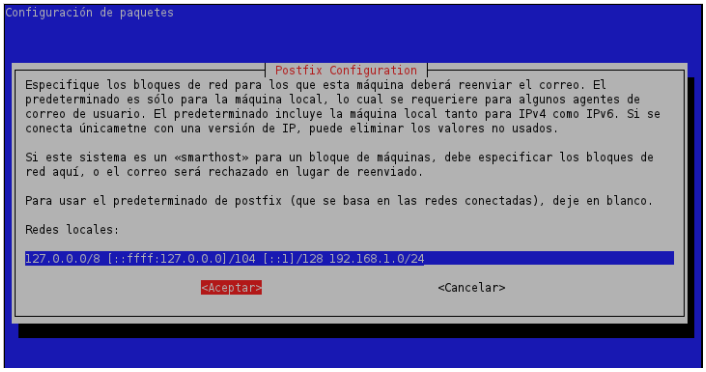

File Edit View Bookmarks Settings Help
Configuración de paquetes
Postfix Configuration
Tipo genérico de configuración de correo:
Sin configuración
Sitio de Internet
Internet con «smarthost»
Sistema satélite
Sólo correo local
<Aceptar> <Cancelar>

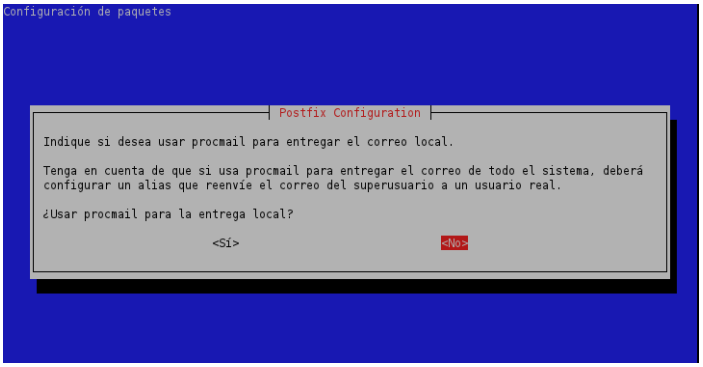

Configuración de paquetes
Postfix Configuration
El «nombre de sistema de correo» es el nombre del dominio que se utiliza para «cualificar» _TODAS_ las direcciones de correo sin un nombre de dominio. Esto incluye el correo hacia y desde <root>: por favor, no haga que su máquina envíe los correo electrónicos desde root@ejemplo.org a menos que root@ejemplo.org se lo haya pedido.
Otros programas utilizarán este nombre. Deberá ser un único nombre de dominio cualificado (FQDN).
Por consiguiente, si una dirección de correo en la máquina local es algo@ejemplo.org, el valor correcto para esta opción será ejemplo.org.
Nombre del sistema de correo:
Audif.local
<Aceptar> <Cancelar>

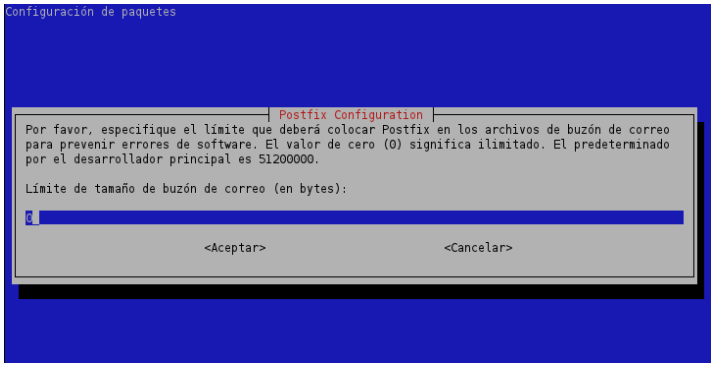

Configuración de paquetes
Postfix Configuration
El correo para el «postmaster», «root», y otras cuentas del sistema se debe direccionar a la cuenta de usuario del verdadero administrador del sistema.
Si deja este valor en blanco, los correos se almacenarán en «/var/mail/nobody», lo cual no está recomendado.
El correo no se entrega a un agente de entrega externo como superusuario.
Si ya tiene un archivo «/etc/aliases», entonces posiblemente necesite añadir esta entrada. Deje esto en blanco para no añadir ninguna.
Recipiente de correo para el administrador y «postmaster»:
<Aceptar> <Cancelar>


Configuración de paquetes
Postfix Configuration
Por favor, introduzca una lista, separada por comas, de dominios para los que esta máquina deberá considerarse como su destino final. Si esta es una pasarela de correo del dominio, probablemente querrá incluir el dominio padre.
Otros destinos para los cuales aceptar correo (en blanco para ninguno):
Audif.local, BCNserver, localhost
<Aceptar> <Cancelar>

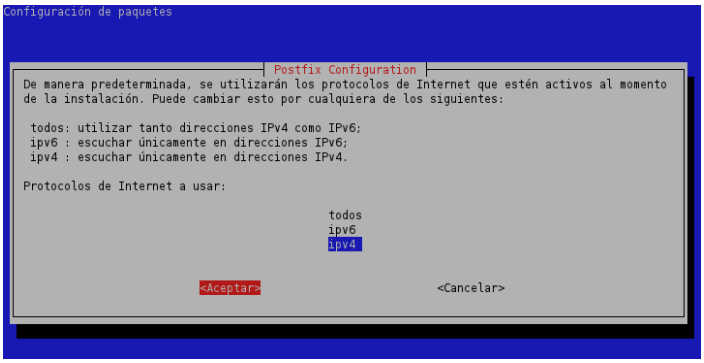

Configuración de paquetes
Postfix Configuration
Si se fuerzan las actualizaciones síncronas, el correo será procesado más lentamente. Si no se fuerzan, existe la posibilidad remota de perder algunos correos si el sistema colapsa en un momento inoportuno y no está usando un sistema de archivos transaccional (como ext3).
¿Forzar actualizaciones síncronas en la cola de correo?
<Sí> <No>


Configuración de paquetes
Postfix Configuration
Especifique los bloques de red para los que esta máquina deberá reenviar el correo. El predeterminado es sólo para la máquina local, lo cual se requeriere para algunos agentes de correo de usuario. El predeterminado incluye la máquina local tanto para IPv4 como IPv6. Si se conecta únicametne con una versión de IP, puede eliminar los valores no usados.
Si este sistema es un «smarthost» para un bloque de máquinas, debe especificar los bloques de red aquí, o el correo será rechazado en lugar de reenviado.
Para usar el predeterminado de postfix (que se basa en las redes conectadas), deje en blanco.
Redes locales:
127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24
<Aceptar>
<Cancelar>


Configuración de paquetes
Postfix Configuration
Indique si desea usar procmail para entregar el correo local.
Tenga en cuenta de que si usa procmail para entregar el correo de todo el sistema, deberá configurar un alias que reenvíe el correo del superusuario a un usuario real.
¿Usar procmail para la entrega local?
<Sí>
<No>


Configuración de paquetes
Postfix Configuration
Por favor, especifique el límite que deberá colocar Postfix en los archivos de buzón de correo para prevenir errores de software. El valor de cero (0) significa ilimitado. El predeterminado por el desarrollador principal es 51200000.
Límite de tamaño de buzón de correo (en bytes):
0
<Aceptar>
<Cancelar>


Configuración de paquetes
Postfix Configuration
Indique el carácter que se usará para definir una extensión de dirección local.
Para no usar extensiones de dirección, deje la cadena en blanco.
Carácter de extensión de direcciones locales:
+
<Aceptar>
<Cancelar>


Configuración de paquetes
Postfix Configuration
De manera predeterminada, se utilizarán los protocolos de Internet que estén activos al momento de la instalación. Puede cambiar esto por cualquiera de los siguientes:
todos: utilizar tanto direcciones IPv4 como IPv6;
ipv6 : escuchar únicamente en direcciones IPv6;
ipv4 : escuchar únicamente en direcciones IPv4.
Protocolos de Internet a usar:
todos
ipv6
ipv4
<Aceptar>
<Cancelar>

Ya tenemos configurado el servidor SMTP Potsfix.

El siguiente paso es configurar el formato de los buzones de correo, para ello decidimos que fuera MailDir, se hace con el siguiente comando.

```
jaime@BCNserver:~$ sudo postconf -e 'home_mailbox=Maildir/'
```

10.9.2. INSTALACIÓN Y CONFIGURACIÓN DE DOVECOT (IMAP, POP3)

El siguiente comando es el que se utiliza para la instalación de *dovecot.*

```
jaime@BCNserver:~$ sudo apt-get install dovecot-imapd dovecot-pop3d
```

Hay que configurar el archivo /etc/dovecot/dovecot.conf. Se configurará para usar el protocolo IMAP, buzones de tipo Maildir y se haga referencia al archivo /etc/dovecot/dovecot-dap.conf como un argumento para autenticarnos para la autenticación puesto que la validación de los usuarios también será mediante LDAP. Quedaría el siguiente archivo:

```
/etc/dovecot/dovecot.conf
protocols = imap
log_timestamp = "%Y-%m-%d %H:%M:%S "
first_valid_uid = 100
mail_debug = yes
mail_location = maildir:~/Maildir
disable_plaintext_auth = no
listen = *

auth default {
        mechanisms = plain

        socket listen {
                client{
                        path = /var/spool/postfix/private/auth-client
                        mode = 0660
                        user = postfix
                        group = postfix
                }
        }

        passdb ldap{
                args = /etc/dovecot/dovecot-ldap.conf
        }
        userdb ldap {
                args = /etc/dovecot/dovecot-dalp.conf
        }
}
```

También hay que configurar el archivo /etc/dovecot/dovecot-ldap.conf con los datos de nuestro servidor LDAP para podernos autenticar en él, de la siguiente forma.

```
hosts = 192.168.1.240
dn = cn=admin,dc=Audif,dc=local
dnpass = Passw0rd
tls = no
auth_bind = no
auth_bind_userdn = uid=%u,ou=Barcelona,ou=Usuarios,dc=Audif,dc=local
base = ou=Barcelona,ou=Usuarios,dc=Audif,dc=local
ldap_version = 3
scope = subtree
user_attrs = nomeDirectory=home,uidNombre=uid,gidNumber=gid
user_filter = (&(objectClass=posixAccount)(uid=%u))
pass_attrs = uid=user,userPassword=password
pass_filter = (&(objectClass=posixAccount)(uid=%u))
user_global_uid = 5000
user_global_gid = 5000
```

10.9.3. INSTALACIÓN Y CONFIGURACIÓN DE SQUIRRELMAIL

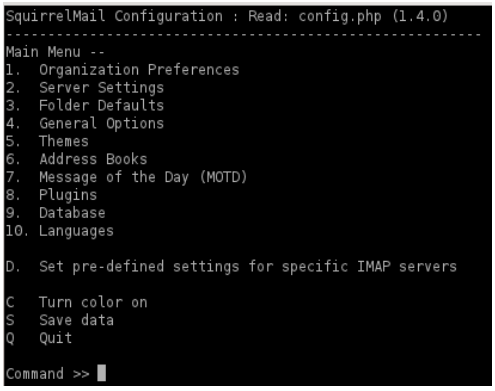
Para la instalación de *squirrelmail* se utiliza el siguiente comando.

```
jaime@BCNserver:~$ sudo apt-get install squirrelmail
```

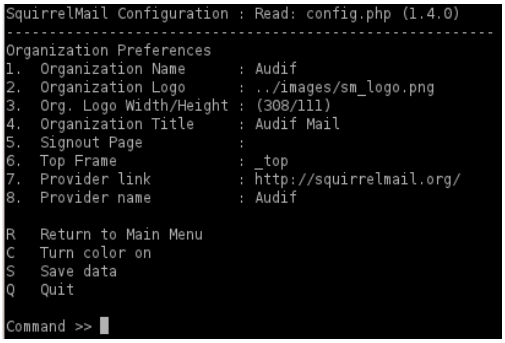
Una vez instalado hay que configurarlo, mediante el siguiente comando.

```
jaime@BCNserver:~$ sudo squirrelmail-configure
```

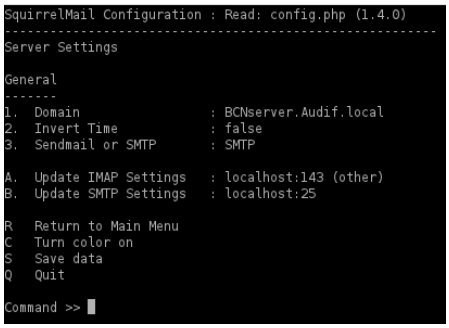
Sale el siguiente menú:



Seleccionamos la opción "1" y cambiamos el nombre de la organización y el titulo de la organización dejándolo como se ve en la siguiente pantalla.



Ahora volvemos al menú inicial y seleccionamos la opción "2" para insertar los datos del servidor de correo, hay que configurarlo de la siguiente forma.



Ya está instalado *squirrelmail* en el sistema pero para terminar de configurarlo y poder ejecutarlo hay que crear un enlace para ello nos situamos en el directorio */var/www* y creamos la ruta de enlace a */usr/share/squirrelmail* mediante los siguientes comandos.

```
jaime@BCNserver:~$ cd /var/www
jaime@BCNserver:/var/www$ sudo ln -s /usr/share/squirrelmail webmail
```

Con esta configuración ya está disponible el servidor de correo por completo.

10.9.4. INSTALACIÓN Y CONFIGURACIÓN DE ANTISPAM Y ANTIVIRUS

A continuación instalamos los paquetes *amavisd-new, spamassassin* y *clamav-deamon,* para ello utilizamos el siguiente comando.

```
jaime@BCNserver:~$ sudo apt-get install amavisd-new spamassassin clamav-daemon
```

Además instalamos el paquete opcional *pyzor razor* para mejorar la detección de spam mediante *spamassassin.* Utilizamos el siguiente comando.

```
jaime@BCNserver:~$ sudo apt-get install pyzor razor
```

10.9.4.1. CONFIGURACIÓN DE CLAMAV

La configuración por defecto de *ClamAv* encaja con nuestras necesidades, todos los días lanza un proceso para actualizar las firmas de detección de virus.

Pero hay que configurar *ClamAv* para que trabaje conjunto con nuestro filtro de correo, para ello hay que añadir el usuario clamav al grupo amavis con el siguiente comando.

```
jaime@BCNserver:~$ sudo adduser clamav amavis
[sudo] password for jaime:
Añadiendo al usuario `clamav' al grupo `amavis' ...
Añadiendo al usuario clamav al grupo amavis
Hecho.
```

10.9.4.2. CONFIGURACIÓN DE SPAMASSASSIN

Se edita el fichero */etc/default/spassmassin* para activarlo. Hay que cambiar el valor de *ENABLED* de 0 a 1 y el valor *CRON* de 0 a 1 para activar las actualizaciones automáticas.

```
# Change to one to enable spamd
ENABLED=1

# Options
# See man spamd for possible options. The -d option is automatically added.

# SpamAssassin uses a preforking model, so be careful! You need to
# make sure --max-children is not set to anything higher than 5,
# unless you know what you're doing.

OPTIONS="--create-prefs --max-children 5 --helper-home-dir"

# Pid file
# Where should spamd write its PID to file? If you use the -u or
# --username option above, this needs to be writable by that user.
# Otherwise, the init script will not be able to shut spamd down.
PIDFILE="/var/run/spamd.pid"

# Set nice level of spamd
#NICE="--nicelevel 15"

# Cronjob
# Set to anything but 0 to enable the cron job to automatically update
# spamassassin's rules on a nightly basis
CRON=1
```

Y se inicia el servicio.

```
jaime@BCNserver:~$ sudo /etc/init.d/spamassassin start
Starting SpamAssassin Mail Filter Daemon: spamd.
```

10.9.4.3. CONFIGURACIÓN DE AMAVISD-NEW

Lo primero que tenemos que hacer es activar la detección de spam y antivirus en *Amavis*, para ello hay que editar el archivo */etc/amavis/conf.d/15-content_filter_mode* quedando de la siguiente forma.

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Please note, that anti-virus checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:


@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);


#
# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:


@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;  # ensure a defined return
```

Y reiniciamos el servicio para que los cambios tengan efecto.

```
jaime@BCNserver:~$ sudo /etc/init.d/amavis restart
Stopping amavisd: amavisd-new.
Starting amavisd: amavisd-new.
```

10.9.4.4. INTEGRACIÓN EN POSTFIX

Para integrar en nuestro servidor *Postfix* el filtro del correo y antivirus que acabamos de instalar y configurar hay que ejecutar el siguiente comando:

```
jaime@BCNserver:~$ sudo postconf -e "content_filter = smtp-amuvis:[127.0.0.1]:10024"
```

Y editamos el archivo de configuración */etc/postfix/master.cf* al final del documento se añadirán las siguientes líneas.

```
smtp-amavis     unix    -       -       -       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes
        -o max_use=20

127.0.0.1:10025 inet    n       -       -       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

También hay que añadir debajo del servicio *"pickup"* las siguientes líneas.

```
pickup    fifo  n       -       -       60      1       pickup
        -o content_filter=
        -o receive_override_options=no_header_body_checks
```

Y se reinicia el servicio para que los cambios tengan efecto.

```
jaime@BCNserver:~$ sudo /etc/init.d/postfix restart
```

10.9.4.5. PRUEBAS DE CORREO ENTRE USUARIOS

Para acceder al correo hay que abrir una ventana del navegador de internet y poner la dirección *http://bcnserver/webmail* Y se mostrará la siguiente pantalla de autenticación de usuario.

Cada usuario pondrá su nombre de usuario y password y tendrá acceso a la plataforma para mandar correos electrónicos.

10.10. INSTALACIÓN DE SERVIDOR DE ARCHIVOS

Para que los equipos de la sede de Barcelona puedan acceder a archivos y carpetas del servidor se hace necesario instalar un sistema NFS (Network File System) en él. Para ello seguimos los siguientes pasos:

1. Instalación del paquete con el siguiente comando:
   ```
   jaime@BCNserver:~$ sudo apt-get install nfs-kernel-server
   ```
2. Editamos el archivo */etc/host.allow* para permitir acceso a los recursos compartidos a los equipos de nuestra red interna.
   ```
   portmap: 192.168.1.0/255.255.255.0
   nfs:     192.168.1.0/255.255.255.0
   ```
3. Y compartimos la carpeta que queremos, en este caso */home* modificando el archivo */etc/exports.*
   ```
   /home 192.168.1.0/255.255.255.0 (rw,sync,no_root_squash,no_subtree_check)
   ```
4. Reiniciamos los servicios de nfs y portmap.
   ```
   jaime@BCNserver:~$ sudo service portmap restart
   jaime@BCNserver:~$ sudo service nfs-kernel-server restart
   ```
5. Configuramos los servicios para que se arranquen automáticamente al arrancar el sistema operativo, mediante los siguientes comandos:

```
jaime@BCNserver:~$ sudo update-rc.d -f nfs-kernel-server defaults
 System start/stop links for /etc/init.d/nfs-kernel-server already exist.
jaime@BCNserver:~$ sudo update-rc.d -f portmap defaults
update-rc.d: warning: /etc/init.d/portmap missing LSB information
update-rc.d: see <http://wiki.debian.org/LSBInitScripts>
 Adding system startup for /etc/init.d/portmap ...
   /etc/rc0.d/K20portmap -> ../init.d/portmap
   /etc/rc1.d/K20portmap -> ../init.d/portmap
   /etc/rc6.d/K20portmap -> ../init.d/portmap
   /etc/rc2.d/S20portmap -> ../init.d/portmap
   /etc/rc3.d/S20portmap -> ../init.d/portmap
   /etc/rc4.d/S20portmap -> ../init.d/portmap
   /etc/rc5.d/S20portmap -> ../init.d/portmap
jaime@BCNserver:~$
```

10.10.1. CONFIGURACIÓN SAMBA CON SERVIDOR DE ARCHIVOS

Para realizar la configuración del servidor de archivos dentro de *Samba* hay que añadir al archivo de configuración (*/etc/Samba/smb.conf*) las siguientes líneas.

```
[share]
comment = Servidor de Archivos
path = /srv/Samba/share
browsable = yes
guest ok = yes
read only = yes
create mask = 0755
```

Se comparte la carpeta */usr/samba/share* se usará esta carpeta para todos los usuarios del dominio teniendo todos permisos de escritura y lectura sobre ella.

Para finalizar hay que reiniciar Samba con los siguientes comandos.

```
jaime@BCNserver:~$ sudo restart smbd
smbd start/running, process 3123
jaime@BCNserver:~$ sudo restart nmbd
nmbd start/running, process 3132
```

11. INSTALACIÓN DEL SERVIDOR PROXY BARCELONA

En el servidor llamado *BCNproxy* se instala y configura el proxy, firewall y VPN, como se puede ver en la figura del esquema de la situación final del punto 6.2 del presente documento.

11.1. INMPLEMENTACIÓN DE SQUID (PROXY)

Para instalar *Squid* utilizamos el siguiente comando.

```
jaime@BCNproxy:~$ sudo apt-get install squid
```

Una vez instalado hay que configurarlo, para ello editamos el archivo */etc/squid/squid.conf* añadiendo las siguientes líneas:

```
http_port 8888
visible_hostname proxy
acl redlocal src 192.168.1.0/24
acl biz_redlocal src 192.168.1.0/24
acl biz_horas time M T W T F 8:00-18:00
http_access allow biz_redlocal biz_horas
cache_mem 16 MB
```

Con estas modificaciones lo que se consigue es:

- Cambiar el puerto de escucha al 8888
- El servidor se denomina "proxy"
- Se crea un acl para todos los equipos de la red local
- Se restringe el acceso a internet en horario laboral (de 8:00 a 18:00)
- Se aumenta la memoria caché a 16 MB

Una vez configurado se reinicia el servicio.

```
jaime@BCNproxy:~$ sudo /etc/init.d/squid restart
```

11.2. BLOQUEO DE SITIOS WEB

A continuación vamos a configurar el servidor proxy para que aún fuera de horario laboral no se tengan acceso a algunas páginas web o que contengan algún contenido específico, para ello procedemos de la siguiente manera.

1. Crear archivo */etc/squid/sitiosdenegados*
2. Editar el archivo creado con las páginas web no permitidas. Tendrá el siguiente formato el archivo:

3. Se añaden las siguientes líneas al archivo */etc/squid/squid.conf*

```
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
http_access deny all sitiosdenegados
```

4. Se reinicia el servicio para que tengan efecto los cambios.

```
jaime@BCNproxy:~$ sudo /etc/init.d/squid restart
```

11.3. INSTALACIÓN DEL SERVIDOR FIREWALL

La herramienta de configuración predeterminada de Ubuntu es *UWF*. Desarrollado para facilitar la configuración del firewall Iptables, ufw proporciona una manera fácil de crear un firewall basado en host IPv4 o IPv6.

UFW por defecto está deshabilitado inicialmente, lo activamos con el siguiente comando.

```
jaime@BCNproxy:~$ sudo ufw enable
```

Inicialmente denegamos todas las conexiones.

```
jaime@BCNproxy :~$ sudo ufw default deny
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
```

Permitimos la comunicación entre nuestra red local, tanto la de Barcelona como la de Madrid.

```
jaime@BCNproxy :~$ sudo ufw allow from 192.168.1.0/24
Regla añadida
jaime@BCNproxy :~$ sudo ufw allow from 192.168.2.0/24
Regla añadida
```

Ahora vamos a dar permisos a los equipos de nuestra red para que puedan acceder a internet. Para ello lo primero que hay que hacer es modificar el archivo */etc/default/ufw* y modificar

```
DEFAULT_FORWARD_POLICY a “ACCEPT”
```

Seguidamente modificamos el archivo */etc/ufw/sysctl.conf* y descomentamos las siguientes líneas.

```
net/ipv4/ip_forward=1
net/ipv6/conf/default/forwarding=1
```

La última modificación hay que hacerla en el archivo */etc/ufw/before.rules* donde hay que insertar la siguiente regla.

```
# nat Table rules // reglas de la tabla NAT
*nat
:POSTROUTING ACCEPT [0:0]

# . Forward traffic from eth1 through eth0.
-A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

# don't delete the 'COMMIT' line or these nat table rules won't be processed
COMMIT
```

Finalmente deshabilitamos y habilitamos el firewall para que los cambios tengan efecto.

```
jaime@BCNproxy :~$ sudo ufw disable
El cortafuegos está detenido y no será activado durante la carga del sistema
jaime@BCNproxy :~$ sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
```

12. INSTALACIÓN SERVIDOR MADRID.

12.1. INSTALACIÓN DISTRIBUCIÓN LINUX

La distribución de Linux del servidor de Madrid es la misma que la del servidor de Barcelona por lo que me remito a el punto 9.1 del presente documento donde se explica cómo instalar paso a paso la distribución elegida.

La única diferencia es en el paso número ocho del proceso de instalación que especificamos como nombre del servidor MADserver.

12.2. INSTALACIÓN DE SERVICIOS LDAP

Al igual que en el punto anterior, la instalación y primera configuración del servicio LDAP en el servidor de Madrid es igual que en el servidor de Barcelona. Por lo que nos remitiremos al punto 9.2 del presente documento para llevarlo a cabo.

La configuración al ser exactamente igual se puede, en vez de ir editando los archivos que hay que modificar, copiar del servidor estos del servidor de Barcelona y pegar en este. Una vez hecho se reinician los demonios ldap y quedaría configurado exactamente igual.

12.3. INSTALACIÓN Y CONFIGURACION SAMBA

El proceso de instalación de *Samba* en el servidor de Madrid se lleva a cabo de la misma forma que en el servidor de Barcelona, recogido en el punto 9.3 del presente documento.

12.4. CONFIGURACIÓN PARA AUTENTICACIÓN DE USUARIOS

La configuración del servidor de Madrid para permitir la autenticación de usuarios, se lleva a cabo de la misma forma que en el servidor de Barcelona en el punto 9.4 del presente documento.

Excepto en la primera pantalla donde pide la dirección del servidor LDAP que hay que rellenar con la dirección IP del servidor de Madrid (192.168.2.240, como se muestra en la siguiente pantalla.

12.5. INSTALACIÓN DE COLA DE IMPRESIÓN

De la misma forma que en el servidor de Barcelona instalamos la cola de impresión.

1. *sudo apt-get install cups*
2. Para compartir impresoras se añaden al archivo */etc/Samba/smb.conf* lo siguiente:

```
[print$]
Coment = Print Drivers
Path = /var/lib/Samba/printers
browsable = yes
read only = yes
guest ok = yes
[printers]
Comment = Printer
browsable = yes
path = /var/spool/Samba
printable = yes
guest ok = yes
read only = no
create mask = 0755
```

12.5.1. INSTALACIÓN DE IMPRESORA PDF

En la oficina de Madrid también se instalará una impresora de red, y una impresora pdf para poder imprimir documentos en este formato.

Para ello ejecutamos el siguiente comando.

```
sudo apt-get install cups-pdf
```

Para que la impresora sea vista por todos los usuarios hay que cambiar los permisos mediante el siguiente comando.

```
sudo chmod u+s /usr/lib/cups/backend/cups-pdf
```

Ya tenemos la impresora compartida y con los permisos necesarios para poder instalarla en los equipos clientes.

12.6. INSTALACIÓN DE CONTROL DE VERSIONES

La instalación del control de versiones en el servidor de Madrid se instala y se configura exactamente igual que en el servidor de Barcelona por lo que me remito al punto 9.6 para llevarlo a cabo, con el fin de no duplicar la información.

12.7. INSTALACIÓN DE GESTIÓN DE DOCUMENTACIÓN

La instalación de la gestión de documentación en el servidor de Madrid se instala y se configura exactamente igual que en el servidor de Barcelona por lo que me remito al punto 9.7 para llevarlo a cabo, con el fin de no duplicar la información.

12.8. INSTALACIÓN SERVIDOR DE CORREO

La instalación y posterior configuración del servidor de correo, y el software asociado para su correcto funcionamiento es muy similar a la instalación y configuración en el servidor de Barcelona, pero alguno de los archivos de configuración cambian.

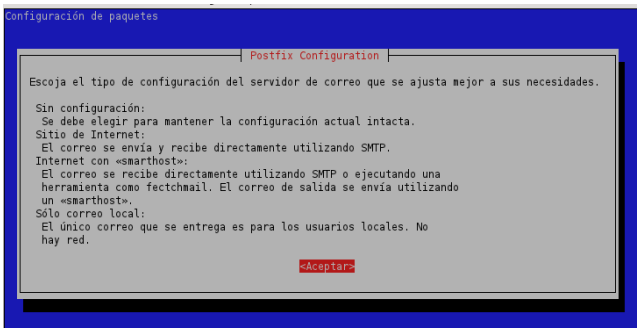
Por lo que a continuación detallo paso a paso la instalación en el servidor de Madrid cómo instalar y configurar el servidor de correo.

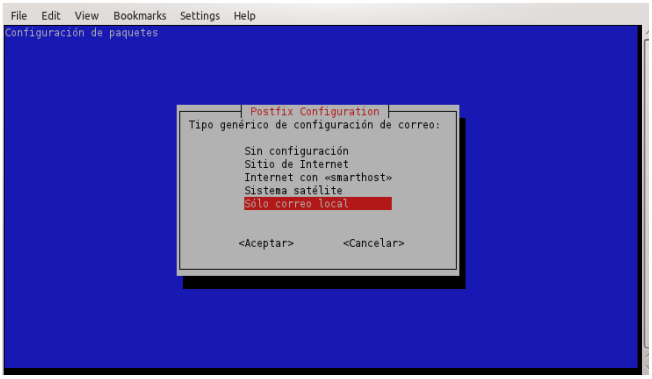
12.8.1. INSTALACIÓN DE SERVIDOR SMTP POSTFIX

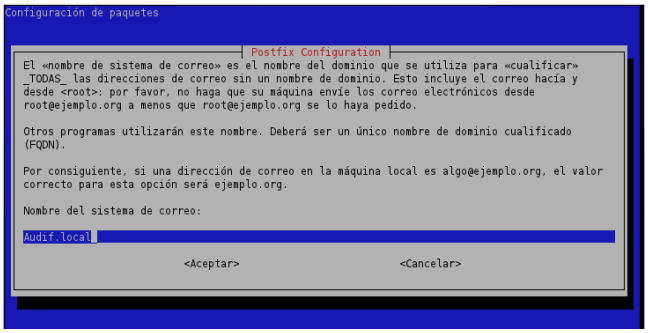
Se instala Postfix con el siguiente comando.

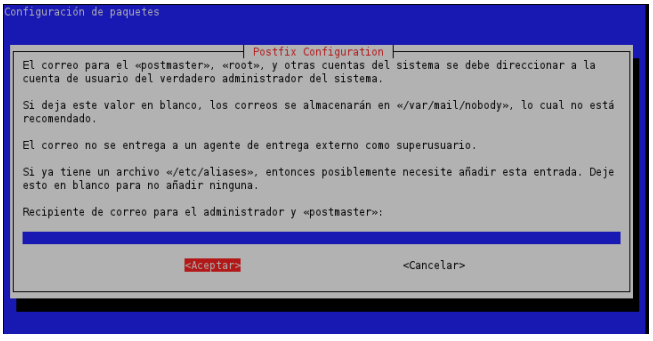
```
jaime@MADserver:~$ sudo apt-get install postfix
```

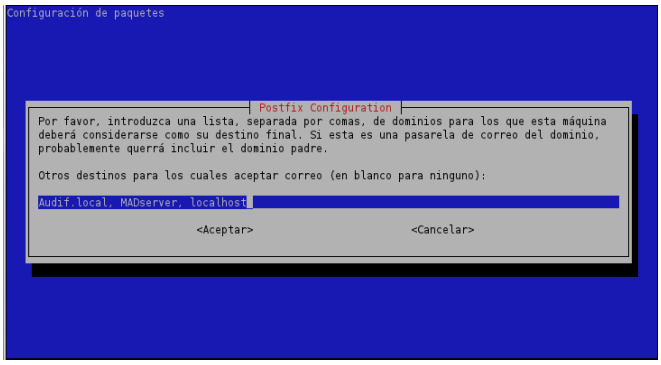
Después se lanzará el asistente de configuración (si no se lanzará hay que forzar el lanzamiento mediante el comando *"sudo dpkg-reconfigure postfix"*) Se contestará de la siguiente forma a las preguntas de configuración.

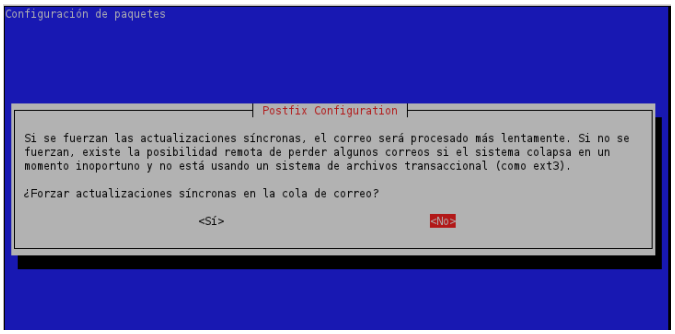


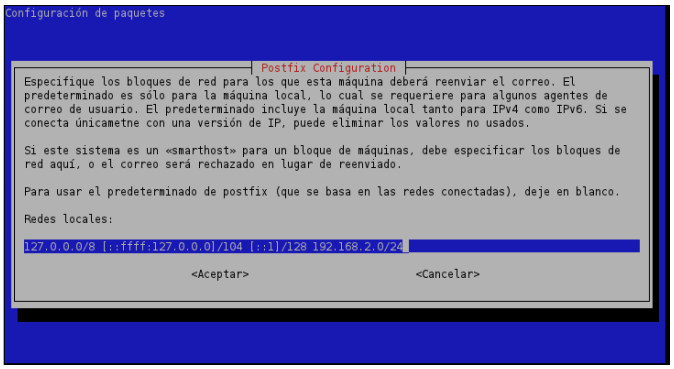


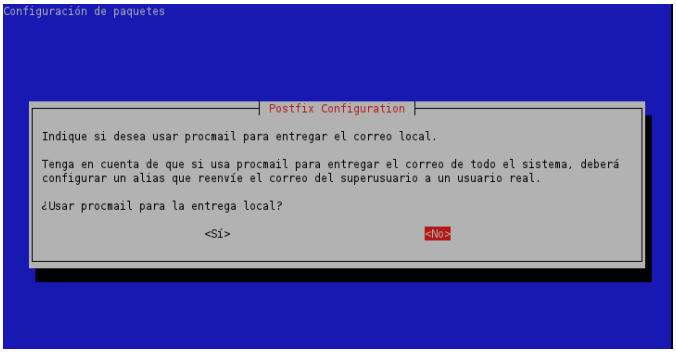


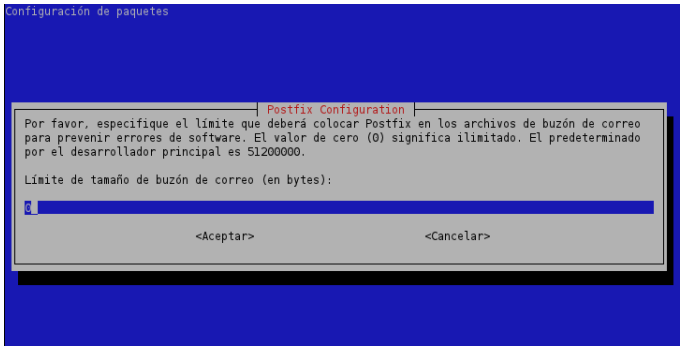


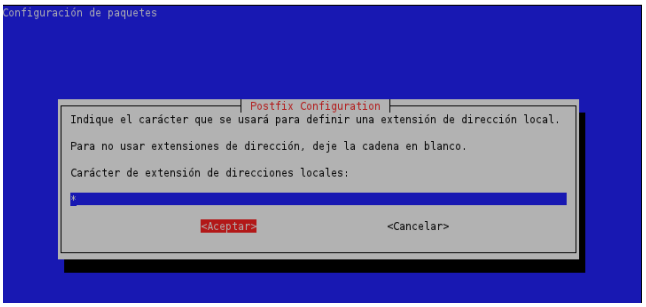

Configuración de paquetes
Postfix Configuration
Por favor, introduzca una lista, separada por comas, de dominios para los que esta máquina deberá considerarse como su destino final. Si esta es una pasarela de correo del dominio, probablemente querrá incluir el dominio padre.
Otros destinos para los cuales aceptar correo (en blanco para ninguno):
Audif.local, MADserver, localhost
<Aceptar>
<Cancelar>

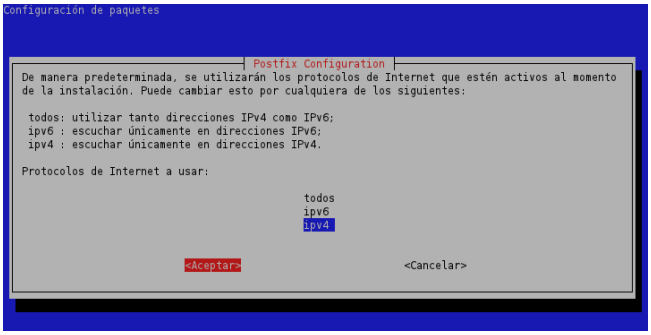

Configuración de paquetes
Postfix Configuration
Si se fuerzan las actualizaciones síncronas, el correo será procesado más lentamente. Si no se fuerzan, existe la posibilidad remota de perder algunos correos si el sistema colapsa en un momento inoportuno y no está usando un sistema de archivos transaccional (como ext3).
¿Forzar actualizaciones síncronas en la cola de correo?
<Sí>
<No>


Configuración de paquetes
Postfix Configuration
Especifique los bloques de red para los que esta máquina deberá reenviar el correo. El predeterminado es sólo para la máquina local, lo cual se requeriere para algunos agentes de correo de usuario. El predeterminado incluye la máquina local tanto para IPv4 como IPv6. Si se conecta únicametne con una versión de IP, puede eliminar los valores no usados.
Si este sistema es un «smarthost» para un bloque de máquinas, debe especificar los bloques de red aquí, o el correo será rechazado en lugar de reenviado.
Para usar el predeterminado de postfix (que se basa en las redes conectadas), deje en blanco.
Redes locales:
127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.2.0/24
<Aceptar>
<Cancelar>


Configuración de paquetes
Postfix Configuration
Indique si desea usar procmail para entregar el correo local.
Tenga en cuenta de que si usa procmail para entregar el correo de todo el sistema, deberá configurar un alias que reenvíe el correo del superusuario a un usuario real.
¿Usar procmail para la entrega local?
<Sí>
<No>


Configuración de paquetes
Postfix Configuration
Por favor, especifique el límite que deberá colocar Postfix en los archivos de buzón de correo para prevenir errores de software. El valor de cero (0) significa ilimitado. El predeterminado por el desarrollador principal es 51200000.
Límite de tamaño de buzón de correo (en bytes):
0
<Aceptar>
<Cancelar>





Ya tenemos configurado el servidor SMTP Potsfix.

El siguiente paso es configurar el formato de los buzones de correo, para ello decidimos que fuera MailDir, se hace con el siguiente comando.

```
jaime@MADserver:~$ sudo postconf -e 'home_mailbox=Maildir/'
```

12.8.2. INSTALACIÓN Y CONFIGURACIÓN DE DOVECOT (IMAP, POP3)

El siguiente comando es el que se utiliza para la instalación de *dovecot.*

```
jaime@MADserver:~$ sudo apt-get install dovecot-imapd dovecot-pop3d
```

Hay que configurar el archivo */etc/dovecot/dovecot.conf.* Se configurará para usar el protocolo *IMAP*, buzones de tipo *Maildir* y se haga referencia al archivo */etc/dovecot/dovecot-dap.conf* como un argumento para autenticarnos para la autenticación puesto que la validación de los usuarios también será mediante *LDAP*. Quedaría el siguiente archivo:

```
/etc/dovecot/dovecot.conf
protocols = imap
log_timestamp = "%Y-%m-%d %H:%M:%S "
first_valid_uid = 100
mail_debug = yes
mail_location = maildir:~/Maildir
disable_plaintext_auth = no
listen = *

auth default {
        mechanisms = plain

        socket listen {
                client{
                        path = /var/spool/postfix/private/auth-client
                        mode = 0660
                        user = postfix
                        group = postfix
                }
        }

        passdb ldap{
                args = /etc/dovecot/dovecot-ldap.conf
        }
        userdb ldap {
                args = /etc/dovecot/dovecot-dalp.conf
        }
}
```

También hay que configurar el archivo */etc/dovecot/dovecot-ldap.conf* con los datos de nuestro servidor *LDAP* para podernos autenticar en él, de la siguiente forma.

```
hosts = 192.168.2.240
dn = cn=admin,dc=Audif,dc=local
dnpass = Passw0rd
tls = no
auth_bind = no
auth_bind_userdn = uid=%u,ou=Madrid,ou=Usuarios,dc=Audif,dc=local
base = ou=Madrid,ou=Usuarios,dc=Audif,dc=local
ldap_version = 3
scope = subtree
user_attrs = homeDirectory=home,uidNombre=uid,gidNumber=gid
user_filter = (&(objectClass=posixAccount)(uid=%u))
pass_attrs = uid=user,userPassword=password
pass_filter = (&(objectClass=posixAccount)(uid=%u))
user_global_uid = 5000
user_global_gid = 5000
```

12.8.3. INSTALACIÓN Y CONFIGURACIÓN DE SQUIRRELMAIL

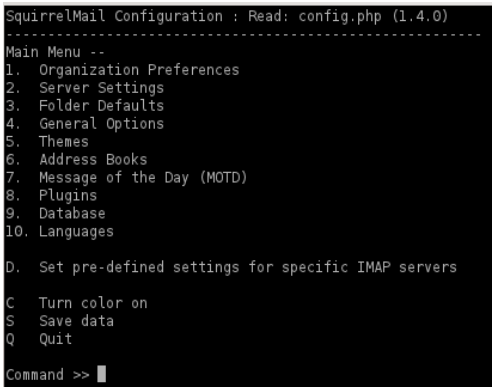
Para la instalación de *squirrelmail* se utiliza el siguiente comando.

```
jaime@MADserver:~$ sudo apt-get install squirrelmail
```

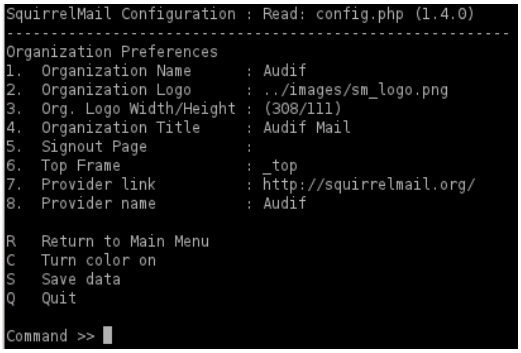
Una vez instalado hay que configurarlo, mediante el siguiente comando.

```
jaime@MADserver:~$ sudo squirrelmail-configure
```

Sale el siguiente menú:



Seleccionamos la opción "1" y cambiamos el nombre de la organización y el titulo de la organización dejándolo como se ve en la siguiente pantalla.



Ahora volvemos al menú inicial y seleccionamos la opción "2" para insertar los datos del servidor de correo, hay que configurarlo de la siguiente forma.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Server Settings

General
-------
1.  Domain                 : MADserver.Audif.local
2.  Invert Time            : false
3.  Sendmail or SMTP       : SMTP

A.  Update IMAP Settings   : localhost:143 (dovecot)
B.  Update SMTP Settings   : localhost:25

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit
```

Ya está instalado *squirrelmail* en el sistema pero para terminar de configurarlo y poder ejecutarlo hay que crear un enlace para ello nos situamos en el directorio */var/www* y creamos la ruta de enlace a */usr/share/squirrelmail* mediante los siguientes comandos.

```
jaime@MADserver:~$ cd /var/www
jaime@MADserver:/var/www$ sudo ln -s /usr/share/squirrelmail webmail
```

Con esta configuración ya está disponible el servidor de correo por completo.

12.8.4. INSTALACIÓN Y CONFIGURACIÓN DE ANTISPAM Y ANTIVIRUS

A continuación instalamos los paquetes *amavisd-new, spamassassin* y *clamav-deamon,* para ello utilizamos el siguiente comando.

```
jaime@MADserver:~$ sudo apt-get install amavisd-new spamassassin clamav-daemon
```

Además instalamos el paquete opcional *pyzor razor* para mejorar la detección de spam mediante *spamassassin.* Utilizamos el siguiente comando.

```
jaime@MADserver:~$ sudo apt-get install pyzor razor
```

12.8.4.1. CONFIGURACIÓN DE CLAMAV

La configuración por defecto de *ClamAv* encaja con nuestras necesidades, todos los días lanza un proceso para actualizar las firmas de detección de virus.

Pero hay que configurar *ClamAv* para que trabaje conjunto con nuestro filtro de correo, para ello hay que añadir el usuario clamav al grupo amavis con el siguiente comando.

```
jaime@MADserver: sudo adduser clamav amavis
[sudo] password for jaime:
Añadiendo al usuario `clamav' al grupo `amavis' ...
Añadiendo al usuario clamav al grupo amavis
Hecho.
```

12.8.4.2. CONFIGURACIÓN DE SPAMASSASSIN

Se edita el fichero */etc/default/spassmassin* para activarlo. Hay que cambiar el valor de *ENABLED* de 0 a 1 y el valor *CRON* de 0 a 1 para activar las actualizaciones automáticas.

```
# Change to one to enable spamd
ENABLED=1

# Options
# See man spamd for possible options. The -d option is automatically added.

# SpamAssassin uses a preforking model, so be careful! You need to
# make sure --max-children is not set to anything higher than 5,
# unless you know what you're doing.

OPTIONS="--create-prefs --max-children 5 --helper-home-dir"

# Pid file
# Where should spamd write its PID to file? If you use the -u or
# --username option above, this needs to be writable by that user.
# Otherwise, the init script will not be able to shut spamd down.
PIDFILE="/var/run/spamd.pid"

# Set nice level of spamd
#NICE="--nicelevel 15"

# Cronjob
# Set to anything but 0 to enable the cron job to automatically update
# spamassassin's rules on a nightly basis
CRON=1
```

Y se inicia el servicio.

```
jaime@MADserver:~$ sudo /etc/init.d/spamassassin start
Starting SpamAssassin Mail Filter Daemon: spamd.
```

12.8.4.3. CONFIGURACIÓN DE AMAVISD-NEW

Lo primero que tenemos que hacer es activar la detección de *spam* y antivirus en *Amavis*, para ello hay que editar el archivo */etc/amavis/conf.d/15-content_filter_mode* quedando de la siguiente forma.

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Please note, that anti-virus checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:


@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);


#
# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:


@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;  # ensure a defined return
```

Y reiniciamos el servicio para que los cambios tengan efecto.

```
jaime@MADserver:~$ sudo /etc/init.d/amavis restart
Stopping amavisd: amavisd-new.
Starting amavisd: amavisd-new.
```

12.8.4.4. INTEGRACIÓN EN POSTFIX

Para integrar en nuestro servidor *Postfix* el filtro del correo y antivirus que acabamos de instalar y configurar hay que ejecutar el siguiente comando:

```
jaime@MADserver:~$ sudo postconf -e "content_filter = smtp-amuvis:[127.0.0.1]:10024"
```

Y editamos el archivo de configuración */etc/postfix/master.cf* al final del documento se añadirán las siguientes líneas.

```
smtp-amavis     unix    -       -       -       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes
        -o max_use=20

127.0.0.1:10025 inet    n       -       -       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

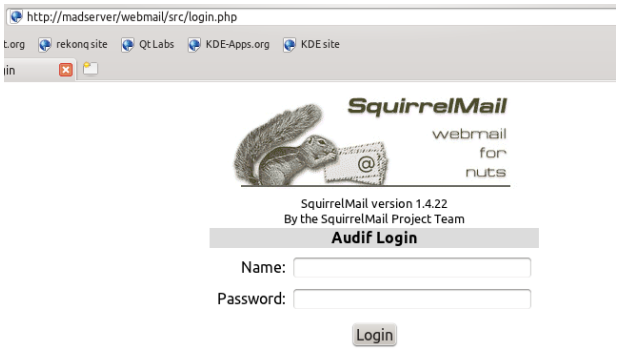
También hay que añadir debajo del servicio *"pickup"* las siguientes líneas.

```
pickup    fifo  n       -       -       60      1       pickup
          -o content_filter=
          -o receive_override_options=no_header_body_checks
```

Y se reinicia el servicio para que los cambios tengan efecto.

12.8.4.5. PRUEBAS DE ACCESO A CORREO

Para acceder al correo hay que abrir una ventana del navegador de internet y poner la dirección *http://madserver/webmail* Y se mostrará la siguiente pantalla de autenticación de usuario.



Cada usuario pondrá su nombre de usuario y password y tendrá acceso a la plataforma para mandar correos electrónicos.

12.9. INSTALACIÓN DE SERVIDOR DE ARCHIVOS

Para que los equipos de la sede de Madrid puedan acceder a archivos y carpetas del servidor se hace necesario instalar un sistema *NFS (Network File System)* en él. Para ello seguimos los siguientes pasos:

5. Instalación del paquete con el siguiente comando:

```
jaime@MADserver:~$ sudo apt-get install nfs-kernel-server
```

6. Editamos el archivo /etc/*host.allow* para permitir acceso a los recursos compartidos a los equipos de nuestra red interna.

```
portmap: 192.168.2.0/255.255.255.0
nfs:     192.168.2.0/255.255.255.0
```

7. Y compartimos la carpeta que queremos, en este caso */home* modificando el archivo */etc/exports.*

```
/home 192.168.2.0/255.255.255.0 (rw,sync,no_root_squash,no_subtree_check)
```

8. Reiniciamos los servicios de *nfs* y *portmap*.

```
jaime@MADserver:~$ sudo service portmap restart
jaime@MADserver:~$ sudo service nfs-kernel-server restart
```

9. Configuramos los servicios para que se arranquen automáticamente al arrancar el sistema operativo, mediante los siguientes comandos:

```
jaime@MADserver:~$ sudo update-rc.d -f nfs-kernel-server defaults
 System start/stop links for /etc/init.d/nfs-kernel-server already exist.
jaime@MADserver:~$ sudo update-rc.d -f portmap defaults
update-rc.d: warning: /etc/init.d/portmap missing LSB information
update-rc.d: see <http://wiki.debian.org/LSBInitScripts>
 Adding system startup for /etc/init.d/portmap ...
   /etc/rc0.d/K20portmap -> ../init.d/portmap
   /etc/rc1.d/K20portmap -> ../init.d/portmap
   /etc/rc6.d/K20portmap -> ../init.d/portmap
   /etc/rc2.d/S20portmap -> ../init.d/portmap
   /etc/rc3.d/S20portmap -> ../init.d/portmap
   /etc/rc4.d/S20portmap -> ../init.d/portmap
   /etc/rc5.d/S20portmap -> ../init.d/portmap
jaime@MADserver:~$
```

12.9.1. CONFIGURACIÓN SAMBA CON SERVIDOR DE ARCHIVOS

Para realizar la configuración del servidor de archivos dentro de *Samba* hay que añadir al archivo de configuración (*/etc/Samba/smb.conf*) las siguientes líneas.

```
[share]
comment = Servidor de Archivos
path = /srv/Samba/share
browsable = yes
guest ok = yes
read only = yes
create mask = 0755
```

Se comparte la carpeta */usr/samba/share* se usará esta carpeta para todos los usuarios del dominio teniendo todos permisos de escritura y lectura sobre ella.

Para finalizar hay que reiniciar Samba con los siguientes comandos.

```
jaime@MADserver:~$ sudo restart smbd
smbd start/running, process 4813
jaime@MADserver:~$ sudo restart nmbd
nmbd start/running, process 4821
```

13. INSTALACIÓN DEL SERVIDOR PROXY MADRID

En el servidor llamado MADproxy se instala y configura el proxy, firewall y VPN, como se puede ver en la figura del esquema de la situación final del punto 6.2 del presente documento.

13.1. INMPLEMENTACIÓN DE SQUID (PROXY)

Para instalar *Squid* utilizamos el siguiente comando.

```
jaime@MADproxy:~$ sudo apt-get install squid
```

Una vez instalado hay que configurarlo, para ello editamos el archivo */etc/squid/squid.conf* añadiendo las siguientes líneas:

```
http_port 8888
visible_hostname proxy
acl redlocal src 192.168.2.0/24
acl biz_redlocal src 192.168.2.0/24
acl biz_horas time M T W T F 8:00-18:00
http_access allow biz_redlocal biz_horas
cache_mem 16 MB
```

Con estas modificaciones lo que se consigue es:

- Cambiar el puerto de escucha al 8888
- El servidor se denomina "proxy"
- Se crea un acl para todos los equipos de la red local
- Se restringe el acceso a internet en horario laboral (de 8:00 a 18:00)
- Se aumenta la memoria caché a 16 MB

Una vez configurado se reinicia el servicio.

```
jaime@MADproxy:~$ sudo /etc/init.d/squid restart
```

13.2. BLOQUEO DE SITIOS WEB

A continuación vamos a configurar el servidor proxy para que aún fuera de horario laboral no se tengan acceso a algunas páginas web o que contengan algún contenido específico, para ello procedemos de la siguiente manera.

10. Crear archivo */etc/squid/sitiosdenegados*
11. Editar el archivo creado con las páginas web no permitidas. Tendrá el siguiente formato el archivo:

12. Se añaden las siguientes líneas al archivo */etc/squid/squid.conf*

```
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
http_access deny all sitiosdenegados
```

13. Se reinicia el servicio para que tengan efecto los cambios.

```
jaime@MADproxy:~$ sudo /etc/init.d/squid restart
```

13.3. INSTALACIÓN DEL SERVIDOR FIREWALL

La herramienta de configuración predeterminada de Ubuntu es *UWF*. Desarrollado para facilitar la configuración del firewall Iptables, ufw proporciona una manera fácil de crear un firewall basado en host IPv4 o IPv6.

UFW por defecto está deshabilitado inicialmente, lo activamos con el siguiente comando.

```
jaime@MADproxy:~$ sudo ufw enable
```

Inicialmente denegamos todas las conexiones.

```
jaime@MADproxy:~$ sudo ufw default deny
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
```

Permitimos la comunicación entre nuestra red local, tanto la de Barcelona como la de Madrid.

```
jaime@MADproxy:$ sudo ufw allow from 192.168.1.0/24
Regla añadida
jaime@MADproxy:$ sudo ufw allow from 192.168.2.0/24
Regla añadida
```

Ahora vamos a dar permisos a los equipos de nuestra red para que puedan acceder a internet. Para ello lo primero que hay que hacer es modificar el archivo */etc/default/ufw* y modificar

```
DEFAULT_FORWARD_POLICY a “ACCEPT”
```

Seguidamente modificamos el archivo */etc/ufw/sysctl.conf* y descomentamos las siguientes líneas.

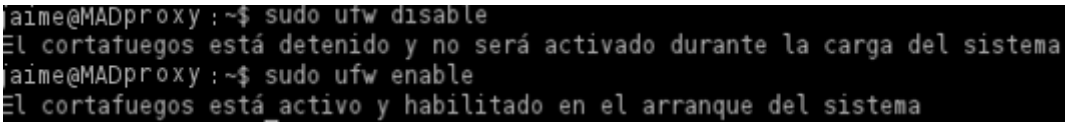
```
net/ipv4/ip_forward=1
net/ipv6/conf/default/forwarding=1
```

La última modificación hay que hacerla en el archivo */etc/ufw/before.rules* donde hay que insertar la siguiente regla.

```
# nat Table rules // reglas de la tabla NAT
```

```
*nat
:POSTROUTING ACCEPT [0:0]

# . Forward traffic from eth1 through eth0.
-A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQUERADE

# don't delete the 'COMMIT' line or these nat table rules won't be processed
COMMIT
```

Finalmente deshabilitamos y habilitamos el firewall para que los cambios tengan efecto.



14. CONFIGURACIÓN DE REPLICACIÓN LDAP

Al tener dos servidores controladores LDAP, estos deben de estar sincronizados entre ellos, y así se evitarán errores y duplicidades de trabajo.

Dada la versión LDAP instalada en los servidores podemos utilizar para la realización de la réplica *Syncrepl*. Existen varias formas de réplica, la elegida es *MirrorMode,* de esta forma se pueden hacer cambios en cualquiera de los dos servidores, replicándose en todo momento los cambios entre ellos para tener la misma estructura en los dos en todo momento.

14.1. CONFIGURACIÓN SERVIDOR BARCELONA.

Para llevar a cabo la sincronización entre los dos servidores hay que configurar el archivo */usr/share/slapd/slapd.conf* añadiendo las siguientes líneas.

```
ServerID        1

overlay         syncprov

Syncrpl         rid=2
                provider=ldap://MADserver.audif.local:389
                bindmethod=simple
                binddn="cn=admin,dc=audif,dc=local"
                credentials=Passw0rd
                searchbase="dc=audif,dc=local"
                type=refreshAndPersist
                retry="5 + 5 +"
                interval=00:00:00:05

mirrormode      true
```

Seguidamente reiniciamos el servidor *LDAP* mediante el comando

```
:~$ sudo /etc/init.d/slapd restart
```

14.2. CONFIGURACIÓN SERVIDOR MADRID.

Para terminar la configuración de la sincronización también hay que configurar en el servidor de Madrid el archivo */usr/share/slapd/slapd.conf* añadiendo las siguientes líneas.

```
ServerID        2

overlay         syncprov

Syncrpl         rid=1
                provider=ldap://BCNserver.audif.local:389
                bindmethod=simple
                binddn="cn=admin,dc=audif,dc=local"
                credentials=Passw0rd
                searchbase="dc=audif,dc=local"
                type=refreshAndPersist
                retry="5 + 5 +"
                interval=00:00:00:05

mirrormode      true
```

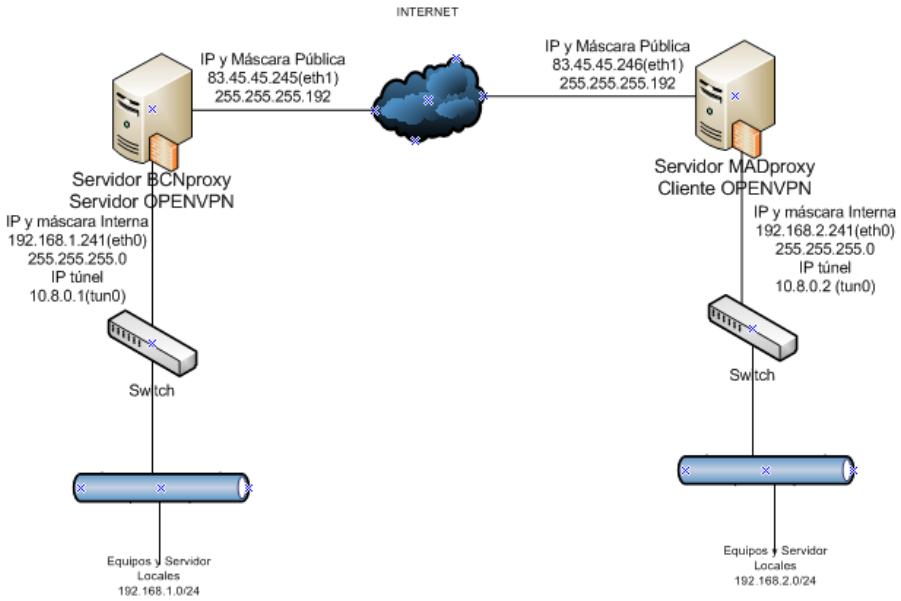
Seguidamente reiniciamos el servidor *LDAP* mediante el comando

```
:~$ sudo /etc/init.d/slapd restart
```

15. INSTALACIÓN VPN PUNTO A PUNTO

La instalación de la VPN se llevará a cabo en los dos servidores llamados *BCNproxy* y *MADproxy* situados en la sede de Barcelona y Madrid respectivamente, por lo tanto será una configuración de *VPN Site to Site (Punto a Punto).*

La estructura básica de la VPN entre las dos sedes se recoge en el siguiente esquema.



15.1. INSTALACIÓN VPN BARCELONA

1. Instalar *openVPN* en el servidor mediante el comando siguiente.

```
jaime@BCNproxy:~$ sudo apt-get install openvpn
```

2. Se crea, carga y habilita el routing en el dispositivo TUN/TAP integrado en el Kernel de Linux.

```
sudo mknod /dev/net/tun c 10 200
```

3. Se añade al fichero /etc/modules.conf la siguiente línea

```
alias char-major-10-200 tu
```

4. Se carga el driver TUN/TAP

```
sudo modprobe tun
```

5. Se habilita el routing en el driver TUN/TAP

```
jaime@BCNproxy:~$ sudo -s
jaime@BCNproxy:# echo 1 > /proc/sys/net/ipv4/ip_forward
jaime@BCNproxy:# exit
exit
```

6. Ahora hay que incluir una nueva entrada en la tabla de rutas del servidor OPENVPN para que se pueda comunicar con el cliente de openVPN de Madrid, mediante el siguiente comando.

```
jaime@BCNproxy:~$ sudo route add -net 192.168.2.0 netmask 255.255.255.0 gw 10.8.0.2
```

7. Copiamos el contenido de la carpeta /usr/share/doc/openvpn/examples/easy-rsa/2.0 a /etc/openvpn/easy-rsa, para cerciorarnos de que con cualquier actualización del paquete no se perderán las secuencias de órdenes.

8. Damos permisos al usuario actual en el directorio para que pueda crear archivos.

```
jaime@BCNproxy:~$ sudo chown -R $USER /etc/openvpn/easy-rsa/
```

9. Cambiamos el fichero /etc/openvpn/easy-rsa/vars con los datos de nuestra empresa.

```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="SP"
export KEY_PROVINCE="BCN"
export KEY_CITY="Barcelona"
export KEY_ORG="Audifon"
export KEY_EMAIL="adminbcn@audif.local"
```

10. Creamos la clave/certificado de la CA mediante los siguientes comandos. Mediante este procedimiento hemos generado 2 ficheros nuevos:

- *ca.crt:* fichero correspondiente al certificado público de la CA.
- *ca.key:* fichero correspondiente a la clave privada de la CA, la cual debe mantenerse protegida ya que es la clave más importante de toda la PKI

```
jaime@BCNproxy:~$ cd /etc/openvpn/easy-rsa/
jaime@BCNproxy:/etc/openvpn/easy-rsa$ source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
jaime@BCNproxy:/etc/openvpn/easy-rsa$ ./clean-all
jaime@BCNproxy:/etc/openvpn/easy-rsa$ ./build-ca
Generating a 1024 bit RSA private key
.....++++++
.............++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SP]:
State or Province Name (full name) [BCN]:
Locality Name (eg, city) [Barcelona]:
Organization Name (eg, company) [Audifon]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [Audifon CA]:Audifon_CA
Name []:
Email Address [adminbcn@audif.local]:
jaime@BCNproxy:/etc/openvpn/easy-rsa$
```

El fichero ca.key se puede guardar en algún dispositivo seguro que no tenga conexión (por seguridad) pero el fichero ca.crt tenemos que tenerlo tanto en el Cliente OpenVPN como en el Servidor OpenVPN.

11. Creamos la clave/certificado del servidor mediante los siguientes comandos.

```
jaime@BCNproxy:/etc/openvpn/easy-rsa$ ./build-key-server servidor
Generating a 1024 bit RSA private key
.......++++++
............++++++
writing new private key to 'servidor.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SP]:
State or Province Name (full name) [BCN]:
Locality Name (eg, city) [Barcelona]:
Organization Name (eg, company) [Audifon]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [servidor]:
Name []:
Email Address [adminbcn@audif.local]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'SP'
stateOrProvinceName   :PRINTABLE:'BCN'
localityName          :PRINTABLE:'Barcelona'
organizationName      :PRINTABLE:'Audifon'
commonName            :PRINTABLE:'servidor'
emailAddress          :IA5STRING:'adminbcn@audif.local'
Certificate is to be certified until Jan  3 16:38:37 2022 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Tras realizar estos pasos hemos generado 4 ficheros nuevos:

- *servidor.crt:* fichero correspondiente al certificado público del servidor.
- *servidor.key:* fichero correspondiente a la clave privada del servidor, la cual debe permanecer protegida.
- *01.pem:* fichero correspondiente al certificado público del servidor en formato PEM. El nombre del fichero proviene de su número de serie del certificado, el cual es 01.
- *servidor.csr*: este fichero sirve para poder crear el certificado del servidor en otra máquina que pueda crearlo y firmarlo, ya que este fichero tiene toda la información que le hace falta.

12. Creamos la clave/certificado del Cliente

```
jaime@BCNproxy:/etc/openvpn/easy-rsa$ ./build-key cliente
Generating a 1024 bit RSA private key
.............++++++
.............................++++++
writing new private key to 'cliente.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SP]:
State or Province Name (full name) [BCN]:
Locality Name (eg, city) [Barcelona]:
Organization Name (eg, company) [Audifon]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [cliente]:
Name []:
Email Address [adminbcn@audif.local]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'SP'
stateOrProvinceName   :PRINTABLE:'BCN'
localityName          :PRINTABLE:'Barcelona'
organizationName      :PRINTABLE:'Audifon'
commonName            :PRINTABLE:'cliente'
emailAddress          :IA5STRING:'adminbcn@audif.local'
Certificate is to be certified until Jan  3 16:52:01 2022 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Tras realizar estos pasos hemos generado 4 ficheros nuevos:

- *client.crt:* fichero correspondiente al certificado público del cliente.
- *client.key:* fichero correspondiente a la clave privada del cliente, la cual debe permanecer protegida.
- *02.pem:* fichero correspondiente al certificado público del cliente en formato
- PEM. El nombre del fichero proviene de su número de serie del certificado, el cual es 02.
- *client.csr:* este fichero sirve para poder crear el certificado del cliente en otra máquina que pueda crearlo

Estos ficheros habrá que transferirlos al cliente.

13. Generamos los parámetros Diffie Hellman.

```
jaime@BCNproxy:/etc/openvpn/easy-rsa$ ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....................................................................................+.....
.....................................+.....................+.....................+.+....
.....................................+++*++*++*
```

Tras ejecutar este script se genera un fichero en formato PEM llamado dh1024.pem. Los parámetros Diffie Hellman se utiliza para poder realizar el intercambio de una clave entre dos participantes de manera segura. Para ello se realizan una serie de funciones matemáticas que utilizan estos parámetros y que garantizan que solo los dos participantes conocerán la clave una vez se realice todo el proceso y funciones matemáticas.

Este archivo solo debe de estar ubicado en el servidor *openVPN*.

14. Cremos el archivo */etc/openvpn/server.conf* con las siguientes líneas

server.conf

```
local 83.45.45.245
port 1194
dev tun
proto udp
ifconfig 10.8.0.1 10.8.0.2
tls-server
dh dh1024.pem
ca ca.crt
cert servidor.crt
key servidor.key
comp-lzo
keealive 10 120
persist-key
persist-tun
status openvpn-status.log
verb 6
```

15.2. INSTALACIÓN VPN MADRID

1. Lo primero es instalar openVPN en el servidor mediante el comando siguiente.

```
jaime@MADproxy:~$ sudo apt-get install openvp
```

2. Se crea, carga y habilita el routing en el dispositivo TUN/TAP integrado en el Kernel de Linux.

```
sudo mknod /dev/net/tun c 10 200
```

3. Se añade al fichero /etc/modules.conf la siguiente línea

```
alias char-major-10-200 tu
```

4. Se carga el driver TUN/TAP

```
sudo modprobe tun
```

5. Se habilita el routing en el driver TUN/TAP

```
jaime@MADproxy:~$ sudo -s
jaime@MADproxy:# echo 1 > /proc/sys/net/ipv4/ip_forward
jaime@MADproxy:# exit
exit
```

6. Ahora hay que incluir una nueva entrada en la tabla de rutas del servidor OPENVPN para que se pueda comunicar con el cliente de openVPN de Madrid, mediante el siguiente comando.

```
jaime@MADproxy  :~$ sudo route add -net 192.168.1.0 netmask 255.255.255.0 gw 10.8.0.1
```

7. Se importan los certificados de usuario y archivo ca.crt generados en el servidor BCNproxy a la ruta */etc/openvpn/easy-rsa/keys* del servidor MADproxy.

8. Se crea el archivo */etc/openvpn/cliente.conf* con las siguientes líneas

client.conf

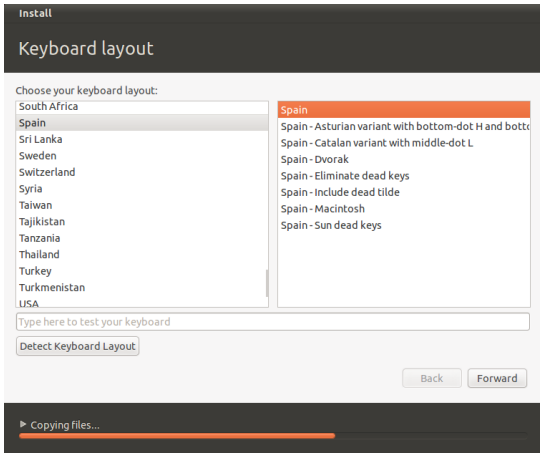
```
dev tun
proto udp
remote 80.45.45.245 1194
ifconfig 10.8.0.2 10.8.0.1
tls-client
nobind
ca ca.crt
cert cliente.crt
key cliente.crt
comp-lzo
resolv-rety infinite
keepalive 10 120
persist-key
persist-tun
status openvpn-status.log
verb 6
```

16. INSTALACIÓN Y CONFIGURACIÓN EQUIPOS ESCRITORIO (CLIENTES)

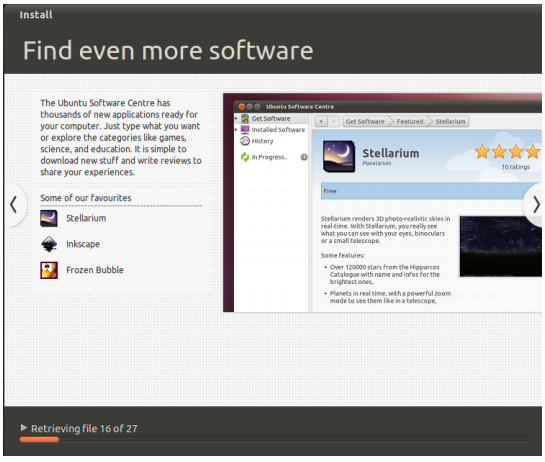
16.1. INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS NUEVOS

En los equipos nuevos lo primero que hay que instalar es, como en el caso de los servidores, el sistema operativo, en este caso instalaremos para todos ellos la versión *Ubuntu Desktop 11.04* mediante el siguiente procedimiento.

1. Bajar la versión de *Linux Ubuntu* de la página Web http://www.ubuntu.com/download/ubuntu/download y grabar el archivo .iso en un CD-ROM.
2. Arrancamos con el CD-ROM donde esté grabada la imagen del paso anterior.
3. Empieza la copia de archivos al ordenador
4. Seleccionamos el idioma del teclado



5. Sigue la copia de archivos automática.

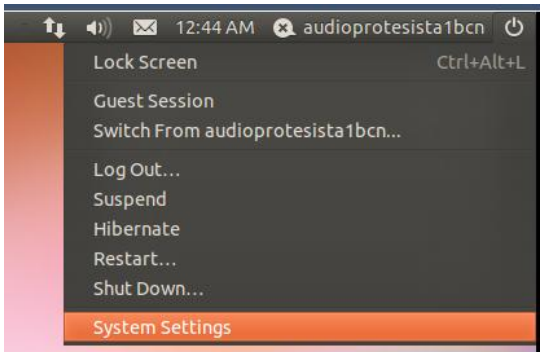


6. Se reinicia el equipo y ya tenemos el sistema operativo instalado.

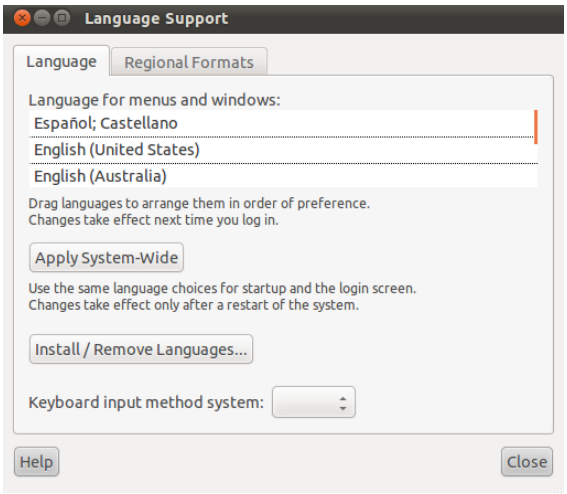
16.2. INSTALAR IDIOMA CASTELLANO

Lo primero que hacemos es poner el idioma del sistema operativo en castellano. Para ello seguimos los siguientes pasos.

1. Hacemos clic en el icono de apagado (parte superior derecha de la pantalla) y después en *system settings*



2. Hacemos clic en *Language Support*



3. Pinchamos en el botón *Install/Remove Languages*, buscamos el idioma Español, lo seleccionamos y damos al botón *Apply Changes.*
4. Una vez que lo tenemos instalado nos aparecerá en el listado de lenguajes disponibles. Lo ponemos en la primera posición.
5. Reiniciamos el equipo, y lo tenemos en Castellano.

y terminará el proceso de instalación de la máquina virtual java en el equipo.

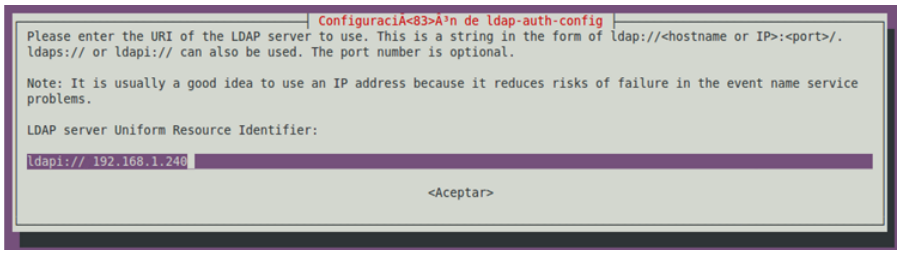
16.3. CONFIGURACIÓN PARA AUTENTICAR EN DOMINIO

Para añadir un ordenador al dominio LDAP de creado hay que instalar los siguientes paquetes.

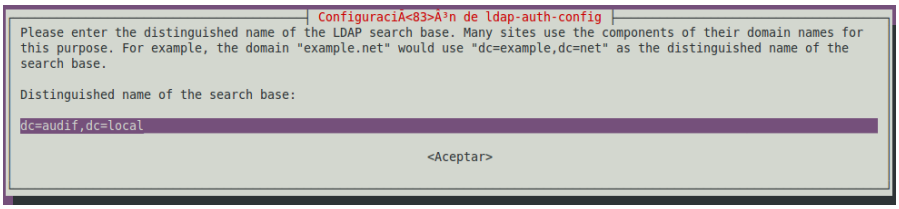
```
audioprotesista1bcn@ubuntu:~$ sudo apt-get install auth-client-config libpam-ldap libnss-ldap
```

Nos saldrá un asistente para la configuración y contestamos como se ve en las siguientes pantallas.

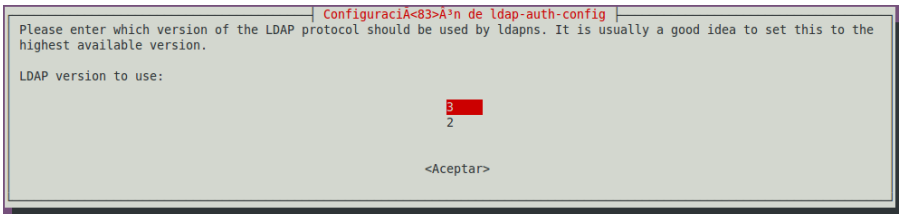
1. Ponemos la dirección IP del servidor *LDAP*, si son equipos de Barcelona se pone la que sale en pantalla si son de Madrid se pone la dirección IP del servidor de Madrid, 192.168.2.240.



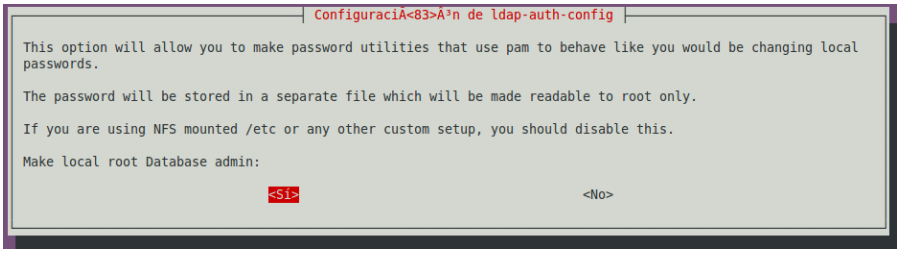
2. Insertamos el nombre del dominio.



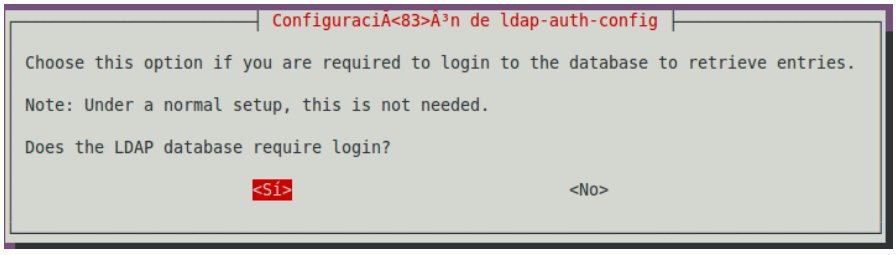
3. Seleccionamos la versión 3 del protocolo LDAP.



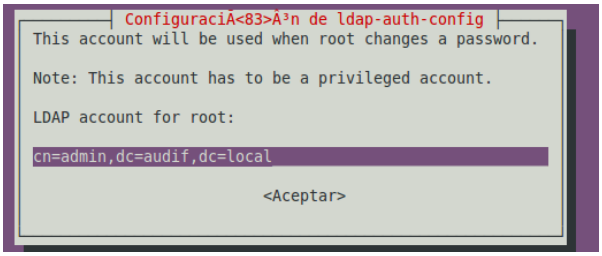
4. Seleccionamos "SI"



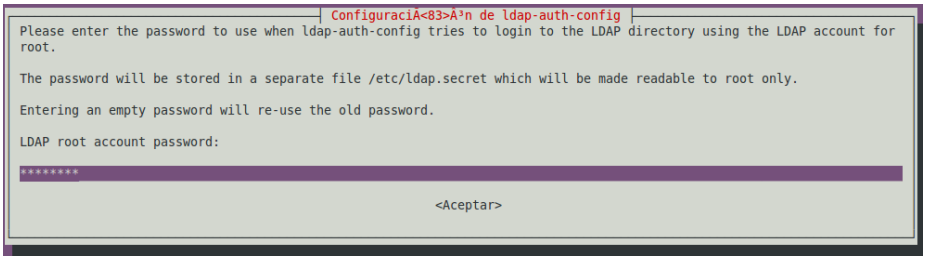
5. Seleccionamos "SI"



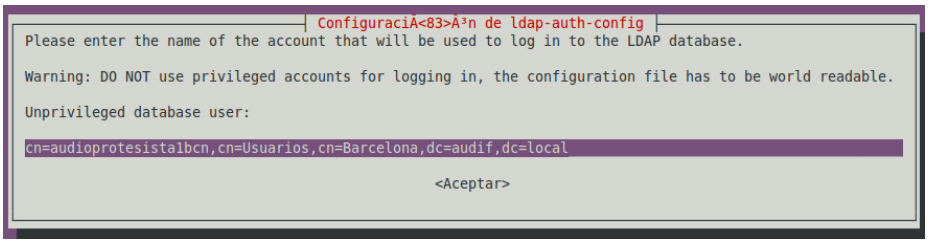
6. Insertamos la cuenta del usuario administrador del dominio



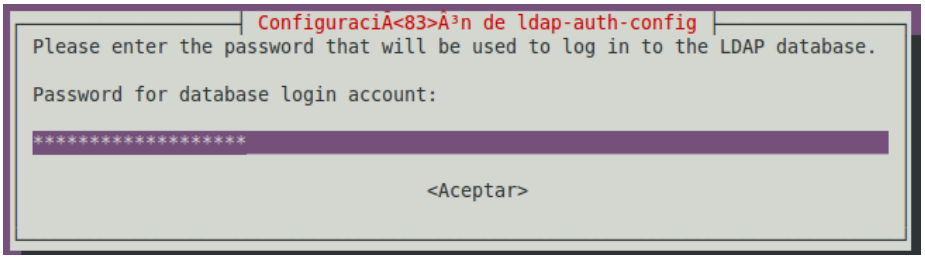
7. Insertamos el password del usuario administrador del dominio (Pasw0rd)



8. Insertamos la cuenta del usuario *LDAP* que se va a autenticar en este equipo. Para cada equipo será diferente.



9. Insertamos la contraseña del usuario LDAP insertado en el punto anterior, en este caso "audioprotesista1bcn"



10. Verificamos que los datos han sido introducidos correctamente en el archivo /etc/ldap.conf
11. Añadimos al archivo la línea "bind_policy_soft"
12. Copiamos el archivo a la ruta /etc/ldap/
13. Creamos el archivo del perfil /etc/auth-client-config/profile.d/open_ldap con el siguiente contenido.

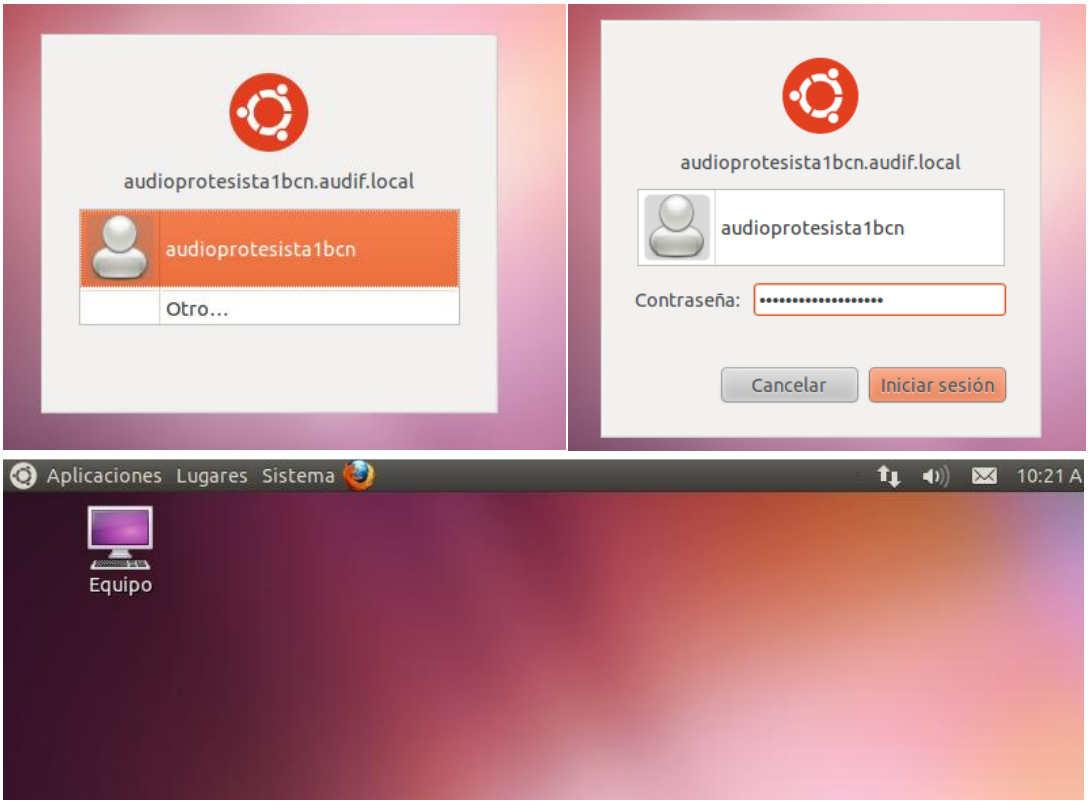
```
[open_ldap]
nss_passwd=passwd: compat ldap
nss_group=group: compat ldap
nss_shadow=shadow: compat ldap
pam_auth=auth required pam_env.so
auth sufficient pam_unix.so likeauth nullok
auth sufficient pam_ldap.so use_first_pass
auth required pam_deny.so
pam_account=account sufficient pam_unix.so
account 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
```

14. Activamos la autenticación *LDAP* que acabamos de crear con el siguiente comando.

```
audioprotesista1bcn@ubuntu:~$ sudo auth-client-config -a -p open_ldap
```

15. Y reiniciamos el equipo para que tengan efecto los cambios.

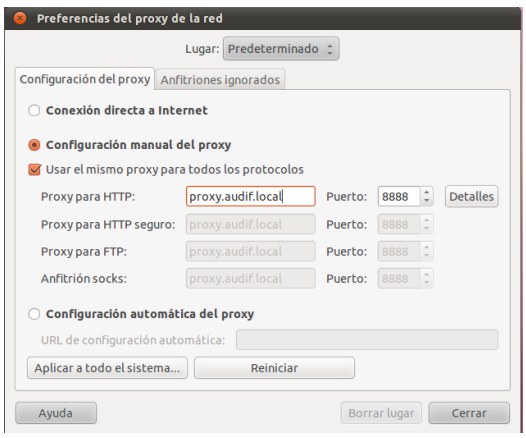
16.3.1. PRUEBA DE AUTENTICACIÓN EN DOMINIO



Vemos que se autentica correctamente en el dominio e inicia sesión.

16.4. CONFIGURACIÓN PROXY

Para configurar el servidor proxy en los equipos de escritorio con Ubuntu hay que ir a la opción del menú "*Sistemas/Preferencias/Proxy de la Red*" y lo configuramos de la siguiente forma.



17. MIGRACIÓN EQUIPOS WINDOWS

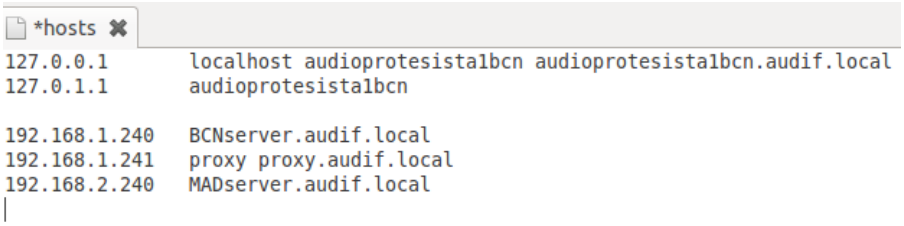
El proceso de migración de los equipos actuales con Windows Xp a Ubuntu, seguirá el siguiente guión:

- Salvado de datos del usuario del equipo en un dispositivo externo.
- Salvado de copia de seguridad de actual sistema, mediante la clonación. Esto se hace por si el usuario no ha salvado algún documento que no creía necesario pero luego constata que lo necesita, así podremos recuperarlo. Estas copias se mantendrán únicamente durante un mes.
- Formateo del Disco Duro.
- Instalación y configuración del nuevo Sistema operativo (Ubuntu) siguiendo el punto 16 del presente documento.
- Recuperación de los documentos salvados del usuario guardados en el dispositivo externo.

18. CONFIGURACIÓN COMÚN PARA TODOS LOS CLIENTES

18.1. MODIFICACIÓN ARCHIVO HOSTS

Para una correcta resolución de nombres configuramos en cada equipo el archivo */etc/hosts* de la siguiente forma.



Donde *"audioprotesista1bcn"* corresponde al nombre de cada máquina a configurar.

18.2. INSTALAR MAQUINA VIRTUAL JAVA

La máquina virtual java es necesario para todos los equipos ya que su herramienta principal de trabajo funciona con ella.

Para la instalación ponemos los siguientes comandos en el terminal de cada equipo.

```
sudo apt-get-repository ppa:ferramroberto/java
sudo apt-get update
sudo apt-get install sun-java6-jre sun-java6-plugin
```

Aparecerá una pantalla indicando la licencia de SUN que la aceptaremos.

19. CONCLUSIONES

19.1. CONSECUCIÓN DE OBJETIVOS PROPUESTOS

Recordando el punto del proyecto 4 "*Objetivos del Proyecto*" tenemos que hacer un estudio de los puntos que hemos conseguido, para ello en la siguiente tabla podemos ver de un vistazo cuáles han sido conseguidos, cuáles no y un breve comentario sobre cada uno.

Objetivo	Conseguido	Observaciones
Migración de todo el sistema actual a plataforma GNU/Linux	SI	Se realiza con todos los equipos actuales de la empresa, los futuros en la medida de lo posible también se incluirán bajo plataforma GNU/Linux
Posibilidad incluir equipos con plataforma Windows	SI	Gracias a *Samba* tenemos la posibilidad de incluir equipos *Windows*en la empresa
Reutilización parqué informático actual	SI	Se reutiliza todo el parqué informático actual, lo único que hace falta a mayores son dos equipos para los servidores de VPN, Firewall y Proxy de características mínimas
Eliminar externalización de servicio de Correo	SI	Gracias a la implementación de *Postfix, Dovecot, Squirremail, Amavis-new, Spamassain, ClamAV* se elimina la externalización del servicio de correo
Eliminar externalización de servicio de Firewall	SI	Se implementa *UFW* para la eliminación de la externalización del servicio
Eliminar externalización de servicio de VPN	SI	Se implementa *OpenVPN* para la eliminación de la externalización del servicio
Unión de las dos sedes	SI	Gracias a la implementación de *OpenVPN* se realiza la unión *"punto a punto"* de las dos sedes
Implementar política de compartición de ficheros	SI	Se implementa *NFS* para la compartición de archivos desde el servidor, la política de seguridad hay que tratarla en una reunión con los gerentes de cada sede
Implementar política de seguridad de acceso a Internet	SI	Se implementa *Squid* como servidor proxy y se crea una política de acceso a internet pudiendo solo acceder a daterminadas páginas y fuera de horario laboral

19.2. CONSECUCIÓN DE OBJETIVOS NO PROPUESTOS

Además de los objetivos propuestos por la empresa, con el proyecto se han conseguido los siguientes:

Objetivo	Conseguido	Observaciones
Generalización de los nombres de los equipos	SI	Para poner el nombre a los equipos se utiliza el puesto que va a cubrir la persona que lo utilice en vez de su nombre.
Reducción de costes	SI	Gracias a la implementación de software libre en todo el sistema informático de la empresa no habrá costes de licencias, además se elimina el coste de externalización de los servicios de VPN, Firewall y Correo
Se implementa un dominio común para las dos sedes	SI	De esta forma podrán acceder sin problemas a los equipos de redes distintas, también gracias a la VPN.
Se estructuran los grupos de usuarios en función de cada departamento	SI	Gracias a la estructuración por departamento nos facilitará en el futuro la implementación de políticas de seguridad aplicando los cambios a todos los usuarios que pertenecen a cada grupo
Se implementa un gestor de documentación y un control de versiones	SI	Gracias a estos servicios varios usuarios podrán modificar documentos a la vez desde distintos puestos sin problemas ni errores.
Eliminar externalización de servicio de VPN	SI	Se implementa *OpenVPN* para la eliminación de la externalización del servicio
Se instala el servicio de Webmail	SI	Pudiendo acceder al correo electrónico desde cualquier punto de la empresa sin tener porque estar cada usuario en su equipo.
Se instala un Antivirus y AntiSpam en Correo	SI	De esta forma evitamos correo malicioso dentro de la empresa.

20. GLOSARIO

Autenticación: es el acto de establecimiento o confirmación de algo (o alguien) como auténtico, es decir que reclama hecho por, o sobre la cosa son verdadero. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. La autenticación depende de uno o varios factores.

Audioprotesista: El audioprotesista es el único profesional sanitario autorizado oficialmente para adaptar audífonos. Profesionalmente, podríamos equiparlo a un óptico.

Amavisd-new: Es una interfaz confiable y de alto rendimiento entre el cliente de correo (MTA, Mail Transporte Agente) y uno o más supervisores de contenido, como es el caso de supervisores anti-virus, y/o SpamAssassin.

APACHE: El servidor HTTP Apache es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP / 1.1 y la noción de sitio virtual.

BACKUP: Copia de información que se realiza para ser restaurada en caso de pérdida de datos o en caso de ser requerida en posterioridad.

ClamAV: Es una herramienta utilizada en la inspección de mensajes electrónicos que permite identificar si el contenido del correo es un virus.

CUPS (Common Une Printing System): Es un sistema de impresión modular para sistemas operativos de tipos Unix que permite que un ordenador actúe como servidor de impresión. Un ordenador que ejecuta CUPS actúa como un servidor que puede aceptar tareas de impresión desde otros ordenadores clientes, los procesa y los envía al servidor de impresión apropiado.

CVS (Concurrente Versiones System o simplemente): Es una aplicación informática que implementa un sistema de control de versiones: mantiene el registro de todo el trabajo y los cambios en los ficheros y permite que diferentes desarrolladores (potencialmente situados a gran distancia) colaboren. CVS se ha hecho popular en el mundo del software libre. Sus desarrolladores difunden el sistema bajo la licencia GPL.

Dominio: En una red de área local, es un conjunto de ordenadores conectados a la red que confían a unos de los equipos (llamado controlador de dominio) la administración de los usuarios y los privilegios que tienen estos sobre los recursos compartidos disponibles.

Dovecot: Es un servidor de IMAP y POP3 de código abierto para sistemas GNU/Linux / UNIX-like, escrito fundamentalmente pensando en seguridad. Desarrollado por Timo Sirainen.

Firewall: es un elemento de hardware o software utilizado en una red de equipos informáticos que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, según las políticas de red que haya definido la organización responsable de la red.

HTTP (HyperText Transfer Protocolo): Establece el protocolo para el intercambio de documentos de hipertexto y multimedia a la web.

HTTPS (Hypertext Transfer Protocolo sobre Secure Socket Layer): Es la cabecera de URI utilizada para indicar una conexión segura HTTP.

IMAP: Protocolo de acceso a los mensajes de Internet, de la inglés Internet Message Access Protocolo (antiguamente Internet Mail Access Protocolo) es un protocolo informático, basado en TCP/IP, que permite a los usuarios leer sus correos electrónicos en el servidor.

LDAP (Lightweight Directory Acces Protocolo): Es un protocolo a nivel de aplicación, de tipo cliente-servidor el cual permite el acceso a un servicio del directorio ordenado y distribuido para buscar diversa información en un entorno de red. Se usó inicialmente como un Front-end o interfaz final para x.500, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio. LDAP se puede utilizar de muchas maneras: autenticación, directorio compartido (para clientes de correo), libreta de direcciones, etc

MTA (Mail Transfer Agente): Es una aplicación informática que nos permite enviar mensajes de correo de unos usuarios a otros, con independencia de la red que estos usuarios estén utilizando. Entre los más usados encontramos Postfix, sendmail, qmail y Exim.

NFS (Network Hile System): Es un protocolo a nivel de aplicación, de sistema de ficheros en red originalmente desarrollado por Sun Microsystems el 1983, Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.. NFS funciona sobre el protocolo RPC.

ORL (Otorrinolaringología): es la especialidad médica que se encarga de la prevención, diagnóstico y tratamiento, tanto médico como quirúrgico, de las enfermedades de, oídos, vías aéreo-digestivas superiores y la estructura próxima de la cara y cuello.

Phpldapadmin: también conocido como PLA, es una herramienta para la administración de servidores LDAP escrito en PHP, basado en interfaz Web. Trabaja en varias plataformas, pudiendo acceder al servidor LDAP desde cualquier lugar en Internet usando un navegador Web. Se encuentra disponible bajo licencia GPL

POP3 (Tabla Office Protocolo versión 3): Es un protocolo que se utiliza para recoger el correo electrónico.

Postfix: Es un servidor de correo de software libre/código abierto, un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail.

Proxy: Un programa o dispositivo que realiza una acción en representación de otro. Su uso más habitual es la de servidor proxy, sirviendo para permitir el acceso a Internet a todos (o algunos) de los equipos de una organización.

OpenLDAP: Es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocolo (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.

OpenSSH (Open Secure Shell): es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, utilizando el protocolo SSH. Fue creado como una alternativa libre y abierta en el programa Secure Shell, que es software propietario.

Samba: Es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, actualmente denominado CIFS). De esta forma, es posible que ordenadores con GNU/Linux, Mac HUESO X o Unix actúen como servidores o

actúen como clientes en redes de Windows. Samba también para validar usuarios haciendo de Controlador Principal de Dominio, como miembro de dominio o todo como un dominio de Directorio Activo para redes basadas en Windows. A aparte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.

SMTP (Simple Mail Transfer Protocolo): Es decir protocolo simple de transferencia de correo y es un protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre ordenador y/o varios dispositivos (PDAs, móviles, etc).

Spamassassin: Es una herramienta para inspeccionar correos electrónicos que permite determinar si el correo se trata de un SPAM.

Squid: Es un popular programa de software libre que implementa un servidor proxy y un dominio por memoria cae de páginas web, publicado debajo licencia GPL. Proporciona servicios de proxy y memoria cae para Hyper Texto Transporte Protocolo (HTTP), Hilo Transfer Protocolo (FTP), y otros protocolos de red populares.

SquirrelMail: Es una aplicación webmail creada por Nathan y Luke Ehresman y escrita en PHP. Puede ser instalado en la mayoría de servidores web siempre que este apoyo PHP y el servidor web tenga acceso a un servidor IMAP y otro SMTP.

SSH (Secure Shell): Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo el ordenador mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriente.

UFW (Uncomplicated Firewall): Es un cortafuegos diseñado para ser de fácil uso desarrollado por Ubuntu. Utiliza la línea de comandos para configurar las iptables usando un pequeño número de comandos simples.

VPN: de las siglas en inglés de Virtual Private Network , es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

VPN Site to Site: unión mediante la tecnología VPN de dos redes locales a través de una red pública, para la unión de sedes por ejemplo.

21. BIBLIOGRAFÍA

Introducción

http://es.wikipedia.org

GNU/Linux

http://hispalinux.es/GNULinux

Distribuciones Linux

http://www.debian.org/index.es.html
http://www.ubuntu-es.org/
http://www.es.redhat.com/
http://www.centos.org/
http://es.opensuse.org/
http://www.linuxhispano.net/2010/02/16/distribuciones-linux-para-servidores/
http://www.linux-es.org/distribuciones
http://www.guia-ubuntu.org/index.php?title=Versiones_de_Ubuntu

Estudio programas de sustitución bajo Linux

http://www.openldap.org/
http://www.samba.org/
http://www.cvshome.org/
http://www.cups.org/
http://www.apache.org/
http://www.postfix.org/
http://www.dovecot.org/
http://squirrelmail.org/
http://es.libreoffice.org/
http://projects.gnome.org/brasero/
http://www.ubuntu-es.org/forum

Instalación Servidor de Archivos NFS

https://help.ubuntu.com/10.04/serverguide/C/network-file-system.html

Instalación y configuración LDAP

http://cayu.com.ar/wiki/doku.php?id=notas:openldap
http://www.stress-free.co.nz/setting_up_phpldapadmin
http://www.slideshare.net/ocwmexico/instalarphp-lda-padmin
http://www.youtube.com/watch?v=DM_UQVVVtoY

Replicación LDAP

http://www.openldap.org/doc/admin24/replication.html

Samba - LDAP

http://jroliva.wordpress.com/samba-ldap-debian-40-etch/

http://www.ajduenas.com/wp-content/uploads/2007/07/proyecto-integrado-antonio-jesus-duenas.pdf

http://elcorteingles.bdat.net/documentos/validacion_ldap/c294.html

Samba Servidor de Impresión

https://help.ubuntu.com/10.04/serverguide/C/samba-fileprint-security.html

https://help.ubuntu.com/10.04/serverguide/C/samba-printserver.html

Samba Servidor de Archivos

https://help.ubuntu.com/10.04/serverguide/C/samba-fileserver.html

https://help.ubuntu.com/10.04/serverguide/C/samba-fileprint-security.html

Servidor de correo SMTP, IMAP, Webmail, antiSpam:

https://help.ubuntu.com/10.04/serverguide/C/postfix.html

https://help.ubuntu.com/10.04/serverguide/C/dovecot-server.html

http://wiki2.dovecot.org/

http://pedroreina.net/recetas/squirrelmail.html

http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-squirrelmail

http://www.telepieza.com/wordpress/2008/06/23/instalar-squirrelmail-en-un-hosting-mis-primeros-pasos-1a-parte/

https://help.ubuntu.com/10.04/serverguide/C/mail-filtering.html

Servidor de versiones:

https://help.ubuntu.com/10.04/serverguide/C/cvs-server.html

Servidor de gestión de documentación:

https://help.ubuntu.com/10.04/serverguide/C/moinmoin.html

Servidor proxy:

http://www.ibiblio.org/pub/linux/docs/LuCaS/Tutoriales/doc-servir-web-escuela/doc-servir-web-escuela-html/x518.html

https://help.ubuntu.com/10.04/serverguide/C/squid.html

Firewall:

https://help.ubuntu.com/10.04/serverguide/C/firewall.html

http://doc.ubuntu-es.org/UFW

Servidor VPN:

http://repositorio.bib.upct.es/dspace/bitstream/10317/758/1/pfc2873.pdf

https://sites.google.com/site/tutorialeslinuxporrafa/configurar-openvpn-site-to-site-en-centos