Migración de sistemas privativos y de pago a soluciones gratuitas y de libre distribución basada en GNU/Linux.

Memoria TFC

Fernando Gómez Marino **ITIG** 2013/2014-1

INDICE

INTRODUCCIÓN

El presente documento será utilizado como guía y refuerzo de conocimientos sobre el proceso migratorio de sistemas Windows Server de una empresa hacia sistemas GNU/Linux.

Aquí aparecerán reflejados los estados de la arquitectura de redes y sistemas implantados, antes y después de la migración de sistemas y servicios, así como los objetivos generales y concretos a superar.

Todo el proyecto estará enfocado a los sistemas de código abierto; por tanto, aunque se haga mención a lo largo del proyecto a diversos productos de origen privativo, únicamente se detallarán algunos procesos migratorios de un tipo de sistema a otro, así como las diferencias existentes entre los sistemas y servicios de ambas plataformas, evitándose dar detalles sobre configuración de los sistemas antiguos y así quedar reflejados en el documento únicamente las configuraciones de los sistemas resultantes.

Contexto y justificación del proyecto

Nos encontramos ante una empresa que consta de una oficina central y una sede, ambas de ámbito nacional.

Desde el punto de vista de los sistemas informáticos, el aplicativo e información se encuentran centralizadas.

El principal objetivo, por el que se lleva a cabo dicho proyecto, busca un ahorro económicamente importante a largo plazo en los gastos relacionados con la infraestructura y servicios de TI y el departamento de informática de la empresa.

Sin embargo, el cambio radical de sistemas garantizará o mejorará el funcionamiento de los servicios, así como la calidad de los mismos.

Todo esto deberá ser realizado por etapas y de forma correctamente coordinado y controlada, ya que tanto el funcionamiento general de la empresa como su producción deben verse afectado al mínimo por estos cambios.

Por todo esto, podemos indicar que el presente proyecto podrá aplicarse a cualquier empresa, de forma generalizada. Su implantación puede llevarse a cabo en cualquier Pyme o gran empresa, tenga varias sedes o no.

Muchas empresas le gustarían dar el paso para realizar las migraciones de sistemas servidores así como aplicativos que tienen su alternativa gratuita y de libre distribución.

Para llevar a cabo esta tarea se precisa de un equipo de trabajo exclusivamente dedicado a esa labor. Lamentablemente, y dado la precaria actual situación laboral en nuestro país, la mayoría de las empresas se niegan a realizar este tipo de inversiones rápidamente amortizables.

Está considerado un proyecto enriquecedor, técnicamente hablando, dónde el personal que lo lleva a cabo toca ampliamente muchas áreas de la administración de los sistemas informáticos.

Además, generará interesantes beneficios económicos a la empresa tal y como se ha citado más arriba.

Objetivos a alcanzar

Los objetivos del proyecto a lograr pueden ser diferenciados en dos grupos:

- Generales
- Concretos

Cada objetivo general está compuesto de un objetivo concreto, en caso de ser este mismo su propósito, o más de uno. En cualquier caso, los objetivos concretos detallan las tareas exactas e hitos más importantes para el correcto funcionamiento de los servicios informáticos de la empresa.

Objetivos generales

- Migración de todos los sistemas informáticos propietarios de la empresa.
- Reducción de costes de TI.
- Análisis comparativo entre ambas escenas (antes y después de la implantación).

Objetivos concretos

- Migración de sistemas de **autenticación de usuarios** a la red corporativa.
- Migración de sistemas de **conexión de los equipos clientes** a la red corporativa y al exterior de la misma (intranet e internet).
- Migración del sistema de **impresión**.
- Migración de los sistemas de **comunicación**.
- Migración del sistema de **control de versiones**.
- Migración del servidor de **archivos**.
- Migración del sistema de **backups** de la información.
- **Análisis comparativo** entre ambos tipos de sistema.
- **Análisis contable y económico** del ahorro tras la inversión.

Principales Servicios

En la siguiente lista se detallan los servicios así como los sistemas que deberán quedar en funcionamiento tras la migración.

- Autenticación de los usuarios
  - **LDAP**
  - **Samba**
  - **PAM**
- Conexión de los equipos clientes
  - **DHCP**
  - **DNS**
- **Impresión**
- Comunicación
  - **Correo Electrónico (SMTP, IMAP, POP3…)**
  - **Antispam**
- **Servidor de archivos**
- **Copia de seguridad de la información (Backups)**

Se tiene en consideración que pueden aplicarse muchas más migraciones de servicios, como pueden ser los sistemas cortafuegos, enrutamiento o encaminamiento. Sin embargo, se cree que los servicios arriba indicados son los más esenciales e importantes de cara a la red interna de la empresa.

Todos estos servicios podrán proporcionar un ahorro económico a largo plazo en licencias de software de pago, tanto de sistemas operativos servidores y clientes, como del software específico.

A continuación se explica brevemente la utilidad de cada servicio, dándose la versión detallada de los mismos más adelante:

LDAP es el servicio que administra la base de datos de todos los usuarios de un sistema de autenticación cliente-servidor completo.

Samba es un servicio/protocolo encargado de la comunicación entre sistemas *Windows* y otros como *Unix*, *GNU/Linux* o *MacOs*. En este caso nos interesa para que clientes *Windows*, en caso de dejar alguno operativo por exigencias de software específico, puedan conectar al servidor Linux con *OpenLDAP*. Además, será utilizado como servicio **WINS**, que es el encargado de recordar y almacenar las asociaciones entre nombres de dominio y direcciones IP.

PAM será utilizado para asegurar la autenticación de los usuarios al sistema.

DHCP es el servicio destinado a la repartición automática de direcciones IP por toda la red interna de la empresa, evitando así conflictos entre equipos clientes. De esta forma, aunque los ordenadores de sobremesa permanezcan aferrados en el puesto, cada uno con una dirección IP interna fija, asignará dirección IP a aquellos ordenadores que por otros motivos conectan y desconectan habitualmente a la red interna, sin asignarles ninguna dirección ya reservada.

DNS será el encargado de traducir los nombres y direcciones de internet a direcciones IP, y viceversa.

Se proporcionará un servicio de **impresión** a través de la red interna.

Para mantener una buena comunicación de forma interna y externa a la empresa, es conveniente implantar el sistema de **correo electrónico**, a través de los protocolos de envío (***SMTP***) o recuperación de correo (***IMAP*** y ***POP3***). A su vez, y debido a la importancia y fragilidad de los datos internos de las empresas, se implantará también un sistema **antispam** que evite y prevenga la recepción del correo basura o no deseado. Así podrá evitarse la confusión del lector en caso de correos de suplantación de identidad (***phishing***).

Para la comodidad del personal interno, se implantará un **servicio de archivos** centralizado.

Y para concluir, y evitar la pérdida de información del servidor de archivos, se creará un sistema de copias de seguridad (***backups***). En caso de pérdidas de información o supresión errónea, poder recuperarlo.

Planificación del proyecto

El proyecto dispondrá de un total de 123 días desde su inicio hasta finalizar su implantación. Podemos separar las tareas a realizar en 4 grandes fases:

- Fase de **Decisión**
- Fase de **Recopilación Técnica**
- Fase de **Implantación**
- Fase de **Migración**

La primera fase del proyecto se centra en la toma de decisiones y la planificación del proyecto en sí misma: tiempos de ejecución, elección y planteamiento del proyecto, posibles aplicaciones en el mundo real, servicios y necesidades a cubrir, etc.

En la siguiente fase se recopila toda la información técnica posible acerca de las tecnologías empleadas o a sustituir (antes y después de la implantación): sistemas operativos, aplicaciones, versiones y distribuciones, comparaciones con alternativas, etc., así como la selección de la documentación necesaria para afianzar y asegurar que la implantación sea un éxito.

La fase de implantación es la más gruesa con diferencia del proyecto. En esta etapa se establecen y toman forma los nuevos sistemas. Sin modificar aún los sistemas antiguos, el nuevo sistema de información estará operativo al concluir esta fase.

Por último, en la fase migratoria, la parte cliente de los sistemas de información conectarán con los nuevos sistemas, ya puestos operativos en la fase anterior, pudiéndose apagar los servicios antiguos. Esta etapa quizás pueda ser la menos entretenida. En ella habrá que dar soporte a toda la empresa bajo el nuevo funcionamiento, formar a los empleados para su correcto uso, solucionar incidencias que surjan y cubrir cualquier tipo de infortunio inesperado.

A continuación se resume, a nivel cronológico, el transcurso de todo el proyecto mediante un diagrama de Gantt.

Está organizado en varias tareas principales que contemplan, cada una de ellas, los hitos a realizar más relevantes del proyecto.

Diagrama de Gantt Completo (minimizado)

La siguiente imagen muestra el proyecto completo, de forma minimizada, resaltando únicamente los pasos importantes.

Id	Tareas e hitos	Duración	Inicio	Fin
1	TFC - Plataforma GNU/Linux	123 días	23 sep '13	23 ene '14
2	Toma de decisiones y Planificación del proyecto	22 días	23 sep '13	14 oct '13
9	Recopilación de datos técnicos	21 días	15 oct '13	04 nov '13
13	Fase de implantación de nuevos servidores GNU/Linux (preproducción)	28 días	05 nov '13	02 dic '13
67	Fase migratoria de sistemas a producción	21 días	03 dic '13	23 dic '13
75	Memoria del Proyecto	18 días	24 dic '13	10 ene '14
76	Video Presentación del Proyecto	7 días	11 ene '14	17 ene '14
77	Corrección y Entrega de Proyecto	6 días	18 ene '14	23 ene '14

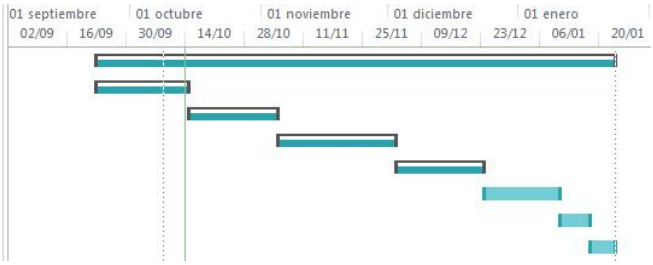
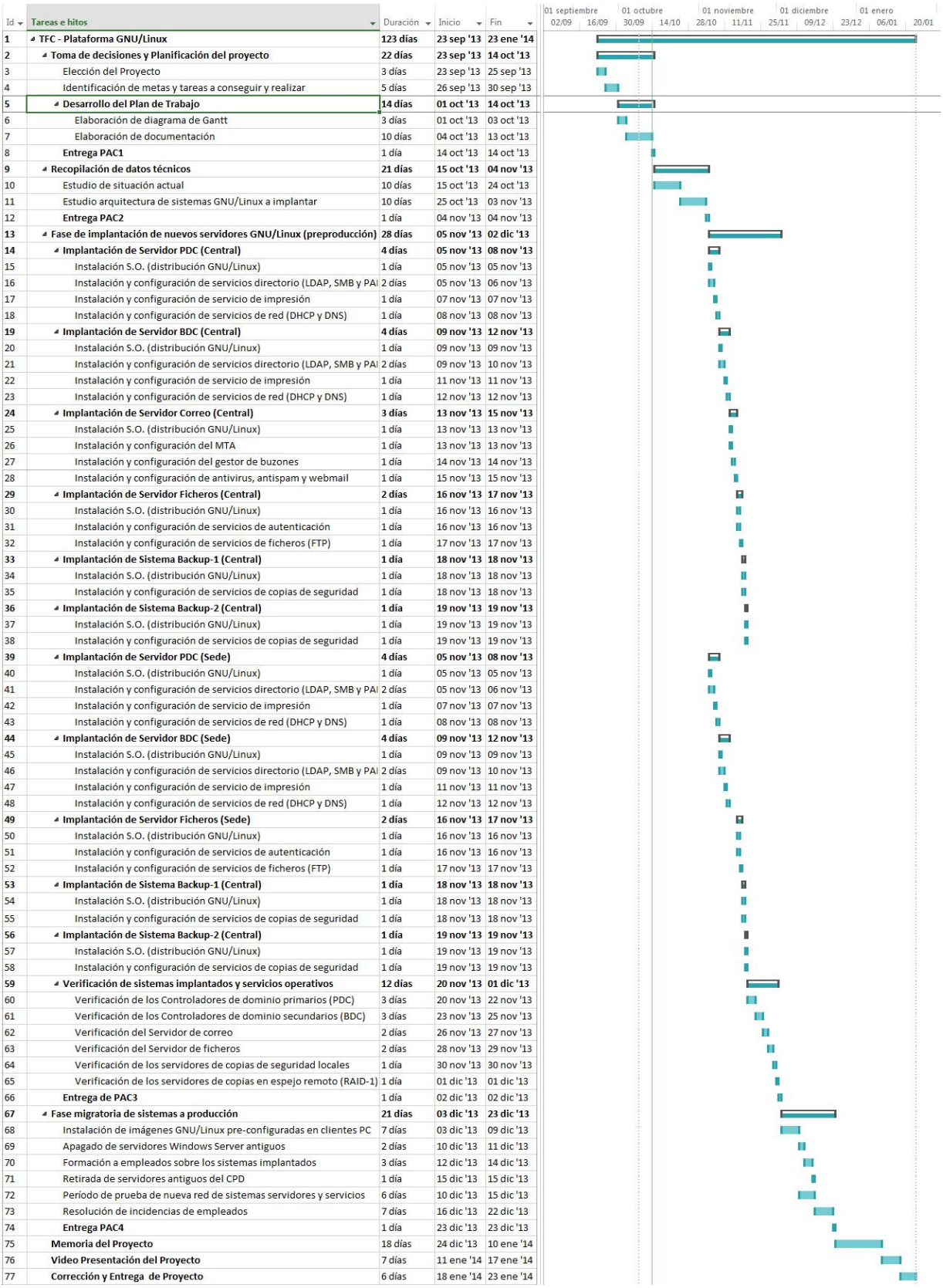


Imagen 1. Diagrama de Gantt minimizado

Diagrama de Gantt Completo (detallado)

Para describir con más detalles cada una de las tareas que refleja la imagen anterior, se muestra el proyecto completo, de forma detallada, reflejando absolutamente todo.



Id	Tareas e hitos	Duración	Inicio	Fin
1	**TFC - Plataforma GNU/Linux**	**123 días**	**23 sep '13**	**23 ene '14**
2	**Toma de decisiones y Planificación del proyecto**	**22 días**	**23 sep '13**	**14 oct '13**
3	Elección del Proyecto	3 días	23 sep '13	25 sep '13
4	Identificación de metas y tareas a conseguir y realizar	5 días	26 sep '13	30 sep '13
5	**Desarrollo del Plan de Trabajo**	**14 días**	**01 oct '13**	**14 oct '13**
6	Elaboración de diagrama de Gantt	3 días	01 oct '13	03 oct '13
7	Elaboración de documentación	10 días	04 oct '13	13 oct '13
8	**Entrega PAC1**	1 día	14 oct '13	14 oct '13
9	**Recopilación de datos técnicos**	**21 días**	**15 oct '13**	**04 nov '13**
10	Estudio de situación actual	10 días	15 oct '13	24 oct '13
11	Estudio arquitectura de sistemas GNU/Linux a implantar	10 días	25 oct '13	03 nov '13
12	**Entrega PAC2**	1 día	04 nov '13	04 nov '13
13	**Fase de implantación de nuevos servidores GNU/Linux (preproducción)**	**28 días**	**05 nov '13**	**02 dic '13**
14	**Implantación de Servidor PDC (Central)**	**4 días**	**05 nov '13**	**08 nov '13**
15	Instalación S.O. (distribución GNU/Linux)	1 día	05 nov '13	05 nov '13
16	Instalación y configuración de servicios directorio (LDAP, SMB y PA	2 días	05 nov '13	06 nov '13
17	Instalación y configuración de servicio de impresión	1 día	07 nov '13	07 nov '13
18	Instalación y configuración de servicios de red (DHCP y DNS)	1 día	08 nov '13	08 nov '13
19	**Implantación de Servidor BDC (Central)**	**4 días**	**09 nov '13**	**12 nov '13**
20	Instalación S.O. (distribución GNU/Linux)	1 día	09 nov '13	09 nov '13
21	Instalación y configuración de servicios directorio (LDAP, SMB y PA	2 días	09 nov '13	10 nov '13
22	Instalación y configuración de servicio de impresión	1 día	11 nov '13	11 nov '13
23	Instalación y configuración de servicios de red (DHCP y DNS)	1 día	12 nov '13	12 nov '13
24	**Implantación de Servidor Correo (Central)**	**3 días**	**13 nov '13**	**15 nov '13**
25	Instalación S.O. (distribución GNU/Linux)	1 día	13 nov '13	13 nov '13
26	Instalación y configuración del MTA	1 día	13 nov '13	13 nov '13
27	Instalación y configuración del gestor de buzones	1 día	14 nov '13	14 nov '13
28	Instalación y configuración de antivirus, antispam y webmail	1 día	15 nov '13	15 nov '13
29	**Implantación de Servidor Ficheros (Central)**	**2 días**	**16 nov '13**	**17 nov '13**
30	Instalación S.O. (distribución GNU/Linux)	1 día	16 nov '13	16 nov '13
31	Instalación y configuración de servicios de autenticación	1 día	16 nov '13	16 nov '13
32	Instalación y configuración de servicios de ficheros (FTP)	1 día	17 nov '13	17 nov '13
33	**Implantación de Sistema Backup-1 (Central)**	**1 día**	**18 nov '13**	**18 nov '13**
34	Instalación S.O. (distribución GNU/Linux)	1 día	18 nov '13	18 nov '13
35	Instalación y configuración de servicios de copias de seguridad	1 día	18 nov '13	18 nov '13
36	**Implantación de Sistema Backup-2 (Central)**	**1 día**	**19 nov '13**	**19 nov '13**
37	Instalación S.O. (distribución GNU/Linux)	1 día	19 nov '13	19 nov '13
38	Instalación y configuración de servicios de copias de seguridad	1 día	19 nov '13	19 nov '13
39	**Implantación de Servidor PDC (Sede)**	**4 días**	**05 nov '13**	**08 nov '13**
40	Instalación S.O. (distribución GNU/Linux)	1 día	05 nov '13	05 nov '13
41	Instalación y configuración de servicios directorio (LDAP, SMB y PA	2 días	05 nov '13	06 nov '13
42	Instalación y configuración de servicio de impresión	1 día	07 nov '13	07 nov '13
43	Instalación y configuración de servicios de red (DHCP y DNS)	1 día	08 nov '13	08 nov '13
44	**Implantación de Servidor BDC (Sede)**	**4 días**	**09 nov '13**	**12 nov '13**
45	Instalación S.O. (distribución GNU/Linux)	1 día	09 nov '13	09 nov '13
46	Instalación y configuración de servicios directorio (LDAP, SMB y PA	2 días	09 nov '13	10 nov '13
47	Instalación y configuración de servicio de impresión	1 día	11 nov '13	11 nov '13
48	Instalación y configuración de servicios de red (DHCP y DNS)	1 día	12 nov '13	12 nov '13
49	**Implantación de Servidor Ficheros (Sede)**	**2 días**	**16 nov '13**	**17 nov '13**
50	Instalación S.O. (distribución GNU/Linux)	1 día	16 nov '13	16 nov '13
51	Instalación y configuración de servicios de autenticación	1 día	16 nov '13	16 nov '13
52	Instalación y configuración de servicios de ficheros (FTP)	1 día	17 nov '13	17 nov '13
53	**Implantación de Sistema Backup-1 (Central)**	**1 día**	**18 nov '13**	**18 nov '13**
54	Instalación S.O. (distribución GNU/Linux)	1 día	18 nov '13	18 nov '13
55	Instalación y configuración de servicios de copias de seguridad	1 día	18 nov '13	18 nov '13
56	**Implantación de Sistema Backup-2 (Central)**	**1 día**	**19 nov '13**	**19 nov '13**
57	Instalación S.O. (distribución GNU/Linux)	1 día	19 nov '13	19 nov '13
58	Instalación y configuración de servicios de copias de seguridad	1 día	19 nov '13	19 nov '13
59	**Verificación de sistemas implantados y servicios operativos**	**12 días**	**20 nov '13**	**01 dic '13**
60	Verificación de los Controladores de dominio primarios (PDC)	3 días	20 nov '13	22 nov '13
61	Verificación de los Controladores de dominio secundarios (BDC)	3 días	23 nov '13	25 nov '13
62	Verificación del Servidor de correo	2 días	26 nov '13	27 nov '13
63	Verificación del Servidor de ficheros	2 días	28 nov '13	29 nov '13
64	Verificación de los servidores de copias de seguridad locales	1 día	30 nov '13	30 nov '13
65	Verificación de los servidores de copias en espejo remoto (RAID-1)	1 día	01 dic '13	01 dic '13
66	**Entrega de PAC3**	1 día	02 dic '13	02 dic '13
67	**Fase migratoria de sistemas a producción**	**21 días**	**03 dic '13**	**23 dic '13**
68	Instalación de imágenes GNU/Linux pre-configuradas en clientes PC	7 días	03 dic '13	09 dic '13
69	Apagado de servidores Windows Server antiguos	2 días	10 dic '13	11 dic '13
70	Formación a empleados sobre los sistemas implantados	3 días	12 dic '13	14 dic '13
71	Retirada de servidores antiguos del CPD	1 día	15 dic '13	15 dic '13
72	Período de prueba de nueva red de sistemas servidores y servicios	6 días	10 dic '13	15 dic '13
73	Resolución de incidencias de empleados	7 días	16 dic '13	22 dic '13
74	**Entrega PAC4**	1 día	23 dic '13	23 dic '13
75	**Memoria del Proyecto**	18 días	24 dic '13	10 ene '14
76	**Video Presentación del Proyecto**	7 días	11 ene '14	17 ene '14
77	**Corrección y Entrega de Proyecto**	6 días	18 ene '14	23 ene '14

ENTORNO TECNOLÓGICO

En los próximos puntos se remarcará todo lo relacionado con la parte tecnológica, física y lógica, del proyecto.

Serán objeto de análisis el esquema de red y de arquitectura de sistemas, los datos generales del equipamiento informático, el software usado por la empresa, la distribución de redes, etc… Todo esto será visto antes y después de la implantación en la que se trabaja.

Sin embargo antes de la inmersión en los asuntos más arduos del proyecto, conviene conocer determinados aspectos teóricos sobre el "lugar" hacia dónde nos dirigimos.

Orígenes

A continuación, en los siguientes apartados, se resumen conceptos y algo de historia sobre la tecnología GNU/Linux que tanto nos interesa implantar.

¿Qué es GNU?

GNU es un acrónimo recursivo del inglés *GNU's Not Unix* ("*GNU* no es *Unix*"). Fue iniciado por *Richard Stallman* con el objetivo de crear un sistema operativo libre: el sistema *GNU*. El 27 de septiembre de 1983 se anunció públicamente el proyecto por primera vez. En el anuncio general, siguieron varios escritos de *Richard Stallman*, como el "Manifiesto *GNU*", que establecieron sus motivaciones para realizar el proyecto *GNU*, entre las que destaca "retornar al espíritu de cooperación que había en los tiempos iniciales a la comunidad de usuarios de ordenadores".

UNIX es un sistema operativo privativo muy popular, porque está basado en una arquitectura que ha demostrado ser técnicamente estable. El sistema *GNU* fue diseñado para ser completamente compatible con *UNIX*. El hecho de ser compatible con la arquitectura *UNIX* implicó que *GNU* está 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 se tuvieron que volver a escribir.

Para asegurar que el software *GNU* fuera siempre libre para que todos los usuarios pudieran "ejecutarlo, copiar, modificar y distribuir", el proyecto debía ser lanzado bajo una licencia diseñada para garantizar estos derechos y que evitara las restricciones posteriores de los mismos. La idea en inglés se conoce como *copyleft* (en contraposición al *copyright*), y está contenido en la licencia *GPL*.

¿Qué es GPL?

La Licencia Pública General de *GNU* o más conocida por su nombre en inglés *GNU General Public License* (*GNU GPL*), es una licencia creada por la *Free Software Foundation (FSF*) en 1989, 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.

Al ser un documento que cede ciertos derechos al usuario, asume la forma de un contrato, por lo que usualmente se la denomina contrato o acuerdo de licencia. Por tanto, la *GPL* debe cumplir los requisitos legales de formación contractual en cada jurisdicción.

¿Qué significa Software Libre?

El software libre (en inglés *free software*) es el software que puede ser usado, estudiado y modificado sin restricciones, y que puede ser copiado y redistribuido bien en una versión modificada o sin modificar sin restricción, o bien con unas restricciones mínimas para garantizar que los futuros destinatarios también tendrán estos derechos.

Dado que el software se distribuye libremente, en general se puede encontrar gratuitamente en Internet, o a coste bajo si lo adquirimos por medio de otros medios (*CD-ROM*, *DVD*, disquetes,...). Debido a esto, los modelos de negocio basados en software libre normalmente se basan en proporcionar servicios de valor añadido como soporte técnico, cursos de preparación, personalización, integración, o certificación.

En general, se puede decir que un programa es libre si permite las cuatro libertades definidas por la *Free Software Foundation*:

- La libertad de ejecutar el programa para cualquier propósito (libertad 0).
- La libertad de ver cómo funciona el programa y adaptarlo a las necesidades (libertad 1). El acceso al código fuente es un requisito.
- La libertad de redistribuir copias (libertad 2).
- La libertad de mejorar el programa y distribuir de nuevo con las mejoras realizadas, para que toda la comunidad se pueda beneficiar (libertad 3). Al igual que en la libertad 1, el acceso al código fuente es un requisito.

¿Qué es la Free Software Foundation?

La *Free Software Foundation* (*FSF*) (*Fundación por el software libre*) es una iniciativa de *Richard Stallman* en defensa del software libre y en particular del proyecto *GNU*.

Desde su fundación hasta mediados de los años 90 los fondos de la *FSF* se utilizaron mayoritariamente en ocupar programadores para escribir software libre. Dado que a partir de mediados de los años 90 y hasta la actualidad una multitud de compañías e individuos se han dedicado a escribir software libre, los empleados y voluntarios de la *FSF* trabajan en los aspectos legales y estructurales de la comunidad del software libre.

¿Quién es Richard Stallman?

Richard Matthew Stallman (de nombre en clave *RMS*) es un conocido activista del software libre.

Sus obras más importantes como programador incluyen el editor de texto *Emacs*, el compilador *GCC* y el depurador *GDB*, bajo el Proyecto *GNU*. Pero su influencia es mayor en un marco moral, político y legal para el movimiento del software libre, como una alternativa al desarrollo y distribución del software privativo.

También es el inventor del concepto *Copyleft* (aunque no es él quien le puso nombre), un método para licenciar software para que sea siempre de libre uso y modificación.

¿Quién es Linus Tolvard?

Linus Benedict Torvalds (28 de diciembre de 1969) es un informático finlandés, creador y actual mantenedor del núcleo *Linux*.

En su época de estudiante universitario en Helsinki, a finales de septiembre de 1991, comenzó la creación del núcleo (*kernel*) de un sistema operativo, ya que no podía hacer frente al precio de los sistemas Unix de la época. Originalmente, Linus llamó su proyecto *Freex* (refiriéndose a un sistema Unix libre, mientras que en inglés se pronunciaría igual que *freaks*), pero finalmente lo publicó con el nombre de Linux (mezclando su nombre Linus con *Unix*). Linus involucró mucha más gente a través de un mensaje electrónico que envió a una lista de noticias electrónicas (*news*), que por aquella época era el máximo exponente de Internet. Al poco, la primera versión fue mejorada y ampliada por otros informáticos de todo el mundo, que pudieron leer el código fuente de *Linux* y, por tanto, mejorarlo. En la actualidad continúa colaborando con miles de personas de todas partes, trabajando para mejorar y adecuar a los nuevos tiempos el núcleo *Linux*, organizándose por correo electrónico.

Linux, que es distribuido libremente con licencia *GPL*, ha sido incorporado como parte fundamental de muchas distribuciones de software.

Sus obras más importantes como programador incluyen el editor de texto *Emacs*, el compilador *GCC* y el depurador *GDB*, bajo el Proyecto *GNU*. Pero su influencia es mayor en un marco moral, político y legal para el movimiento del software libre, como una alternativa al desarrollo y distribución del software privativo.

También es el inventor del concepto *Copyleft* (aunque no es él quien le puso nombre), un método para licenciar software para que sea siempre de libre uso y modificación.

¿Qué es 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.

Situación Actual

En el presente, la empresa dispone de dos ubicaciones físicas dónde el personal empleado lleva a cabo sus labores diarias.

Una de estas ubicaciones actúa de sede central de la compañía, teniendo la otra como sede de apoyo geográfico, con menor número de empleados y recursos tecnológicos en ella.

La disponibilidad actual en la empresa es:

- Arquitectura de sistemas privativos, tanto en servidores como en puestos clientes.
- Deficiente uso de los sistemas de correo electrónico, utilizando el protocolo POP para clientes.
- Escasas medidas de seguridad con respecto a los Sistemas de copias y recuperación de información.
- Sobrecarga en la tramitación de información en los controladores de dominios.

Hardware y Software

La **sede central** cuenta con los siguientes equipos:

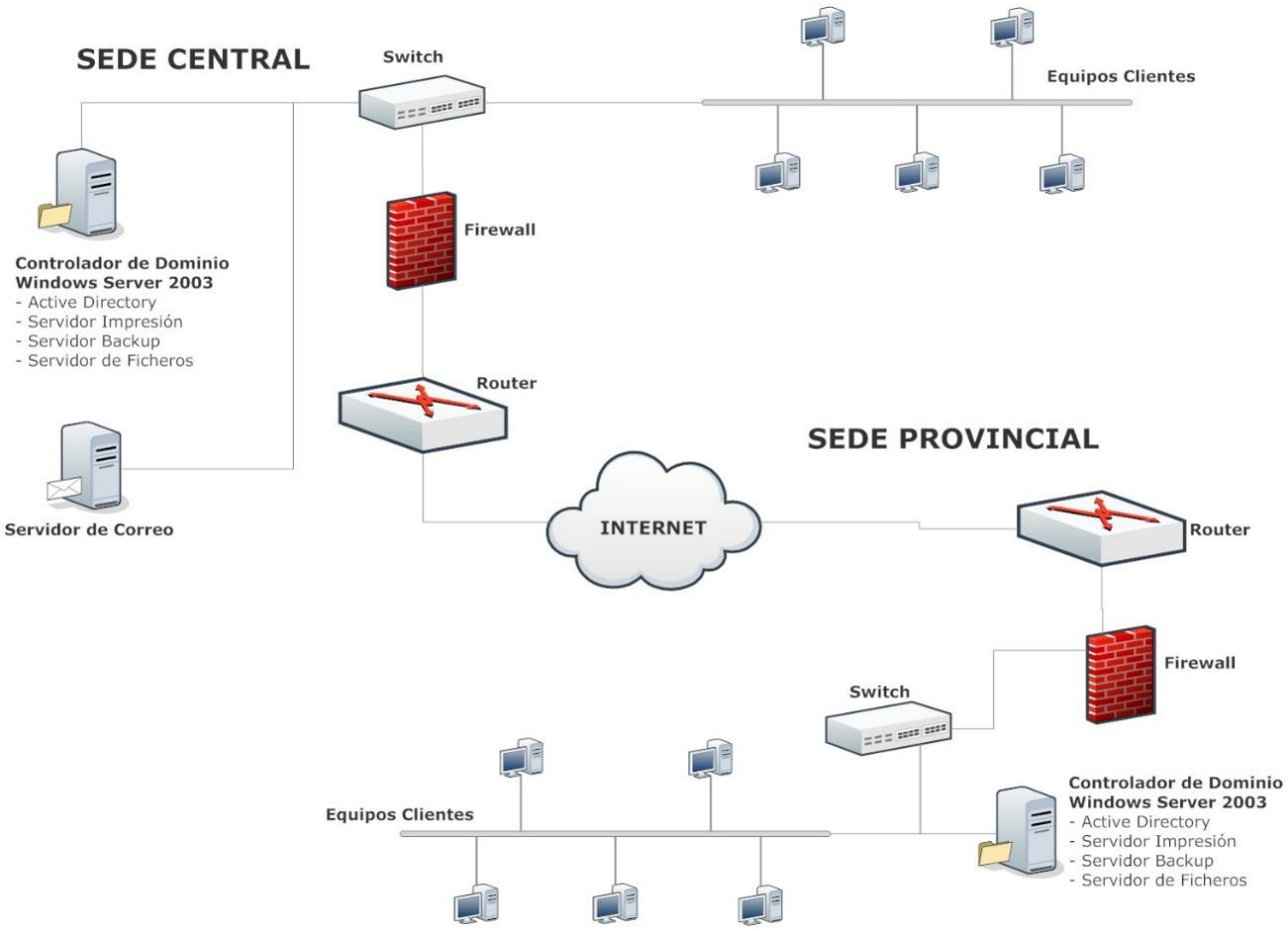
- Servidor Principal (Controlador de Dominio y Servidor de Ficheros)
  - Microsoft Windows Server 2003 SP1
  - Intel Xeon
  - 8 GB de Memoria RAM
  - 4 TB de espacio en disco duro
- Servidor Correo
  - Microsoft Windows Server 2003 SP1
  - Microsoft Exchange Server 2007
  - Intel Xeon
  - 8GB de Memoria RAM
  - 2TB de espacio en disco duro
- 15 PC's clientes de sobremesa
  - Microsoft Windows XP
  - Suite Ofimática: Microsoft Office 2007
  - Intel Core2Duo
  - 1GB de Memoria RAM
  - 250GB de espacio en disco duro
- 10 PC's clientes de sobremesa
  - Microsoft Windows 7
  - Suite Ofimática: Microsoft Office 2010
  - Intel Core2Duo
  - 2GB de Memoria RAM
  - 250GB de espacio en disco duro
- 5 PC's clientes portátiles
  - Microsoft Windows 7
  - Suite Ofimática: Microsoft Office 2010
  - Intel Core2Duo
  - 2GB de Memoria RAM
  - 250GB de espacio en disco duro

La **sede provincial** cuenta con los siguientes equipos:

- Servidor Principal (Controlador de Dominio y Servidor de Ficheros)
    - Microsoft Windows Server 2003 SP1
    - Intel Xeon
    - 8 GB de Memoria RAM
    - 4 TB de espacio en disco duro
- 3 PC's clientes de sobremesa
    - Microsoft Windows XP
    - Suite Ofimática: Microsoft Office 2007
    - Intel Core2Duo
    - 1GB de Memoria RAM
    - 250GB de espacio en disco duro
- 2 PC's clientes portátiles
    - Microsoft Windows 7
    - Suite Ofimática: Microsoft Office 2010
    - Intel Core2Duo
    - 2GB de Memoria RAM
    - 250GB de espacio en disco duro

Esquema de la arquitectura de redes y sistemas

A continuación se muestra el estado actual de la estructura de red y sistemas de la empresa, de forma esquemática, para una mejor comprensión:



Distribución de redes y subredes

La distribución de la red en la empresa es la siguiente:

Sede	Red de la sede	Rango Comunicaciones	Rango Servidores	Rango Clientes e Impresoras	Dominio
Central	192.168.1.0/24	192.168.1.1-192.168.1.19	192.168.1.20-192.168.1.99	192.168.1.100-192.168.1.239	Central.local
Provincia	192.168.2.0/24	192.168.2.1-192.168.2.19	192.168.2.20-192.168.2.99	192.168.2.100-192.168.2.239	Prov.local

Igualmente, se detallan los datos de los equipos más relevantes de la arquitectura:

Nombre equipo	Nombre NetBIOS	IP del Equipo
Router1	Router1.central.local	192.168.1.1
Firewall1	Firewall1.central.local	192.168.1.2
Switch1	Switch1.central.local	192.168.1.3
SRV1	Srv1.central.local	192.168.1.10
SRVCorreo	Srvcorreo.central.local	192.168.1.11
Router2	Router2.prov.local	192.168.2.1
Firewall2	Firewall2.prov.local	192.168.2.2
Switch2	Switch2.prov.local	192.168.2.3
SRV2	Srv2.prov.local	192.168.2.10

Aunque no aparece en la tabla anterior, los equipos correspondientes a PC's clientes tendrán una nomenclatura igualitaria para cada uno de ellos. Sus nombres comenzarán con cliente1, cliente2, etc… y llevarán asignadas las direcciones IP a partir de la 192.168.x.100.

Detalles técnicos de interés

Con respecto a los servidores:

- Ambos servidores/controladores de dominio funcionan mediante la versión *Standard* de *Windows Server 2003*.
- Los dos tienen los servicios de Directorio Activo (*Active Directory*) operativos para proporcionar la funcionalidad de inicio de sesión en red al dominio corporativo.
- Igualmente, dan servicios de DHCP, DNS y WINS a toda la empresa, cada uno a su respectiva sede.
- Son empleados para realizar copias de seguridad de la información de toda la empresa.
- También son utilizados como servidores de ficheros para los empleados.
- Únicamente la Central dispone de un servidor de correo *Microsoft Exchange Server*, bajo *Windows Server 2003 Standard*.

De cara a la parte cliente:

- Todos los equipos clientes tienen *Windows XP/7* Edición Professional.
- Cada uno de ellos dispone de la suite ofimática de *Microsoft* (*Office 2010*).
- Cualquiera de ellos dispone de una grabadora DVD-RW, por lo que todos ellos tienen instalado el software de grabación *Nero BURNING ROM 9*.

Por otro lado y último, ambas sedes están comunicadas entre sí mediante conexión *VPN* (*Red Privada Virtual*), lo cual permitirá acceder a los sistemas de ficheros de una a otra. Gracias a esta conexión, se permite tener sincronizados los datos entre ambos controladores de dominio, por lo que todos los servicios están correctamente distribuidos por toda la compañía sin importar la sede geográfica que se trate, como por ejemplo, el servicio de correo electrónico corporativo.

Situación Final

Tras la implantación de todo el proyecto, la situación de cada sede habrá cambiado considerablemente, con respecto a sus inicios.

La disponibilidad final que se pretende en la empresa es:

- Arquitectura de sistemas libres, tanto en servidores como en la mayoría de los puestos clientes.
- Eficiente uso de los sistemas de correo electrónico, utilizando el protocolo IMAP para clientes y salvaguardando dicha información.
- Mejora sustancial de las medidas de seguridad en los Sistemas de copias y recuperación de información.
- Equilibrado de carga entre los servidores, añadiendo controladores de dominio secundarios en cada sede.
- Separación del servicio de ficheros, inicialmente en el controlador de dominio, a un servidor independiente.

Hardware y Software

La **sede central** cuenta con los siguientes equipos:

- Servidor Controlador de Dominio Principal (PDC)
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8 GB de Memoria RAM
  - 4 TB de espacio en disco duro
- Servidor Controlador de Dominio Secundario (BDC)
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8 GB de Memoria RAM
  - 4 TB de espacio en disco duro
- Servidor Ficheros
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8GB de Memoria RAM
  - 10TB de espacio en disco duro
- Servidor Correo
  - GNU/Linux: Debian (Distribución)
  - Postfix-Dovecot-ClamAV-SpamAssasin-Amavis
  - Intel Xeon
  - 8GB de Memoria RAM
  - 2TB de espacio en disco duro
- Servidor BackupC1
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8GB de Memoria RAM
  - 10TB de espacio en disco duro
- Servidor BackupP2
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8GB de Memoria RAM
  - 4TB de espacio en disco duro
- 2 PC's clientes de sobremesa
  - Microsoft Windows XP
  - Suite Ofimática: Microsoft Office 2007
  - Intel Core2Duo
  - 1GB de Memoria RAM
  - 250GB de espacio en disco duro
- 13 PC's clientes de sobremesa
  - GNU/Linux: Ubuntu Desktop 12.04 x64 (Distribución)
  - Suite Ofimática: Libre Office
  - Intel Core2Duo
  - 1GB de Memoria RAM
  - 250GB de espacio en disco duro

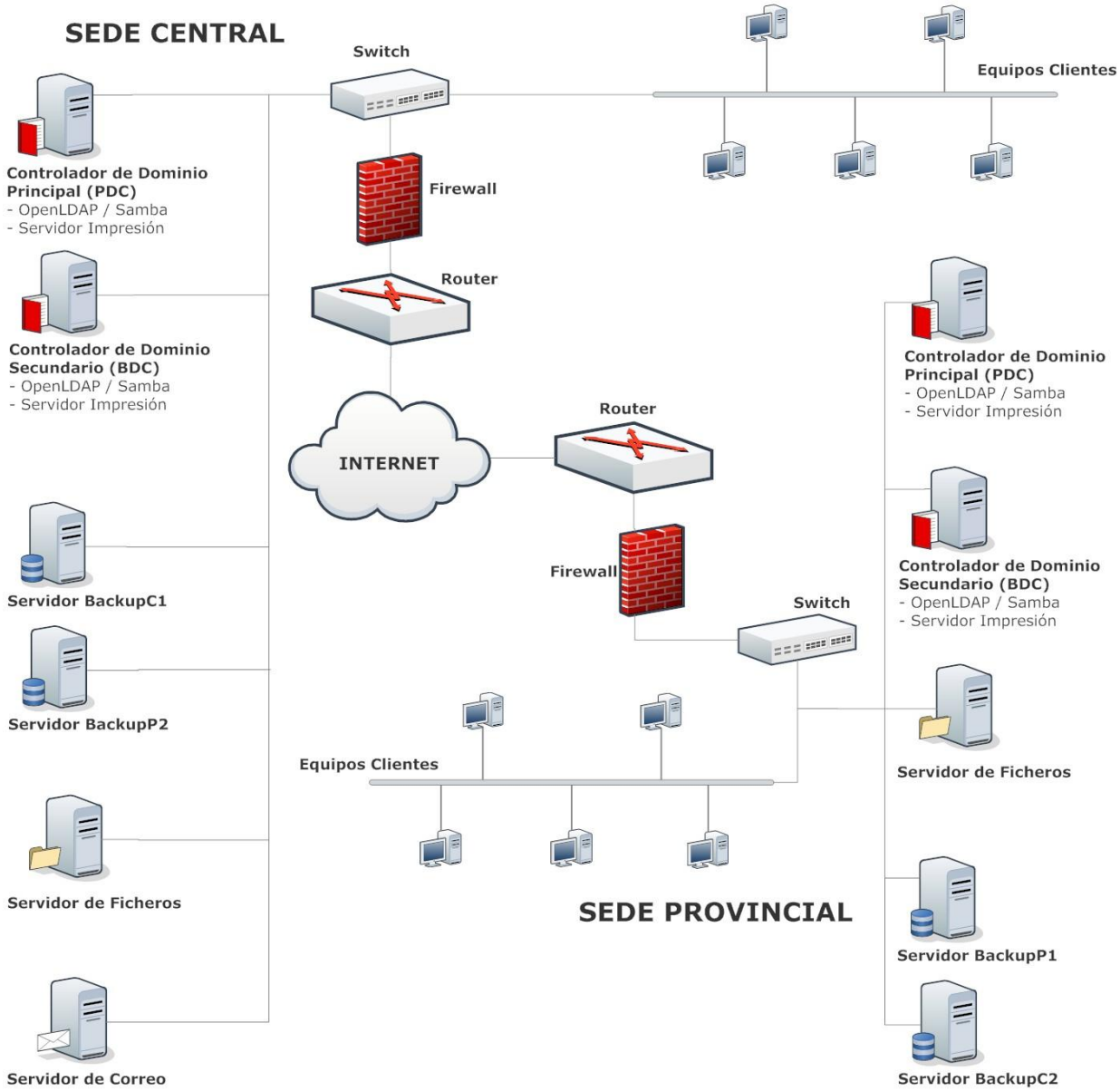
- 1 PC cliente de sobremesa
    - Microsoft Windows 7
    - Suite Ofimática: Microsoft Office 2010
    - Intel Core2Duo
    - 2GB de Memoria RAM
    - 250GB de espacio en disco duro
- 9 PC's clientes de sobremesa
    - GNU/Linux: Ubuntu Desktop 12.04 x64 (Distribución)
    - Suite Ofimática: Libre Office
    - Intel Core2Duo
    - 2GB de Memoria RAM
    - 250GB de espacio en disco duro
- 1 PC cliente portátil
    - Microsoft Windows 7
    - Suite Ofimática: Microsoft Office 2010
    - Intel Core2Duo
    - 2GB de Memoria RAM
    - 250GB de espacio en disco duro
- 4 PC's clientes portátiles
    - GNU/Linux: Ubuntu Desktop 12.04 x64 (Distribución)
    - Suite Ofimática: Libre Office
    - Intel Core2Duo
    - 2GB de Memoria RAM
    - 250GB de espacio en disco duro

La **sede provincial** cuenta con los siguientes equipos:

- Servidor Controlador de Dominio Principal (PDC)
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8 GB de Memoria RAM
  - 4 TB de espacio en disco duro
- Servidor Controlador de Dominio Secundario (BDC)
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8 GB de Memoria RAM
  - 4 TB de espacio en disco duro
- Servidor Ficheros
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8GB de Memoria RAM
  - 4TB de espacio en disco duro
- Servidor BackupP1
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8GB de Memoria RAM
  - 4TB de espacio en disco duro
- Servidor BackupC2
  - GNU/Linux: Debian (Distribución)
  - Intel Xeon
  - 8GB de Memoria RAM
  - 10TB de espacio en disco duro
- 3 PC's clientes de sobremesa
  - GNU/Linux: Ubuntu Desktop 12.04 x64 (Distribución)
  - Suite Ofimática: Libre Office
  - Intel Core2Duo
  - 1GB de Memoria RAM
  - 250GB de espacio en disco duro
- 1 PC cliente portátil
  - Microsoft Windows 7
  - Suite Ofimática: Microsoft Office 2010
  - Intel Core2Duo
  - 2GB de Memoria RAM
  - 250GB de espacio en disco duro
- 1 PC cliente portátil
  - GNU/Linux: Ubuntu Desktop 12.04 x64 (Distribución)
  - Suite Ofimática: Libre Office
  - Intel Core2Duo
  - 2GB de Memoria RAM
  - 250GB de espacio en disco duro

Esquema de la arquitectura de redes y sistemas

Tras la implantación, el resultado de la arquitectura de los sistemas y redes sería como la siguiente:



Distribución de redes y subredes

La distribución de la red en la empresa, tras la implantación de los nuevos sistemas quedaría de la siguiente forma:

Sede	Red de la sede	Rango Comunicaciones	Rango Servidores	Rango Clientes e Impresoras	Dominio
Central	192.168.1.0/24	192.168.1.1-192.168.1.19	192.168.1.20-192.168.1.99	192.168.1.100-192.168.1.239	Central.local
Provincia	192.168.2.0/24	192.168.2.1-192.168.2.19	192.168.2.20-192.168.2.99	192.168.2.100-192.168.2.239	Prov.local

Igualmente, se detallan los datos de los equipos más relevantes de la arquitectura:

Nombre equipo	Nombre NetBIOS	IP del Equipo
Router1	Router1.central.local	192.168.1.1
Firewall1	Firewall1.central.local	192.168.1.2
Switch1	Switch1.central.local	192.168.1.3
PDCC	Pdcc.central.local	192.168.1.10
BDCC	Bdcc.central.local	192.168.1.11
SRVCorreo	Srvcorreo.central.local	192.168.1.12
SRVFich1	Srvfich1.central.local	192.168.1.13
BackupC1	Backupc1.central.local	192.168.1.14
Backupp2	Backupp2.central.local	192.168.1.15
Router2	Router2.prov.local	192.168.2.1
Firewall2	Firewall2.prov.local	192.168.2.2
Switch2	Switch2.prov.local	192.168.2.3
PDCP	Pdcp.prov.local	192.168.2.10
BCDP	BDCP.prov.local	192.168.2.11
SRVFich2	Srvfich2.prov.local	192.168.2.13
BackupP1	Backupp1.prov.local	192.168.2.14
BackupC2	Backupc2.prov.local	192.168.2.15

Al igual que ocurría previo a la implantación, los equipos correspondientes a PC's clientes, que no se han mostrado en la tabla anterior, tendrán una nomenclatura igualitaria para cada uno de ellos. Sus nombres comenzarán con cliente1, cliente2, etc… y llevarán asignadas las direcciones IP a partir de la 192.168.x.100.

Detalles técnicos de interés

Con respecto a los servidores:

- La arquitectura de servidores cambió radicalmente. Se ha pasado de tener un único nodo multifuncional y multiservicio en cada sede a tener dos, uno principal y otro secundario que actuará de backup y respaldo en caso de una caída de servicio en el primero.
- Todos los sistemas operativos servidores han pasado a ser *GNU/Linux*, tomando *Debian* como distribución elegida.
- Los controladores de dominio, tanto los principales como los secundarios deberán de tener exactamente los mismos servicios en funcionamiento para poder realizar el relevo en caso necesario. Dado que ahora los sistemas son libres y no privativos, se cuenta para el servicio de directorio con *OpenLDAP*, complementado por *Samba* y *PAM* para realizar las labores de autenticación de usuarios corporativos.
- Igualmente, dan servicios de *DHCP* y *DNS* a toda la empresa, cada uno a su respectiva sede.
- Los controladores de dominio han dejado de realizar las labores de copias de seguridad, pasando esto a nuevos servidores destinados para ello exclusivamente. Estos nuevos servidores, además, se han implantado de forma que con lleve una mayor seguridad de la información corporativa. El nuevo sistema de backup será explicado mejor en el siguiente apartado.
- Ocurre exactamente lo mismo con la funcionalidad del servicio de ficheros; han pasado a nuevos equipos propuestos para dicha tarea, uno por cada sede.
- En la central, igualmente se dispone de un servidor de correo que dará servicio a ambas sedes. Sin embargo, este servicio también fue migrado a sistemas libres, dejando de lado la dificultad como el precio que supone el anterior Microsoft Exchange.

De cara a la parte cliente:

- Del 80 al 90% de los equipos clientes han pasado a tener instalados un sistema operativo *GNU/Linux*, en este caso tomando *Ubuntu* como distribución elegida.
- Se ha dejado un mínimo porcentaje sin migrar sus sistemas y software ofimático. Es posible que sea necesario el uso de un determinado software específico y este no disponga de alternativa libre.
- La suite ofimática principal para la documentación será *Libre Office*.
- El software de grabación de CD/DVD ha pasado a ser alternativa de software libre, como por ejemplo *Brasero*.

Ambas sedes continuarán conectadas mediante VPN para poder sincronizar los datos entre ambos controladores de dominio principales.

Tras haber implantado los nuevos sistemas, es notable observar una mejora de los servicios así como la carga de los controladores de dominio que ha quedado distribuida en los nuevos servidores.

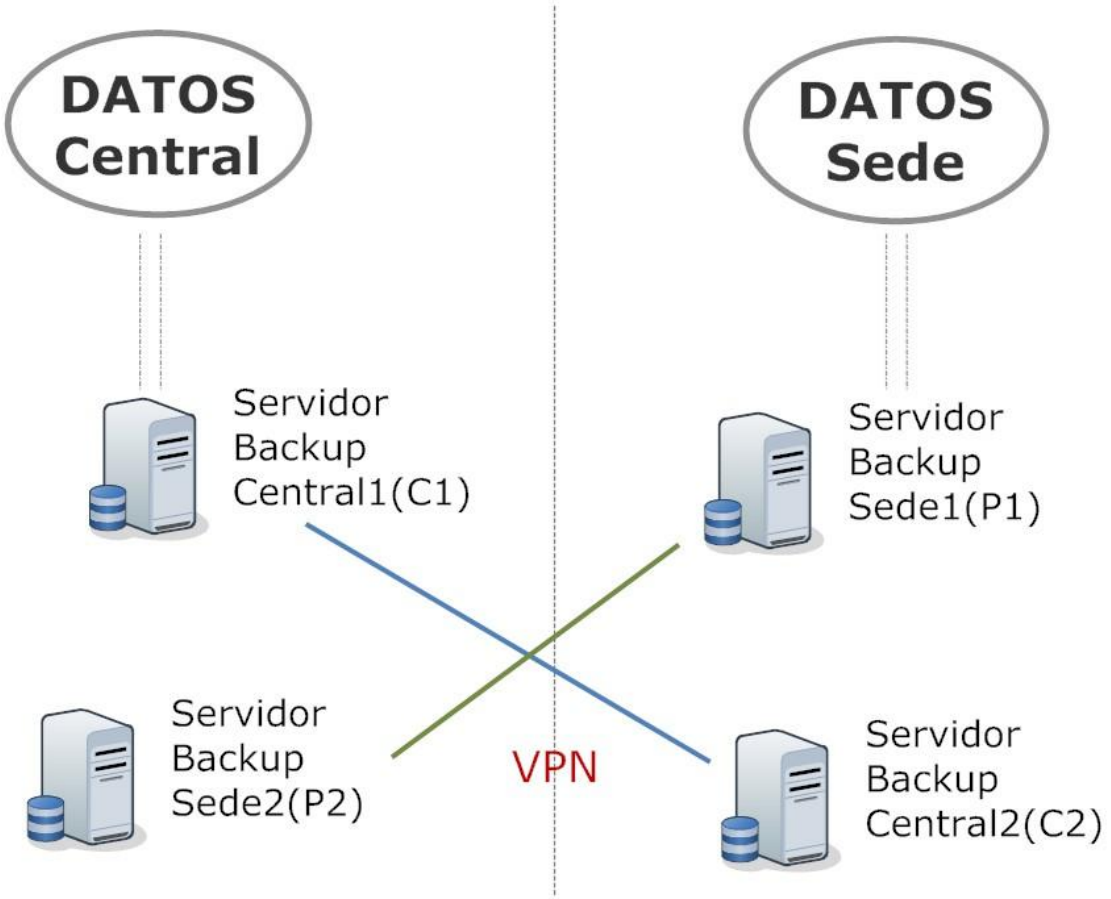
El nuevo sistema BACKUP

Podemos hablar del nuevo sistema de copias de seguridad de la empresa como lo más notorio entre las novedades más preciadas en la arquitectura, desde el punto de vista de la funcionalidad de los sistemas.

¿Qué es lo que trae consigo el nuevo sistema de backup?

Para cumplir con las normativas de calidad en seguridad TI y protección de la información, se ha instalado un doble sistema de seguridad en cuanto a copias se refiere.

El siguiente esquema quizás resuma perfectamente su funcionamiento.



El funcionamiento exacto sería:

- Los datos de la central y la sede provincial son salvaguardados por sus correspondientes servidores de copias de seguridad (backupC1 y backupP1).
- A su vez, cada servidor de backup dispone de otro servidor de backup que lo copia.

Para conseguir una seguridad mucho más óptima, estos segundos servidores de backup estarán situados inversamente en su otra sede; es decir, el servidor que copia al servidor de backup de la central estará situado físicamente en la sede, y viceversa, el servidor que copia al servidor de backup de la sede estará situado físicamente en la central.

Esto consigue que si hay algún problema físico, como un desastre humano o natural (inundación, incendio, terremoto, malos profesionales, empleados vengativos, etc…) y la sede,

los equipos o la información desaparece, se podrá tener al menos una copia de toda la información de la empresa en un lugar geográficamente diferente.

Las oportunidades o posibilidades de que dicho problema ocurra en ambos sitios a la vez es mínima, con lo que por un mínimo coste, la empresa tiene asegurada su información, ya que al fin y al cabo, esta es su principal fuente de ingresos.

Estudio y Análisis Técnico sobre distribuciones GNU/Linux

Actualmente, la comunidad de GNU/Linux ha creado un número bastante considerable de distribuciones diferentes.

Todas las distribuciones, aunque tienen variaciones entre ellas, como son el software que trae preinstalado, la interfaz gráfica utilizada, utilidades mejoradas o implementadas para la comodidad del usuario final, etc., tienen como base distribuciones principales.

Podemos remarcar como las principales distribuciones de GNU/Linux las siguientes:

- Debian
- RedHat

Por supuesto, existen numerosas distribuciones diferentes a las arriba indicadas, sin embargo estas tres han conseguido mayor número de "hijos", por lo que se les puede ver como las principales distribuciones base.

También podemos destacar como distribuciones importantes a Ubuntu, CentOS y Suse. De ellas podemos indicar que son distribuciones significativas en el panorama tecnológico actual, ya que aunque toman como base a las tres primeras, respectivamente, han conseguido mantenerse actualmente como distribuciones independientes, e incluso siendo ellas mismas base de otras muchas.

Sin embargo, aquí denotamos algunas de las características de estos sistemas:

- Debian: 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 basa en Red Hat la gestión de paquetes, distribución y modelo de negocio. Desde 2003 pertenece a la empresa Novell.

Por motivos económicos, las distribuciones Red Hat y Suse quedan descartadas para su instalación en los servidores de la empresa.

Entre las restantes, Debian y Ubuntu, en su versión Server, suponen un peso mucho mayor en entornos empresariales que CentOS.

Debian y Ubuntu Server son bastante similares, con determinadas diferencias, sin embargo para el proyecto actual se ha preferido el uso de Debian ya que, aunque sufre menos actualizaciones que Ubuntu, siempre ha demostrado una estabilidad muy contundente a la hora de su instalación.

Sin embargo, Ubuntu siempre es una de las mejores opciones para el entorno cliente, de ahí su elección para los sistemas de los empleados.

IMPLANTACIÓN

En esta nueva fase del proyecto se dispone toda la información técnica/tecnológica para llevar a cabo la implantación de los nuevos sistemas.

Según lo explicado a lo largo del apartado "Entorno Tecnológico", los sistemas operativos empleados para el grupo de servidores y clientes serán iguales, con Debian y Ubuntu como bases, respectivamente.

Consideraciones Previas

Antes de entrar en *grossa* materia, conviene tener en cuenta las siguientes importantes consideraciones para llevar a cabo con éxito la implantación de los sistemas:

- **Instalación y Uso de Entorno Gráfico**

  Aunque es perfectamente posible la instalación de la interfaz gráfica y no genera inconveniente alguno para estos fines, la elección entre el entorno gráfico y/o textual siempre será de cuestión personal por parte del Administrador de Sistemas de la empresa.

  Siguiendo las pautas de las normativas de seguridad de las TI, se recomienda el uso de la interfaz gráfica únicamente para la instalación y configuración del servidor, por comodidad. Una vez concluidas ambas fases, favorece la desinstalación de dicho entorno para reducir el número de posibles 'puertas' de ataque para un hacker. Por ello la recomendación del mantenimiento de servidores y sus servicios a través de consolas y terminales.

- **Versiones Debian**

  En Internet se pueden encontrar diversas versiones de Debian, sin embargo, para esta implantación nos hemos decantado por la recopilación estable más actual de esta distribución, la 7.2.

  Las causas principales son la actualización de la paquetería, la solidez y madurez del sistema, la reparación de incidencias persistentes en versiones anteriores y la compatibilidad para la incorporación de nuevos servicios en un futuro.

- **Versiones Ubuntu**

  Sin mucho más que comentar en este punto y al igual que en el caso anterior, las decisiones tomadas, nos lleva a decantarnos por la versión 12.04 de Ubuntu.

  En contra de la cuestión anterior, no se ha seleccionado la última versión disponible (13.10) de esta distribución.

  Los desarrollos y publicaciones de las versiones de Ubuntu, a diferencia de Debian, son cortas en el tiempo (dos por año). Esto, aunque permite corregir muchos fallos, puede generar nuevos errores y problemas tras los cambios aplicados. De ahí la selección de

la versión 12.04, con soporte de larga duración (LTS) que ofrece una mayor estabilidad y seguridad en lo que a nuevos problemas surgidos se refiere.

- **Versiones OpenLDAP**

Existen diferentes tipos de configuración a la hora de montar un sistema de directorio LDAP bajo GNU/Linux, con OpenLDAP.

En la siguiente tabla se indica la versión mínima necesaria para poder montar cada tipo de configuración, dependiendo del número de servidores (si es uno o varios servidores) así como, en caso de tratarse de varios, el tipo de apoyo que se ofrecen entre ellos:

Configuración	**Nº de Nodos**	**Versión OpenLDAP (mínima)**
Servidor LDAP	1	2.0
Maestro-Esclavo (slurpd)	2+	2.0-2.2
Maestro-Esclavo (syncprov)	2+	2.3
Multimaster	2+	2.4

Servidores

Para una correcta comprensión por parte del lector y evitar engrosamiento inútil en el documento, se explicará, a continuación, la instalación de los pertinentes sistemas operativos, sin repetir el proceso para cada servidor.

Una vez desarrollada la instalación, se procederá a detallar la configuración para cada tipo de servidor así como las vinculaciones entre ellos.

A continuación se detallan los pasos a seguir relacionados con los servidores: instalación de sistema base, configuración de servicios concretos, migración de datos, etc…

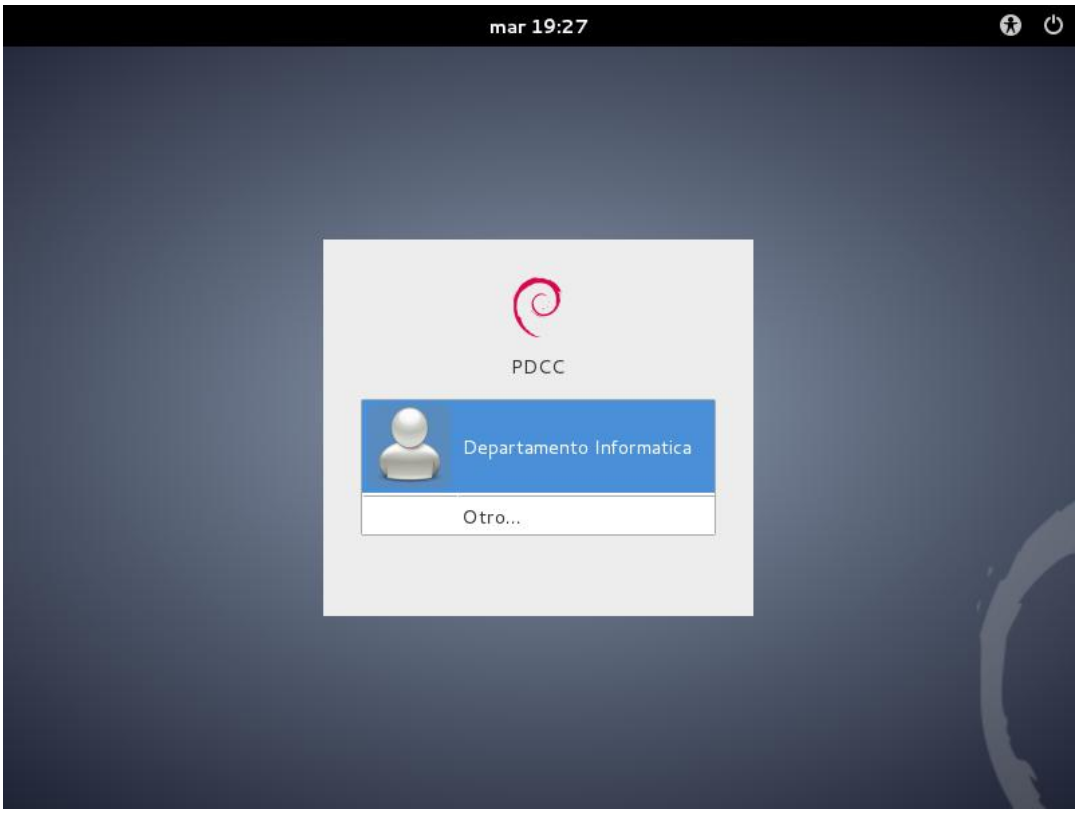
Instalación Sistema Base

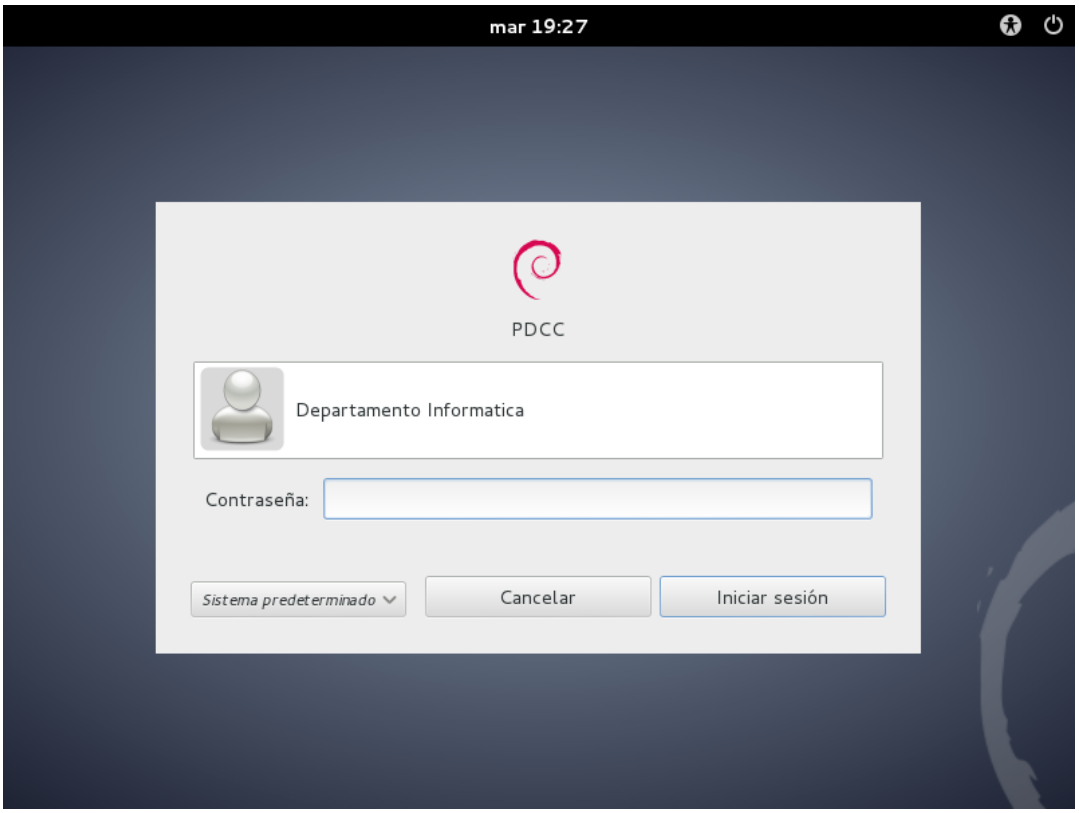
El proceso de instalación del Sistema Operativo base que llevarán los servidores (Debian 7.2) se encuentra detallado en el documento "***ANEXO I_Instalación de sistema base en Servidores***".

Consideraciones Posteriores

Una vez finalizada la instalación del sistema base, hay una serie de pasos iniciales común a todos los servidores. Consiste en instalar una serie de utilidades para poder funcionar correctamente en la implantación y en producción de sistemas.

Antes de instalar nada debe iniciarse sesión con el usuario creado durante la instalación del sistema base como vemos a continuación:





Una vez hemos accedido al sistema, nuestro escritorio será similar a esto (dependiendo del entorno gráfico escogido):

La mayoría de los pasos a seguir serán realizados a través del terminal y como *Super-Usuario* (en adelante **root**).

Para acceder al terminal habrá que dirigirse a ***Aplicaciones*** -> ***Accesorios*** -> ***Terminal***.

Si se desea acceder como *root*, habrá que teclear el siguiente comando y posteriormente la contraseña de este usuario, indicada en la instalación:

```
informatica@PDCC:~$ su –
Contaseña:
root@PDCC:~#
```

Nota

Es muy **recomendable** realizar copia de seguridad de todos los ficheros que se indican en este manual para poder realizar un rollback en caso de necesidad.

Configuración de Red

Para asignar la dirección IP al servidor deberemos modificar el fichero ***/etc/network/interfaces***:

```
root@PDCC:~# vi /etc/network/interfaces
```

El servidor está configurado automáticamente como cliente DHCP:

```
auto lo
iface lo inet loopback
```

Para configurar el servidor con una dirección IP manual, dicho deberá dejarse de la siguiente manera:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static

address <ip servidor>
netmask <subred servidor>
gateway <puerta de enlace>
nameserver <servidor DNS>
```

Cada servidor tendrá sus respectivos valores. En este caso, estos valores fueron indicados en la entrega anterior.

Una vez modificados los datos, se debe reiniciar el sistema.

Para confirmar que los cambios fueron aplicados exitosamente, puede lanzarse el comando de consulta de red ***ifconfig***:

```
root@PDCC:~# ifconfig
eth0      Link encap:Ethernet  HWaddr <dirección MAC servidor>
          inet addr:<ip servidor>  Bcast:<broadcast servidor> Mask:<subred servidor>
          inet6 addr: fe80::a00:27ff:fe2f:7b07/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:956 (956.0 B)  TX bytes:9300 (9.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:780 (780.0 B)  TX bytes:780 (780.0 B)
```

Actualización de repositorios

Para actualizar los repositorios del sistema ejecutaremos lo siguiente:

```
root@PDCC:~# apt-get update
Des:1 http://security.debian.org wheezy/updates Release.gpg [836 B]
Des:2 http://ftp.es.debian.org wheezy Release.gpg [1.672 B]
Des:3 http://security.debian.org wheezy/updates Release [102 kB]
Des:4 http://ftp.es.debian.org wheezy-updates Release.gpg [836 B]
Des:5 http://ftp.es.debian.org wheezy Release [168 kB]
Des:6 http://security.debian.org wheezy/updates/main Sources [74,8 kB]
Des:7 http://security.debian.org wheezy/updates/main i386 Packages [128 kB]
Des:8 http://ftp.es.debian.org wheezy-updates Release [124 kB]
Des:9 http://security.debian.org wheezy/updates/main Translation-en [73,7 kB]
Des:10 http://ftp.es.debian.org wheezy/main Sources [5.959 kB]
Des:11 http://ftp.es.debian.org wheezy/main i386 Packages [5.866 kB]
Des:12 http://ftp.es.debian.org wheezy/main Translation-es [349 kB]
Des:13 http://ftp.es.debian.org wheezy/main Translation-en [3.851 kB]
Des:14 http://ftp.es.debian.org wheezy-updates/main Sources [2.981 B]
Des:15 http://ftp.es.debian.org wheezy-updates/main i386 Packages/DiffIndex [505 B]
Des:16 http://ftp.es.debian.org wheezy-updates/main Translation-en/DiffIndex [505 B]
Descargados 16,7 MB en 9seg. (1.700 kB/s)
Leyendo lista de paquetes... Hecho
root@PDCC:~#
```

La salida por pantalla será similar a la anterior. Se conectará inmediatamente al repositorio pre-configurado durante la instalación del sistema, y actualizará la información del mismo.

En caso de que se desee modificar los orígenes e indicar diferentes o alternativos repositorios, podremos hacerlo desde el fichero ***/etc/apt/sources.list***, que contendrá algo similar a lo siguiente:

```
# deb cdrom:[Debian GNU/Linux 7.2.0 _Wheezy_ - Official i386 NETINST Binary-1 20131012-12:55]/ wheezy main

#deb cdrom:[Debian GNU/Linux 7.2.0 _Wheezy_ - Official i386 NETINST Binary-1 20131012-12:55]/ wheezy main

deb http://ftp.es.debian.org/debian/ wheezy main
deb-src http://ftp.es.debian.org/debian/ wheezy main

deb http://security.debian.org/ wheezy/updates main
deb-src http://security.debian.org/ wheezy/updates main

# wheezy-updates, previously known as 'volatile'
deb http://ftp.es.debian.org/debian/ wheezy-updates main
deb-src http://ftp.es.debian.org/debian/ wheezy-updates main
```

Actualización del software

Para tener la última versión del software del sistema lanzaremos el siguiente comando:

```
root@PDCC:~# apt-get upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
0 actualizados, 0 se instalarán, 0 para eliminar y 0 no actualizados.
root@PDCC:~#
```

En caso de haber actualizaciones nos indicaría cuales son y si deseamos realizarla.

Servicio SSH

Para cualquier servidor es muy práctica y útil la conexión mediante el protocolo SSH.

Para instalarlo ejecutamos el siguiente comando:

```
root@PDCC:~# apt-get install ssh
```

Habilitar usuarios *SUDO*

Sudo permite a un usuario ejecutar aplicaciones con los privilegios del usuario ***root***. Es opcional y no necesario, sin embargo en algún momento puede ser interesante su uso.

A través de la consola se debe editar el archivo ***/etc/sudoers:***

```
root@PDCC:~#  vi /etc/sudoers
```

Al final del archivo añadimos la siguiente línea:

```
<nombre_usuario> ALL=(ALL) ALL
```

Donde <*nombre_usuario*> es el nombre del usuario que tendrá privilegios de ***root***.

Instalación JAVA

Hoy en día JAVA es un complemento para cualquier equipo sea cliente o servidor.

Para instalar el Kit de Desarrollo de Java (*JDK*) en Debian, así como el plugin para el navegador que trae le sistema por defecto (*Icedtea*) lanzamos la siguiente ejecución:

```
root@PDCC:/etc# apt-get install openjdk-7-jre icedtea-7-plugin
```

Una vez tenemos todos los servicios instalados en cada servidor, se procederá a la configuración individual de cada uno de ellos.

Configuración PDC

El servidor principal controlador de domino necesitará servicios como *OpenLDAP*, *Samba*, *PAM*, *PhpLdapAdmin*, etc. Este conjunto de servicios crean el entorno para un servidor de directorio.

Se procede por tanto a explicar cada una de las partes implicadas.

Servicio: OpenLDAP

Comenzamos instalando el servicio de directorio:

```
root@PDCC:/home/informatica# apt-get install slapd ldap-utils
```

Seleccionar "S" para proceder la instalación.

Existen una serie de preguntas a las que damos respuesta a continuación:

Omita la configuración del servidor OpenLDAP? **Si**
Nombre DNS del dominio: *<dominio completo> p.e:* **central.local**
Nombre de la organización: *<dominio> p.e:* **central**
Contraseña de administrador: <ldap_admin_password>
Confirmar contraseña *<ldap_admin_password>*
Permitir protocolo LDAPv2? **No**

Nota

ATENCIÓN: No confundir el usuario administrador de LDAP con el *root* u otro posible usuario, administrador o no, del sistema. Actualmente hablamos del entorno LDAP. Es decir, usuario administrador del domino. Para evitar confusiones muchos administradores emplean la misma contraseña tanto para el *root* del sistema como para el usuario *administrador* de *LDAP*.

Una vez tenemos instalado el servicio de *OpenLDAP* lo siguiente será configurarlo. Sin embargo, es recomendable usar algún Administrador del servicio de directorio LDAP como puede ser *phpLDAPAdmin*:

```
root@PDCC:/home/informatica# apt-get install phpldapadmin
```

Al igual que ocurre con la instalación de OpenLDAP, este servicio igualmente nos requerirá una configuración inicial que vendrá determinado por las siguientes preguntas:

Dirección de host del servidor LDAP: *<ip o nombre dns del servidor> p.e:* **PDCC**
Activa el soporte para el protocolo ldaps? **No**
Nombre distintivo de la base de búsqueda: *<raíz árbol de dominio> p.e:* **dc=central,dc=local**
Tipo de autenticación: **Sesión**
Login dn para el servidor LDAP: *<ruta admin de dominio> p.e:* **cn=admin,dc=central,dc=local**
Servidor Web que se va a reconfigurar automáticamente: **apache2**
Si se reinicia el servidor web (s)? **Sí**

Para conectar *PhpLDAPAdmin* debemos acceder, desde un navegador web, a la dirección *http://localhost/phpldapadmin* ó *http://127.0.0.1/phpldapadmin*, si se accede desde el propio servidor de dominio, o *http://PDCC/phpldapadmin* si se accede desde otro equipo de la red.

Accederemos con el Administrador de LDAP (cn=admin,dc=central,dc=local) y la contraseña configurada para el mismo.

Nota

Si hubiese problemas de conexión con el servicio únicamente habrá que reiniciar el servicio de *LDAP**: #: /etc/init.d/slapd restart***

A continuación deberemos extender el esquema de LDAP para Samba:

```
root@PDCC:/# apt-get install samba-doc
root@PDCC:/# cp  /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/
root@PDCC:/# gunzip /etc/ldap/schema/samba.schema.gz
```

Modificamos el contenido del dichero ***/etc/ldap/ldap.conf*** dejándolo de la siguiente forma:

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/samba.schema
```

```
root@PDCC:/# slaptest -f ldap.conf -F /etc/ldap/slapd.d/
root@PDCC:/# chown -R openldap:openldap /etc/ldap/schema/
root@PDCC:/# chown -R openldap:openldap /etc/ldap/slapd.d/
root@PDCC:/# service slapd restart
```

Chequeamos si el fichero samba.ldif está presente y debemos obtener lo siguiente:

```
root@PDCC:/home/informatica#  ls -l /etc/ldap/slapd.d/cn\=config/cn=\schema
-rw------- 1 openldap openldap 15545 May 16 16:40 cn={0}core.ldif
-rw------- 1 openldap openldap 11379 May 16 16:40 cn={1}cosine.ldif
-rw------- 1 openldap openldap  6509 May 16 16:40 cn={2}nis.ldif
-rw------- 1 openldap openldap  2873 May 16 16:40 cn={3}inetorgperson.ldif
-rw------- 1 openldap openldap 14752 May 16 16:50 cn={4}samba.ldif
```

Servicio: Samba

Para instalar Samba procedemos con los siguientes comandos:

```
root@PDCC:/home/informatica#  apt-get install samba
```

Automáticamente nos pedirá la confirmación para la instalación de paquetería dependiente de *Samba*.

Aparte, necesitaremos instalar las ***Smbldap-tools***. Se trata de un conjunto de scripts hecho en Perl diseñados para administrar las cuentas de usuarios y grupos almacenados en el directorio LDAP.

Tradicionalmente suele instalarse igualmente a través de los repositorios del sistema, sin embargo, en esta ocasión, debido a un error surgido en la última versión del paquete, utilizaremos una versión algo más antigua, aunque igualmente útil.

Descargaremos manualmente la utilidad, que habrá que compilar antes:

```
root@PDCC:/# apt-get install make perl libnet-ldap-perl libcrypt-smbhash-perl
root@PDCC:/# wget http://download.gna.org/smbldap-tools/sources/latest/smbldap-tools-0.9.10.tar.gz
root@PDCC:/# tar xvf smbldap-tools-0.9.10.tar.gz
root@PDCC:/# cd smbldap-tools-0.9.10
root@PDCC:/# ./configure
root@PDCC:/# make
root@PDCC:/a# make install
root@PDCC:/# cp ~/smbldap-tools-0.9.10/doc/smb.conf.example /etc/samba/smb.conf
```

Modificamos el fichero ***/etc/samba/smb.conf*** dejándolo de la siguiente forma:

```
[global]
workgroup = central
server string = PDC
netbios name = PDCC
domain master = yes
local master = yes
domain logons = yes
client lanman auth = yes
client ntlmv2 auth = yes
lanman auth = yes
ntlm auth = yes
security = user
os level = 40
ldap ssl = off
ldap passwd sync = yes
passdb backend = ldapsam:"ldap://127.0.0.1"
ldap admin dn = cn=admin,dc=central,dc=local
ldap suffix = dc=central,dc=local
ldap group suffix = ou=groups
```

```
ldap user suffix = ou=users
ldap machine suffix = ou=machines
ldap delete dn = yes
add user script = /usr/local/sbin/smbldap-useradd -m '%u' -t 1
rename user script = /usr/local/sbin/smbldap-usermod -r '%unew' '%uold'
delete user script = /usr/local/sbin/smbldap-userdel '%u'
set primary group script = /usr/local/sbin/smbldap-usermod -g '%g' '%u'
add group script = /usr/local/sbin/smbldap-groupadd -p '%g'
delete group script = /usr/local/sbin/smbldap-groupdel '%g'
add user to group script = /usr/local/sbin/smbldap-groupmod -m '%u' '%g'
delete user from group script = /usr/local/sbin/smbldap-groupmod -x '%u' '%g'
add machine script = /usr/local/sbin/smbldap-useradd -w '%u' -t 1
logon path = \\%L\profiles\%U
logon drive = P:
logon home = \\%L\%U
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
case sensitive = No
default case = lower
preserve case = yes
short preserve case = Yes
dns proxy = No
wins support = Yes
winbind use default domain = Yes
nt acl support = Yes
msdfs root = Yes
hide files = /desktop.ini/ntuser.ini/NTUSER.*/
unix charset = iso-8859-15
display charset = iso-8859-15
dos charset = 850

[netlogon]
path = /home/samba/netlogon
writable = No
browseable = No
write list = Administrator

[profiles]
path = /home/samba/profiles
browseable = No
writeable = Yes
profile acls = yes
create mask = 0700
directory mask = 0700

[homes]
comment = Home directory
browseable = No
writeable = Yes

[share]
comment = Commun Directory
browseable = Yes
writeable = Yes
```

```
public = No
path = /home/samba/share

[printers]
comment = All Printers
path = /var/spool/samba
create mask = 0700
printable = Yes
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/printers

[group1]
comment = group1 share
path = /home/samba/group1
valid users = @group1
force group = group1
read only = No
create mask = 0660
force create mode = 0660
directory mask = 0770
force directory mode = 0770
```

Una vez guardado el fichero, se deberán crear los siguientes directorios en el servidor:

```
root@PDCC:/# mkdir /home/samba/
root@PDCC:/# mkdir /home/samba/group1
root@PDCC:/# chmod 770 /home/samba/group1
root@PDCC:/# mkdir /home/samba/group2
root@PDCC:/# chmod 770 /home/samba/group2
root@PDCC:/# mkdir /home/samba/homes
root@PDCC:/# mkdir /home/samba/netlogon
root@PDCC:/# mkdir /home/samba/profiles
root@PDCC:/# chmod 777 /home/samba/profiles
root@PDCC:/# mkdir /home/samba/share
root@PDCC:/# chmod 770 /home/samba/share
```

El directorio NETLOGON será utilizado para cargar scripts al inicio de cada sesión de usuario al dominio.

El directorio PROFILE almacenará el perfil móvil de cada usuario de dominio, para ser cargado en cualquier máquina del dominio.

El directorio SHARE es una carpeta para compartir información entre los usuarios y máquinas del dominio.

Realizamos comprobación:

```
root@PDCC:/# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[netlogon]"
Processing section "[profiles]"
Processing section "[homes]"
Processing section "[share]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_DOMAIN_PDC
Press enter to see a dump of your service definitions
```

Deberá salir por pantalla algo similar a lo anterior. Al pulsar *Intro*, nos mostrará el fichero de configuración de *Samba* (***/etc/samba/smb.conf***)

Reiniciamos el servicio de Samba:

```
root@PDCC:/# service samba restart
```

Ahora otorgaremos una contraseña para el administrador del dominio LDAP para Samba:

```
root@PDCC:/# smbpasswd -W
Setting stored password for "cn=admin,dc=central,dc=local" in secrets.tdb
New SMB password:
Retype new SMB password:
```

Obtenemos el SID local:

```
root@PDCC:/# net getlocalsid
SID for domain PDCC is: S-1-5-21-2970213607-3469137201-472098149
```

Nota

Es **IMPORTANTE** almacenar este código SID.

Será empleado más adelante.

Lo siguiente será poblar el servidor OpenLDAP:

```
root@PDCC:/# mkdir -p /usr/local/etc/smbldap-tools
root@PDCC:/# vi /usr/local/etc/smbldap-tools/smbldap.conf
```

Añadiremos al fichero este contenido:

```
SID="S-1-5-21-2970213607-3469137201-472098149" # put SID here
masterLDAP="127.0.0.1"
masterPort="389"
slaceLDAP="127.0.0.1"
slavePort="389"
ldapTLS="0"
verify="require"
suffix="dc=central,dc=local"
usersdn="ou=users,${suffix}"
computersdn="ou=machines,${suffix}"
groupsdn="ou=groups,${suffix}"
idmapdn="ou=idmap,${suffix}"
scope="sub"
hash_encrypt="SSHA"
crypt_salt_format="%s"
userLoginShell="/bin/bash"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="3650"
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
```

Nota

MUY IMPORTANTE realizar el cambio del *SID* y del *suffix*.

Igualmente el fichero ***/usr/local/etc/smbldap-tools/smbldap_bind.conf*** deberá quedar:

```
masterDN="cn=admin,dc=central,dc=local"
masterPw="<contraseña admin LDAP>"
slaveDN="cn=admin,dc=central,dc=local"
slavePw="<contraseña admin LDAP>"
```

Se otorgan los permisos necesarios a dicho fichero:

```
root@PDCC:/# chmod 600 /usr/local/etc/smbldap-tools/smbldap_bind.conf
```

Poblamos el directorio y deberemos recibir algo como lo siguiente:

```
root@PDCC:/# smbldap-populate
Populating LDAP directory for domain CENTRAL (S-1-5-21-2970213607-3469137201-472098149)
(using builtin directory structure)
...
```

```
Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
```

Tras indicar la contraseña para el usuario administrador del dominio se llenará la base de datos del directorio.

Librerías Autenticación: NSS y PAM

Las librerías NSS y PAM son utilizadas para poder autenticar bajo plataformas UNIX.

Instalaremos las librerías con lo siguiente:

```
root@PDCC:/# apt-get install libnss-ldap libpam-ldap
```

Igualmente se requiere una configuración inicial mediante una bateria de preguntas a las que habrá de contestarse de la siguiente manera:

LDAP server Uniform Resource Identifier: **ldap://localhost:389/**
Distinguished name of the search base: **dc=central,dc=local**
LDAP version to use: **3**
Does the LDAP database require login? **No**
Special LDAP privileges for root? **Yes**
Make the configuration file readable/writeable by its owner only? **Yes**
LDAP account for root: **cn=admin,dc=central,dc=local**
LDAP root account password: *<contraseña admin LDAP>*
Allow LDAP admin account to behave like local root? **Yes**
Does the LDAP database require login? **No**
LDAP administrative account: **cn=admin,dc=central,dc=local**
LDAP administrative password: *<contraseña admin LDAP>*
Local encryption algorithm to use for passwords: **crypt**

Tras el asistente, chequeamos la configuración:

```
root@PDCC:/#  sed -e '/^[ ]*#/d' -e '/^$/d' /etc/libnss-ldap.conf
base dc=central,dc=local
uri ldap://localhost:389/
ldap_version 3
rootbinddn cn=admin,dc=central,dc=local
```

```
root@PDCC:/# sed -e '/^[ ]*#/d' -e '/^$/d' /etc/pam_ldap.conf
base dc=central,dc=local
uri ldap://localhost:389/
ldap_version 3
rootbinddn cn=admin,dc=central,dc=local
pam_password crypt
```

Por último deberemos modificar el fichero ***/etc/nsswitch.conf*** dejando las 3 líneas abajo indicadas de la siguiente forma:

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

Una vez hayan concluido las modificaciones, reiniciamos el sistema:

```
root@PDCC:/# reboot
```

Utilidad: LDAP-Utils

El siguiente paquete será necesario para el uso de determinadas herramientas de consulta y modificación de la base de datos de LDAP.

Para instalarlo procedemos únicamente con:

```
root@PDCC:/# apt-get install ldap-utils
```

Ahora estará disponible el comando ***ldapsearch***, tan útil en los servicios de directorio.

Creación de usuarios

Una vez tenemos el servidor con los servicios correctamente configurados, procedemos a crear algún usuario de prueba:

```
root@PDCC:/# smbldap-useradd -a -c "Fernando Gomez" -m -P fgomez
```

Para comprobar su creación basta con ejecutar lo siguiente:

```
root@PDCC:/# ldapsearch -h localhost -b dc=central,dc=local -x uid=fgomez
# extended LDIF
#
# LDAPv3
# base <dc=central,dc=local> with scope subtree
# filter: uid=fgomez
# requesting: ALL
#

# fgomez, users, central.local
dn: uid=fgomez,ou=users,dc=central,dc=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
cn: Fernando Gomez
sn: fgomez
uid: fgomez
uidNumber: 1000
gidNumber: 513
homeDirectory: /home/fgomez
loginShell: /bin/bash
gecos: Fernando Gomez
givenName: fgomez
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
displayName: Fernando Gomez
sambaSID: S-1-5-21-2970213607-3469137201-472098149-3000
sambaPrimaryGroupSID: S-1-5-21-2970213607-3469137201-472098149-513
sambaLMPassword: 5F9A4A0C791AB4FEAAD3B435B51404EE
sambaAcctFlags: [U]
sambaNTPassword: CB8F10319C7864D618378F83E7F68D91
sambaPwdLastSet: 1386056376
sambaPwdMustChange: 1701416376
shadowMax: 3650

# search result
search: 2
result: 0 Success
```

```
# numResponses: 2
# numEntries: 1
root@PDCC:/#
```

Nota

CONSIDERE el cambio del nombre del servidor *localhost* por el *nombre* o *ip* del servidor LDAP en caso de que sea realizado desde otro equipo.
p.e: ***ldapsearch -h PDCC -b dc=central,dc=local -x uid=fgomez***

Creación de Grupos y Asignación de Usuarios

Para crear un grupo de usuarios y su posterior asignación de usuarios únicamente deberá lanzarse los siguientes comandos:

```
root@PDCC:/# smbldap-groupadd -a group1
root@PDCC:/# smbldap-groupmod -m fgomez group1
```

Para verificar la creación y asignación del usuario ejecutamos:

```
root@PDCC:/# smbldap-groupshow group1
...
displayName: group1
memberUid: fgomez
```

Asignamos un directorio común para el grupo de usuarios:

```
root@PDCC:/# chown :group1 /home/samba/group1
```

Asignamos el grupo *Domain Users* al directorio *share*:

```
root@PDCC:/# chown :513 /home/samba/share
```

Servicio: Impresión

El procedimiento para configurar, bajo Debian 7.2, el servicio de impresión (CUPS) y poder imprimir con una impresora de Red, es bastante simple.

Sin embargo en ocasiones no detecta automáticamente el equipo de la red.

A continuación se muestra el procedimiento detallado para la instalación y detección de las impresoras de red por su IP.

Nota

Es posible que el servicio de impresión ya se encuentre instalado. Este paso pudo realizarse si el administrador seleccionó su preinstalación durante la instalación del sistema base.

En este caso, se deberá obviar los pasos de instalación y leer directamente los de configuración.

Primero instalamos CUPS:

```
root@PDCC:/#  apt-get install cups
```

Ingresamos en un navegador web la dirección: *http://localhost:631/admin*

Tiene la opción de autodetectar las impresoras de red. Para ello pulsamos sobre “Encontrar nuevas impresoras”. En caso de que apareciera la impresora deseada, podemos obviar el resto de la configuración.

Si no apareciese de forma automática, agregamos una impresora de forma manual. Pulsamos sobre “Añadir Impresora”, que nos solicitará usuario y clave.

Para ello utilizaremos el usuario *root* y su respectiva contraseña.

En caso de que nuestra impresora de red no sea reconocida, vamos a la opción “Otras Impresoras de Red” y seleccionamos “Protocolo de Impresión de Internet IPP (ipp)”.

Ahora debemos indicar ***ipp://<ip_impresora>:<puerto>/<nombre_impresora>***

P.e: ipp://192.168.1.121:9100/LASERJET4300

Por último, continuamos y colocamos el driver correspondiente.

Una vez finalizada la instalación podremos imprimir con la impresora de red configurada.

Tenga en cuenta que podrá configurar cualquier parámetro de impresión o de la propia impresora a través del mismo panel de control de CUPS del servidor.

Servicio: DHCP

El servicio DHCP es indispensable para cualquier controlador de dominio. Será el encargado de repartir y asignar direcciones IP a cada equipo conectado a la red interna.

Para instalar el servicio lanzamos:

```
root@PDCC:/#  install isc-dhcp-server
```

Se nos mostrará un diálogo pidiendo únicamente la interfaz de red que servirá DHCP a toda la oficina.

Si lo dejamos en blanco intentará detectar automáticamente la interfaz.

Sin embargo, siempre podremos indicar o modificar la interfaz a través del fichero ***/etc/default/isc-dhcp-server***.

Para configurar el servidor debemos dirigirnos al fichero ***/etc/dhcp/dhcpd.conf*** y dejarlo igual (o similar) a lo siguiente:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  authoritative;
  range 192.168.1.180 192.168.1.200;
  default-lease-time 3600;
  max-lease-time 3600;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.1.255;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.160;
  option domain-name "central.local";
}
```

El parámetro ***Authoritative*** supone que la configuración correcta para la red es la definida en el servidor DHCP y tratará de reasignar datos a los clientes mal configurados. Este parámetro puede ser global o asignado a una declaración de subred. Los cambios realizados en en servidor marcado como *authoritative* tienen una rápida propagación en la subred ya que se reconfigura cualquier cliente con la antigua configuración.

El rango (***Range***) básicamente supone el inicio y fin de direcciones disponibles que tomará el propio servidor para asignarlas a los clientes conectados a este.

Default-lease-Time indica el tiempo de asignación en segundos, al igual que ***Max-lease-time*** implica el tiempo máximo, también en segundos, que esperará para asignar.

Y por último se tienen las diferentes opciones:

- ***Subnet-mask*** define la máscara general de red que vamos a utilizar.
- ***Boradcast-address*** define la dirección de difusión de la red.
- ***Routers*** define el Gateway o puerta de enlace de la red.

- ***Domain-name-servers*** define la dirección del servidor DNS de la red.
- ***Domain-name*** define el nombre del dominio DNS que se añade a los nombres de host.

Nota

ADVERTENCIA a tener en cuenta: la dirección del servidor(es) *DNS* de la red deberá cambiarse en el momento que se realice la instalación del servicio *DNS* en este mismo servidor, para que indicarse a sí mismo en este apartado.

El servicio de *DNS* será el único que tendrá indicado la dirección(es) del router y/o del servidore *DNS* que sirvan desde fuera de la empresa.

El protocolo DHCP atribuye direcciones específicas a determinadas máquinas si así se desea, asociando el número de la placa de red a la dirección pretendida. Por tanto, estas direcciones fijas no deberán estar disponibles en la gama o rango de direcciones reservadas para la atribución dinámica.

En caso de que se considere pertinente, para excluir estas direcciones y asignarlas de forma estática a un equipo, se añadiría el siguiente apartado:

```
host <nombre equipo> {
 hardware ethernet <dirección MAC equipo (xx:xx:xx:xx:xx:xx)>;
 fixed-address <dirección IP reservada>;
}
```

Servicio: DNS

Al igual que el servicio DHCP, el DNS es de vital importancia dentro de una red de trabajo de una empresa.

Para instalar el servicio:

```
root@PDCC:/#  install bind9 bind9-doc dnsutils
```

La resolución de nombres traduce nombres de sistemas en sus direcciones IP y viceversa.

Así, la configuración consiste, básicamente en la creación de 2 zonas, una zona de dominio, por ejemplo (zone "central.local"), que convierte nombres en direcciones IP y otra (zone "1.168.192.in-addr.arpa") que convierte direcciones IP en el respectivo nombre de sistema.

Las zonas pueden declararse en el fichero ***/etc/bind/named.conf.local***. Cabría dejar el fichero similar a lo siguiente:

```
zone "central.local"{
   type master;
   file "/etc/bind/db.central.local";
};

zone "1.168.192.in-addr.arpa" {
   type master;
   file "/etc/bind/db.1.168.192";
};
```

Verificamos que el archivo se compuso correctamente:

```
root@PDCC:/# named-checkconf
root@PDCC:/#
```

Lo siguiente será configurar la resolución de nombres.

Para la zona de dominio, crearemos el fichero ***/etc/bind/db.central.local*** tal y como se indicó en el fichero de configuración anterior (*named.conf.local*):

```
;
; BIND zone file for central.local
;

$TTL    3D
@       IN      SOA     ns.central.local.       root.central.local. (
                        2010111101              ; serial
                        8H                      ; refresh
                        2H                      ; retry
```

```
                4W                      ; expire
                1D )                    ; minimum

        NS      ns              ; Inet address of name server

ns              A       192.168.1.160
central.local.  A       192.168.1.160
PDCC            A       192.168.1.160
router          A       192.168.1.1
gateway         CNAME   router
gw              CNAME   router
```

Nota

OBSERVE el parámetro CNAME.

Es empleado para otorgar a un equipo un alias.

Concretamente sería:

<alias>* CNAME *<equipo>

En el fichero puede verse como al *router* se le ha puesto dos alias más: *gateway* y *gw*.

Verificamos que no haya ningún error en el fichero:

```
root@PDCC:/# named-checkzone central.local /etc/bind/db.central.local
zone central.local/IN: loaded serial 2010111101
OK
```

Al igual hacemos con el fichero de base de datos de la resolución de nombres inversa (***db.1.168.192***):

```
;
; BIND zone file for 192.168.1.xxx
;

$TTL    3D
@       IN      SOA     ns.central.local.    root.central.local. (
                2010111101      ; serial
                8H              ; refresh
                2H              ; retry
                4W              ; expire
                1D )            ; minimum
```

```
        NS      ns.central.local.    ; Nameserver address

160         PTR     PDCC.central.local
160         PTR     ns.central.local.
1           PTR     router.central.local
```

Igualmente verificamos que todo esté correcto:

```
root@PDCC:/# named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.1.168.192
zone 1.168.192.in-addr.arpa/IN: loaded serial 2008121701
OK
```

Finalmente, reiniciamos el servicio DNS:

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

Para dejar acabar con este apartado, sólo nos quedará modificar el fichero ***/etc/resolv.conf*** dejándolo de la siguiente forma:

```
domain central.local
search central.local
nameserver 127.0.0.1
```

Para verificar que todo funciona correctamente, podemos realizar las siguientes pruebas:

Comprobar la resolución de Nombres:

```
root@PDCC:/# nslookup PDCC
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:           PDCC.central.local
Address:        192.168.1.160
```

Comprobar la resolución de Aliases:

```
root@PDCC:/# nslookup gateway
Server:         127.0.0.1
Address:        127.0.0.1#53

gateway.central.local       canonical name = router.central.local.
Name:           router.central.local
Address:        192.168.1.1
```

Comprobar la resolución inversa (resolución de direcciones IP):

```
root@PDCC:/# nslookup 192.168.1.160
Server:         127.0.0.1
```

```
Address:        127.0.0.1#53

160.1.168.192.in-addr.arpa      name = ns.central.local.
160.1.168.192.in-addr.arpa      name = PDCC.central.local.1.168.192.in-addr.arpa.
```

Configuración BDC

Dado que la instalación de un servidor controlador secundario de dominio consiste en seguir exactamente los mismos pasos indicados que para el apartado anterior (Configuración de PDC), únicamente reflejaremos los cambios que deben hacerse.

Evidentemente, los cambios a realizar están únicamente relacionados con las direcciones IP y nombres del equipo en los diferentes ficheros de configuración tratados.

Nota

MUY IMPORTANTE: Aunque se modifican algunos atributos, hay uno que deberá ser exactamente igual. El SID deberá ser exactamente el mismo que el del servidor maestro.

Prácticamente en toda la instalación podemos aprovechar copiando del servidor principal los ficheros de configuración que sean extensos. De esta forma ahorraremos tiempos y esfuerzos innecesarios.

Servicio: OpenLDAP

En el caso de OpenLDAP, no es necesaria la modificación de ningún fichero de configuración. La instalación y configuración del servicio será idéntico al explicado anteriormente.

Servicio: Samba

En el caso de Samba, habrá que modificar el fichero ***/etc/samba/smb.conf*** concretamente los atributos siguientes:

```
realm = BDCC.central.local
preferred master = auto
domain master = auto
```

Por lo demás, la instalación se realiza exactamente igual.

Librerías Autenticación: NSS y PAM

Al igual que ocurre con OpenLDAP, la instalación de las librerías NSS y PAM se realizan de la misma forma que se ha explicado.

Nota

RECOMENDACIÓN: Para la instalación del BDC, es aconsejable seguir todos los pasos anteriores, tal y como se han marcado, teniendo en cuenta únicamente los atributos descritos en el apartado de BDC para cada servicio, en caso de que los hubiese.

Replicación entre Controladores de Dominio (PDC y BDC)

Replicación es el proceso de configuración de un directorio para que mantenga múltiples copias de sus datos en otros árboles sincronizadas en el tiempo.

En LDAP, la replicación es un modelo jerárquico, un servidor se considera el maestro, o proveedor, encargado de mantener la última versión de la información del directorio. Bajo el servidor maestro se encuentra uno o más servidores en la sombra (esclavos, replicas o consumidores). Un esclavo mantiene una réplica del árbol del servidor maestro y los clientes pueden realizar las consultas sobre uno de los esclavos. Por lo que los esclavos son de sólo lectura.

Lo primero que vamos a hacer es configurar un servidor como maestro. Este servidor escucha peticiones de sincronización de los esclavos y les envía las actualizaciones solicitadas. La funcionalidad de maestro está implementada en el "overlay" syncprov (proveedor de sincronización).

Paramos el servicio en ambos servidores:

```
root@BDCC:/# /etc/init.d/slapd stop
```

Modificaciones para Maestro

Lo primero es cargar el modulo y configurarlo.

Todas las modificaciones serán realizadas en el fichero ***/etc/ldap/slapd.conf.***

Añadimos la siguiente línea en negrita:

```
moduleload back_bdb
moduleload syncprov
```

Bajo los índices (*index*) añadimos lo siguiente:

```
index   entryCSN,entryUUID   eq
index   contextCSN           eq
```

El siguiente paso es cargar y configurar el overlay syncprov. Sólo existen dos directivas de configuración para este overlay, por lo que nuestra configuración quedaría de la siguiente manera:

```
access to *
    by dn.base="cn=admin,dc=organismo,dc=junta-andalucia,dc=es" read
    by * break

overlay syncprov
syncprov-checkpoint 100 10
```

Modificaciones para Esclavo

En el fichero ***/etc/ldap/slapd.conf:***

Añadimos la siguiente línea en negrita:

```
moduleload back_bdb
moduleload syncprov
```

Al final del fichero añadimos:

```
syncrepl rid=000
  provider=ldap://<ip_maestro>:389
  type=refreshAndPersist
  retry="5 5 300 +"
  searchbase="dc=central,dc=local"
  attrs="*,+"
  bindmethod=simple
  binddn="cn=admin,dc=central,dc=local"
  credentials=<clave>

updateref ldap://<ip_maestro>
```

Cambiar en el fichero ***/usr/local/etc/smbldap-tools/smbldap.conf***:

*masterLDAP="**<ip_maestro>**"*

Por último, arrancamos el servicio en ambos servidores nuevamente.

root@BDCC:/# /etc/init.d/slapd start

Para poder probar la replicación basta con crear nuevos usuarios desde *phpldapadmin* o desde los comandos de *samba* indicados en el apartado anterior y realizar una consulta mediante el comando ***ldapsearch*** a la nueva réplica.

Configuración Servidor Correo

El servidor de correo es sin lugar a dudas una de las partes más complicadas del proyecto, ya que son muchos factores los que influyen: usuarios, directorios, base de datos…

Para tener un entorno bastante completo necesitaremos numerosas utilidad es y diferentes servicios:

- ***Postfix*** como *MTA* principal
- ***Dovecot*** como soporte de los servicios *POP3* e *IMAP*
- ***MYSQL*** como base de datos donde se almacena usuarios, dominios, aliases…
- ***SpamAssasin*** como software de filtrado de spam (*anti-spam*)
- ***Clamav*** como antivirus
- ***Roundcube*** como servicio *webmail*
- ***PhpMyAdmin*** para administrar la base de datos *mysql*

Comencemos por la instalación de la paquetería necesaria:

```
root@SRVCorreo:/# apt-get install postfix
root@SRVCorreo:/# apt-get install mysql-server
root@SRVCorreo:/# apt-get install amavisd-new
root@SRVCorreo:/# apt-get install spamassassin clamav-daemon cpio arj zoo nomarch lzop
cabextract pax
root@SRVCorreo:/# apt-get install openssl
root@SRVCorreo:/# apt-get install libapache2-mod-php5 php5-mysql
root@SRVCorreo:/# apt-get install telnet
root@SRVCorreo:/# apt-get install ruby ruby1.8-dev irb rdoc rubygems
root@SRVCorreo:/# apt-get install dovecot-mysql dovecot-pop3d dovecot-imapd dovecot-
managesieved
root@SRVCorreo:/# apt-get install roundcube roundcube-plugins
root@SRVCorreo:/# apt-get install phpmyadmin
```

Dado que con la instalación de Postfix, Debian instala por defecto Exim como servicio de correo, lo eliminamos:

```
root@SRVCorreo:/# apt-get --purge remove 'exim4*'
```

Certificado (TLS)

Internet se ha convertido en un mal lugar para las empresas, desde el punto de vista de la seguridad.

Hardware y software, así como el personal técnico se encuentran entre el ordenador y el servidor de correo. Algunos de ellos pueden no ser de confianza. Y en casos extremos se paga incluso para espiar la empresa.

Por tanto, hoy en día es muy inseguro la publicación de cualquier servicio sin cifrar a través de Internet - especialmente cuando se trata de administrar su servidor y utilizarlo para su correo electrónico.

Considere que cualquier contraseña enviada a través de HTTP, por ejemplo, puede ser interceptada. Así que antes de utilizar PHPMyAdmin para enviar la contraseña de *root* de su base de datos, hagamos del servidor web Apache algo seguro.

La configuración de TLS no es algo difícil.

Vamos a crear la clave y el certificado que se utiliza para HTTPS webmail, POP3 seguro, IMAP y SMTP Secure Secure.

Hay varios tipos de certificados:

Tipo	Ventajas	Desventajas	Aplicación
Autofirmados	Sin costes. Creados rápidamente.	Los usuarios recibirán un mensaje de advertencia sobre el certificado no es de confianza.	Servidor de correo privado para entornos hogareños que no importa ignorar el mensaje de aviso sobre una identidad verificada.
Auto-firmado con la propia PKI	Sin costes. Puede crear otras certificaciones que sus usuarios consideran de confianza si tienen su certificado raíz instalado.	Tarda 15 minutos. Todos los usuarios deben instalar el certificado raíz como de confianza en sus equipos. Esto tiene sentido sólo si se va a distribuir automáticamente mediante herramientas de despliegue.	Servidor de correo privado en un ámbito algo mayor que no les importa la instalación del certificado raíz de una vez.
Certificado sin costo desde StartSSL	Sin costes. No es probable que los usuarios reciban advertencias.	Tarda 15 minutos.	Servidor de correo público.
Certificado de pago	Los usuarios no recibirán una advertencia.	Coste de 50€ a 200€ / año. Casi siempre el proceso de registro es largo. No se mejora la seguridad de las comunicaciones en modo alguno.	Para cualquier entorno que tenga buena economía.

Para esta implantación seleccionamos un certificado autofirmado, ya que no necesitamos nada más:

```
root@SRVCorreo:/# openssl req -new -x509 -days 3650 -nodes -newkey rsa:4096 -out
/etc/ssl/certs/mailserver.pem -keyout /etc/ssl/private/mailserver.pem
```

Se realizarán varias preguntas de carácter informativo. Ingresar lo que se desee. El único campo importante es el "Nombre común" que debe contener el nombre de host totalmente calificado (*fqdn*) que usted desea que el servidor sea conocido en Internet.

Finalmente asegúrese de que la clave secreta sólo es accesible por el usuario *'root'*:

```
root@SRVCorreo:/# chmod go= /etc/ssl/private/mailserver.pem
```

Habilitar HTTPS en Apache

Ahora que se tiene una clave válida y certificada se usará para el servidor web para hablar de *HTTPS* en lugar de *HTTP*.

Vaya a ***/etc/apache2/sites-available*** y busque el archivo "*default-ssl*". Es una plantilla de configuración buena para habilitar *HTTPS*. Editar y cambiar estas dos líneas:

```
SSLCertificateFile / etc / ssl / certs / mailserver.pem
SSLCertificateKeyFile / etc / ssl / private / mailserver.pem
```

Habilita la configuración de *SSL*:

```
root@SRVCorreo:/# a2ensite default-ssl
```

También se activa el módulo "*mod_ssl*":

```
root@SRVCorreo:/# ssl a2enmod
```

Reiniciar el servidor web *Apache*:

```
root@SRVCorreo:/# servicio apache2 reload
```

Si todo funciona correctamente, verá el mensaje "[ok]".

Ir a **https**://*<ip_servidor_Correo>*/ en un navegador web.

Deberá aparecer la famosa advertencia del certificado. Aceptamos el aviso y debe mostrarnos el funcionamiento correcto de *Apache* con un mensaje (*Works*!).

Si no funciona así, ejecute "*configtest apache2ctl*" para ver si Apache detecta cualquier problema. También puede ojear el archivo de registro ***/var/log/apache2/error.log*** para obtener más sugerencias sobre el problema.

Si queremos dejar redirigidas las peticiones HTTP a HTTPS de forma permanente, solo debemos editar el fichero ***/etc/apache2/sites-available/default*** e insertar:

```
Redirect permanent / https://<ip_servidor_correo>/
```

Preparando la Base de Datos

Accedemos a *phpmyadmin* (***https://<ip_servidor_correo>/phpmyadmin***):

Ingresamos con el usuario *root* y la contraseña pre-configurada en el asistente de instalación del servicio *mysql*.

Como se observa, *phpmyadmin* facilita mucho el trabajo de administración de base de datos gracias a lo intuitivo de su interfaz.

Sin embargo utilizaremos scripts en lenguaje SQL para la creación de la base de datos, así como las tablas, usuarios, etc.

Creación de nueva base de datos:

```
CREATE DATABASE 'mailserver';
```

Por razones de seguridad, añadimos un usuario con menos privilegios que el *root*. En este caso se utilizará el asistente para poder generar la contraseña:

Haga clic en la base de datos "*mailserver*" en la columna izquierda. Luego haga clic en la pestaña "*privilegios*". Luego en "*Crear un nuevo usuario*". Rellene el cuadro de diálogo:

Indicar el "*Nombre de usuario*" en "*servidor de correo*".

Y como "*Host*", seleccione "*Local*" para que el campo de texto se convierte en "*localhost*".

Escriba la contraseña y abajo su verificación. Haga clic en el botón "*Generar*".

Desplácese hacia abajo en la página y haga clic en el último botón "*Continuar*".

Por razones de seguridad usted debe quitar todos los privilegios de acceso, excepto el privilegio "*SELECT*". Por tanto, dentro de la sección "*privilegios específicos de base de datos*", primero haga clic en "Deseleccionar todo" y luego simplemente active la casilla de "*SELECT*".

Ahora haga clic en "Continuar" nuevamente.

En la base de datos recién creada, habrá que crear tablas que almacenan información sobre dominios, redirecciones y los buzones de los usuarios.

En primer lugar crear una tabla para la lista de dominios virtuales que desea ser anfitrión:

```
CREATE TABLE `virtual_domains` (
  `id` int (11) NO AUTO_INCREMENT NULL,
  `nombre` varchar (50) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE = InnoDB DEFAULT CHARSET = utf8;
```

La siguiente tabla contiene información sobre las cuentas de usuario reales. Cada usuario tiene un nombre de usuario y contraseña. Se usará para acceder al buzón POP3 o IMAP, iniciar sesión en el servicio de correo web o para enviar correo ("relay") si no están en tu red local. Dado que los usuarios tienden a olvidar fácilmente las cosas la dirección de correo electrónico del usuario también se utiliza como el nombre de usuario de inicio de sesión. Vamos a crear la tabla de usuarios:

```
CREATE TABLE `virtual_users` (
  `id` int (11) NO AUTO_INCREMENT NULL,
  `int domain_id` (11) NOT NULL,
  `varchar` password (32) NOT NULL,
  `email` varchar (100) NOT NULL,
  PRIMARY KEY ( `id`),
  UNIQUE `email` email `), tecla` (
  FOREIGN KEY (domain_id) Referencias virtual_domains (id) ON DELETE CASCADE
) ENGINE = InnoDB DEFAULT CHARSET = utf8;
```

Y por último se necesita una tabla para los *aliases* (redirecciones de correo electrónico desde una cuenta a otra):

```
CREATE TABLE `virtual_aliases` (
  `id` int (11) NO AUTO_INCREMENT NULL,
```

```
  `int domain_id` (11) NOT NULL,
  `fuente` varchar (100) NOT NULL
  `destino` varchar (100) NOT NULL,
  PRIMARY KEY ( `id`),
  FOREIGN KEY (domain_id) Referencias virtual_domains (id) ON DELETE CASCADE
) ENGINE = InnoDB DEFAULT CHARSET = utf8;
```

Poblamos la base de datos:

```
INSERT INTO `mailserver` `` virtual_domains (.
  `,`id
  `nombre`
)
VALUES (
  '1 ',' central.local '
);
INSERT INTO `mailserver`. `virtual_users` (
  `id`,
  `domain_id`,
  `password`,
  `` email
)
VALUES (
  '1 ', '1', MD5 ('clave'), ‘fgomez@central.local'
);
INSERT INTO `mailserver`. `virtual_aliases` (
  `,`id
  `,`domain_id
  `origen`,
  `` destino
)
VALUES (
  '1 ', '1', 'agomez@central.local', 'fgomez@central.local '
);
```

Conexión de Postfix con la base de datos

Ahora es el momento de hacer uso de la base de datos anteriormente poblada.

El punto de entrada para todo el correo electrónico en su sistema es Postfix. Así que tenemos que decirle a Postfix dónde encontrar la información almacenada - base de datos. Comencemos diciendo qué dominios virtuales existen.

Para hacer que Postfix utilice MySQL para definir una asignación necesitamos un archivo '.cf' (archivo de configuración).

Creamos un archivo llamado ***/etc/postfix/mysql-virtual-mailbox-domains.cf*** para el mapeo *virtual_mailbox_domains* que contiene:

```
user = mailuser
password = <clave mailuser>
hosts = 127.0.0.1
dbname = mailserver
query = SELECT 1 FROM virtual_domains WHERE name='%s'
```

Nota

ADVERTENCIA: Puede tener la tentación de escribir "*localhost*" en lugar de "*127.0.0.1*" en el apartado hosts. No lo haga, porque en efecto, hay una diferencia en este contexto. "*Localhost*" hará que *Postfix* busque el archivo socket de *MySQL* y no podrá encontrar nada en */var/spool/postfix*, ya que es en */var/run/mysqld/mysqld.sock* dónde apunta por defecto. Pero si le indicas *127.0.0.1* tal y como se indicaba utilizará una conexión *TCP* al puerto *3306*.

Ahora se indica a Postfix que utilice este mapeo de base de datos:

```
root@SRVCorreo:/# postconf -e virtual_mailbox_domains=mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
```

Postfix ahora buscará la tabla *virtual_domains* para averiguar si "*central.local*" es un dominio de correo virtual.

Tras haber configurado el dominio "*central.local*" anteriormente, podemos consultar ahora si se puede encontrar el dominio en la base de datos:

```
root@SRVCorreo:/# postmap -q central.local mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
```

Si todo está bien deberá obtener '1 'como resultado.

Ahora van a definirse los *virtual_mailbox_maps*. Son mapeos de direcciones de correo electrónico (lado izquierdo) a la ubicación del buzón del usuario en el disco duro (lado derecho). Si ha guardado el correo entrante en el disco duro utilizando la función de agente de entrega virtual de *Postfix*, entonces la consulta deberá averiguar la ruta del buzón.

Sin embargo, en esta configuración la entrega se hace por *LDA* de *Dovecot* (agente de entrega local), por lo que *Postfix* no intervendrá en la resolución de la ruta del buzón. *Postfix* sólo necesita comprobar si una dirección de correo electrónico es válida o no. Similar a la anterior que necesita una consulta *SQL* para buscar una dirección de correo electrónico. Igualmente devuelve "*1*".

A continuación, debe de crearse otro fichero de configuración ". cf" para decir a *Postfix* la consulta SQL para la tabla. Además de la dirección de correo electrónico también es importante obtener la contraseña del usuario en el futuro. Como la ruta del buzón del usuario está indicada no es importante obtener esta información de la base de datos. La estructura de directorios siempre será ***/var/vmail/$DOMINIO/$USER***. Así, por ejemplo, de *fgomez* sería */var/vmail/central.local/fgomez* .

Teniendo esto claro y viendo las cosas de forma más simple tras esta breve introducción de este apartado, finalmente cree el fichero ***/etc/postfix/mysql-virtual-mailbox-maps.cf*** con el siguiente contenido:

```
user = mailuser
password = <clave mailuser>
hosts = 127.0.0.1
dbname = mailserver
query = SELECT 1 FROM virtual_users WHERE email='%s'
```

Al igual que anteriormente, se indica a Postfix que utilice este mapeo:

```
root@SRVCorreo:/# postconf -e virtual_mailbox_maps=mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
```

Comprobamos si Postfix lo contempla correctamente consultando dónde está el directorio de buzones de un usuario. Sería:

```
root@SRVCorreo:/# postmap -q fgomez@central.local mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
```

Usted debe obtener " 1 " como respuesta. Esto significará que la dirección de correo es un usuario de un buzón virtual existente en el servidor.

Tenemos otro fichero más, que también es importante.

En este caso se trata de los Aliases de las direcciones de correo.

El fichero *virtual_alias_maps* se utiliza para la transmisión de mensajes de correo electrónico desde una dirección de correo electrónico a otro. Es posible nombrar múltiples destinos para un mismo origen. En la base de datos, esto se consigue mediante el uso de diferentes filas.

Cree otro archivo tipo "cf.": ***/etc/postfix/mysql-virtual-alias-maps.cf***

```
user = mailuser
password = <clave mailuser>
hosts = 127.0.0.1
dbname = mailserver
query = SELECT destination FROM virtual_aliases WHERE source='%s'
```

Indicamos y comprobamos en Postfix:

```
root@SRVCorreo:/# postconf -e virtual_alias_maps=mysql:/etc/postfix/mysql-virtual-alias-maps.cf
root@SRVCorreo:/# postmap -q agomez@central.local mysql:/etc/postfix/mysql-virtual-alias-maps.cf
fgomez@central.local
```

Como vemos, obtendremos el destino fijado para la dirección de correo indicada en la consulta.

Configuración de Dovecot

Antes de llegar a la configuración real, por razones de seguridad, se recomienda crear un nuevo usuario del sistema propietario de todos los buzones virtuales.

Los siguientes comandos de *shell* crearán un grupo de sistemas "*vmail*" con *GID 5000* y un usuario del sistema "*vmail*" con *UID 5000*.

Nota

ASEGURESE de que estos *UID* y *GID* no están siendo utilizados por otros - el número puede ser cualquiera entre *1000* y *65000.*

```
root@SRVCorreo:/# groupadd -g 5000 vmail
root@SRVCorreo:/# useradd -g vmail -u 5000 vmail -d /var/vmail -m
```

También debe de estar seguro de que el directorio posee los permisos adecuados:

```
root@SRVCorreo:/# chown -R vmail:vmail /var/vmail
root@SRVCorreo:/# chmod u+w /var/vmail
```

Los archivos de configuración de *Dovecot* se encuentran bajo el directorio ***/etc/dovecot***. En versiones anteriores sólo existían dos ficheros de configuración. Sin embargo, en la versión de *Debian* 7, *Dovecot* dispone de un nuevo directorio "*conf.d*" que contiene cerca de 30 archivos de configuración adicionales. Todos estos archivos se unen entre sí para formar la configuración completa. Esto se consigue gracias a la declaración de todos esos ficheros mediante la siguiente línea en el archivo *dovecot.conf*:

```
!Include conf.d/*.conf
```

Esta línea consigue cargar todos los archivos los ficheros de configuración encontrados en */etc/dovecot/conf.d/.* Los ficheros vienen ordenados: Por ejemplo, "*10-auth.conf*" se carga por la primera y "*90-quota.conf*" la última.

La gran ventaja es que se puede editar o reemplazar partes de la configuración sin tener que sobrescribir la configuración completa.

La desventaja es que si va a actualizar su servidor de correo desde una versión anterior de *Debian* tiene que reconfigurar absolutamente todo.

Los ficheros de configuración a editas son los siguientes:

10-auth.conf

Si se pretende que los usuarios utilicen *Microsoft Outlook* como cliente de correo electrónico que usted debe habilitar la opción de mecanismo de autenticación "*LOGIN*", además del mecanismo estándar "*PLAIN*":

```
auth_mechanisms = plain login
```

Estas son formas de texto plano (sin cifrar) para transmitir la contraseña de un usuario de correo. Sin embargo, no es de preocupar ya que por defecto *Dovecot* establece "*disable_plaintext_auth = yes*" que garantiza que cada conexión será cifrada usando *TLS*.

Al final de este archivo se encuentran varios *backends* de autenticación que usa *Dovecot*. Por defecto se usarán los usuarios del sistema (que se enumeran en */etc/passwd*). Pero en este caso se desea usar el gestor de base de datos *MySQL*. Por tanto habrá que cambiarlo así:

```
#!Include auth-system.conf.ext
!Include auth-sql.conf.ext
#!Include auth-ldap.conf.ext
#!Include -auth passwdfile.conf.ext
#!Include -auth checkpassword.conf.ext
#!Include auth-vpopmail.conf.ext
#!Include auth-static.conf.ext
```

Tras cambiar el tupo de autenticación, habrá que modificar el propio fichero de configuración SQL nuevo:

auth-sql.conf.ext

Comente (añadir "#" delante) la sección estándar "*userdb*".

A continuación, añadir:

```
userdb {
  driver = static
 args = uid=vmail gid=vmail home=/var/vmail/%d/%n
}
```

Nota

ADVERTENCIA: Sólo debe haber una sección *'userdb'*.

OJO: No confundir esta sección con otra muy similar que utiliza "*%u*" en lugar de "*%d/%n*". Este esperaría un sistema de archivos de */var/vmail/usuario@dominio* en lugar de */var/vmail/$DOMAIN /$USER*.

10-mail.conf

Cambie el ajuste de *mail_location*:

```
mail_location = maildir:/var/vmail/%d/%n/Maildir
```

Este es el directorio donde *Dovecot* buscará los mensajes de correo electrónico de un usuario específico. La variable "*%d*" es la parte de dominio y "*%n*" es la parte del usuario de una dirección de correo electrónico. Así que, por ejemplo, para *fgomez@central.local*, esto nos lleva "*/var/vmail/central.local/fgomez/Maildir*".

El formato *maildir* especifica que cada correo electrónico está representado por un único archivo en el disco, con un formato de nombre de archivo definido. Un formato más antiguo y menos flexible es el formato "*mbox*", que almacena todos los mensajes de correo electrónico en una carpeta en un solo archivo, lo que hace que la eliminación de mensajes de correo electrónico sea un proceso lento porque los archivos *mbox* grandes tendrán que ser leídos y escritos para cada vez.

10-master.conf

Este archivo de configuración se ocupa de servicios que permiten la comunicación con otros procesos. Por ejemplo, se activa o desactiva *POP3* o *IMAP*. No te preocupes por los puertos estándar *TCP* no cifradas *110* (para *POP3*) y *143* (para *IMAP*). Se pueden mantener accesibles. Si un usuario se conecta a estos puertos tendrán que emitir un comando *STARTTLS* para cambiar al modo de cifrado antes de poder enviar su contraseña.

Así que la mayoría de los ajustes no tienen que ser cambiado. Sin embargo se requiere un cambio en la sección "*service auth*" ya que queremos que *Postfix* autorice a *Dovecot* como servicio de autenticación. Esto es lo que se debe introducir:

```
# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
  mode = 0660
  user = postfix
  group = postfix
}
```

10-ssl.conf

A principios de este apartado fueron creados una clave y un archivo de certificado para cifrar la comunicación con *POP3*, *IMAPs* y *HTTPS* entre usuarios y el servidor de correo. Aquí es dónde se indica a *Dovecot* dónde encontrar dichos ficheros:

```
ssl_cert = </etc/ssl/certs/mailserver.pem
ssl_key = </etc/ssl/private/mailserver.pem
```

15-lda.conf

En este archivo de configuración se debe habilitar el plugin "*sieve*". *Sieve*, en pocas palabras, permite administrar reglas de correo electrónico del servidor. Una regla consiste en las condiciones y acciones. Por ejemplo, una regla sería la detección de una dirección de correo electrónico de un remitente concreto para mover dichos correos a una carpeta. Estas reglas las almacena el propio servidor *Dovecot* y las ejecuta automáticamente.

Busque la sección "protocol lda" al final del archivo. Añadir "*sieve*" de la lista de plugins de correo:

```
lda protocol {
  mail_plugins = $mail_plugins sieve
}
```

/etc/dovecot/dovecot-sql.conf.ext

Indica a *Dovecot* cómo acceder a la base de datos *MySQL* y dónde encontrar la información sobre los usuarios de correo electrónico/cuentas. Asegúrese de que contenga las siguienteslíneas (puede agregarlas al final del archivo si se desea):

```
driver = mysql
connect = host=127.0.0.1 dbname=mailserver user=mailuser password=<clave mailuser>
default_pass_scheme = PLAIN-MD5
password_query = SELECT email as user, password FROM virtual_users WHERE email='%u';
```

¿Qué significan estas líneas?:

driver: tipo de base de datos

connect: servidor dónde encontrar la base de datos *MySQL* y cómo usarlo (nombre de usuario, contraseña)

default_pass_scheme: formato en el que las contraseñas son almacenadas

password_query: sentencia *SQL* que devuelve al usuario (cuenta de correo) y la contraseña (hash MD5) de la base de datos. Cada vez *Dovecot* necesita comprobar la contraseña de un usuario de correo electrónico se ejecutará esta consulta.

Para finalizar con *Dovecot*, corregiremos los permisos del fichero */etc/dovecot/dovecot.conf* para que sólo el usuario *vmail* pueda acceder a la configuración de *Dovecot*. La razón es que *Postfix* inicia el agente de entrega con permisos de *vmail*:

```
root@SRVCorreo:/# chgrp vmail /etc/dovecot/dovecot.conf
root@SRVCorreo:/# chmod g+ r /etc/dovecot/dovecot.conf
```

También debe asegurarse de que sólo *root* puede acceder al archivo de configuración de SQL para que nadie más pueda leer las contraseñas de acceso a base de datos:

```
root@SRVCorreo:/# chown root:root /etc/dovecot/dovecot-sql.conf.ext
root@SRVCorreo:/# chmod go= /etc/dovecot/dovecot-sql.conf.ext
```

Reiniciar Dovecot:

```
root@SRVCorreo:/# servicio restart palomar
```

Observa el fichero de log */var/log/mail.log*. Si muestra lo siguiente, todo fue bien:

```
…dovecot: master: Dovecot v2.1.7 starting up (core dumps disabled)
```

Conexión Postfix-Dovecot

Ahora configuraremos qué hacer con el correo electrónico. Para hacer que *Postfix* use *Dovecot* como agente para *POP3* e *IMAP* tendrá que añadir un servicio al fichero ***/etc/postfix/master.cf***:

```
dovecot unix - n n - - pipe flags=DRhu user=vmail:vmail
argv=/usr/lib/dovecot/dovecot-lda -f ${sender} -d ${recipient}
```

Reinicie Postfix:

```
root@SRVCorreo:/# servicio postfix restart
```

Compruebe el final del archivo /var/log/mail.log si hay errores. Se debería leer:

```
postfix/master[…]: daemon started -- version 2.9.6, configuration /etc/postfix
```

También asegúrese de que Postfix usa ese servicio para la entrega virtual, añadiendo estas líneas al ***/etc/postfix/main.cf***:

```
virtual_transport = palomar
dovecot_destination_recipient_limit = 1
```

De esta forma ahora Postfix pasará los correos electrónicos entrantes a los usuarios virtuales.

Test: Entrega de correo electrónico

A continuación realizaremos una prueba de los servicios de entrega de correo electrónico para verificar que todo está correcto llegados a este punto.

A estas alturas, el directorio */var/vmail* aún debe estar vacío. Usted puede obtener una lista de todos los archivos y directorios dentro ejecutando:

```
root@SRVCorreo:/# find /var/vmail
```

Probablemente no haya nada, excepto el directorio "*lost+found*" si, y sólo si, */var/vmail* está en una partición separada.

Si ha poblado con datos de prueba la base de datos en la sección anterior, preparación de la base de datos, deberá tenerse "*central.local*" configurado como un dominio virtual y "*fgomez@central.local*" como usuario en ese dominio.

Abra una nueva ventana de terminal y ejecute:

```
root@SRVCorreo:/# tail -f /var/log/mail.log
```

Esto será para ver lo que está haciendo el servidor de correo en tiempo real. Ahora vamos a enviar un correo electrónico a *fgomez*. Una manera sencilla de crear y enviar un correo electrónico es la de texto plano usando el comando "*mail*".

Desde otro terminal:

```
root@SRVCorreo:/# echo test | mail fgomez@central.local
```

Si todo funciona como se espera el fichero *mail.log* mostrará una gran cantidad de información técnica acerca de la entrega de correo electrónico. De esta manera:

```
Nov 20 17:42:32 SRVCorreo postfix/pickup[22273]: A6F8EB55: uid=0 from=<root>
Nov 20 17:42:32 SRVCorreo postfix/cleanup[22582]: A6F8EB55: message-
id=<20131020154232.A6F8EB55@SRVCorreo.localdomain>
Nov 20 17:42:32 SRVCorreo postfix/qmgr[22274]: A6F8EB55: from=<root@SRVCorreo.central.local>,
size=287, nrcpt=1 (queue active)
Nov 20 17:42:32 SRVCorreo dovecot: auth-worker(22635): mysql(127.0.0.1): Connected to database
mailserver
Nov 20 17:42:32 SRVCorreo dovecot: lda(fgomez@central.local): msgid=<20131020154232.A6F8EB55@
SRVCorreo.localdomain>: saved mail to INBOX
Nov 20 17:42:32 SRVCorreo postfix/pipe[22586]: A6F8EB55: to=<fgomez@central.local>, relay=dovecot,
delay=0.14, delays=0.04/0/0/0.1, dsn=2.0.0, status=sent (delivered via dovecot service)
Nov 20 17:42:32 SRVCorreo postfix/qmgr[22274]: A6F8EB55: removed
```

Si observamos el directorio */var/vmail*, se han creado la siguiente pila de directorios, tal y como se tenía previsto tras configurar los ficheros de configuración:

/var/vmail/
/var/vmail/central.local/
/var/vmail/central.local/fgomez
/var/vmail/central.local/fgomez/Maildir
/var/vmail/central.local/fgomez/Maildir/dovecot.index.log
/var/vmail/central.local/fgomez /Maildir/cur
/var/vmail/central.local/fgomez /Maildir/dovecot-uidvalidity.5263f9e8
/var/vmail/central.local/fgomez /Maildir/new
/var/vmail/central.local/fgomez/Maildir/new/1382283752.M737526P22632.sirius,S=352,W=362
/var/vmail/central.local/fgomez /Maildir/dovecot-uidvalidity
/var/vmail/central.local/fgomez /Maildir/tmp
/var/vmail/central.local/fgomez /Maildir/dovecot-uidlist
/var/vmail/central.local/fgomez /Maildir/dovecot.index.cache

Para acceder y visualizar el correo electrónico recibido, de momento, ya que aún no se ha configurado un cliente *Webmail*, únicamente deberemos abrir dicho fichero (marcado de negrita) con cualquier editor de texto.

Autenticación SMTP en Postfix

La autenticación *SMTP* en *Postfix* siempre fue anteriormente una verdadera molestia. Se hacía a través de *SASL* (*Capa de simple autenticación y seguridad*), que fue una vez parte del servidor de correo *Cyrus*. Era casi imposible de depurar y lanzaba mensajes de error que eran bastante confusos.

Afortunadamente hoy en día podemos hacer que *Postfix* solicite a *Dovecot* la verificación del nombre de usuario y contraseña. Como a estas alturas ya se ha configurado parte de autenticación de *Dovecot* lo convierte en algo realmente fácil. *Postfix* sólo necesita alguna configuración adicional.

En su fichero de configuración principal (*main.cf*) *añadimos*:

```
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yesí
smtpd_tls_security_level = may
smtpd_tls_auth_only = yes
smtpd_tls_cert_file = /etc/ssl/certs/mailserver.pem
smtpd_tls_key_file = /etc/ssl/private/mailserver.pem
smtpd_recipient_restrictions = "\
 permit_mynetworks \
 permit_sasl_authenticated \
 reject_unauth_destination"
```

smtpd_sasl_auth_enable permite la autenticación *SMTP* completa.

smtpd_recipient_restrictions define reglas que se comprueban después de que el usuario remoto envía la línea *RCPT TO* durante el diálogo *SMTP*. En este caso se permite la retransmisión si:

permit_mynetworks: el usuario está en la red local (mynetworks)

ó

permit_sasl_authenticated: si el usuario está autenticado

ó

reject_unauth_destination: el correo está destinado a un usuario de un dominio que es un dominio local o virtual en este sistema (*mydestination*, *virtual_alias_domains* o *virtual_mailbox_domains*).

smtpd_tls_security_level está establecido en "*may*" para habilitar el cifrado TLS al enviar el correo electrónico, el nombre de usuario y sobre todo la contraseña. Este previene que los usuarios envien sus contraseñas sin cifrar a través de Internet.

Aunque los correos electrónicos puedan ser entregados sin cifrar desde otros servidores, debemos asegurarnos de que los usuarios no envían accidentalmente (o por ignorancia) sus

contraseñas sin cifrar a través de Internet. Eso es lo que hacemos cumplir usando "*smtpd_tls_auth_only = yes*".

Para autenticarnos vía *SMTP*, utilizaremos conexión *Telnet* por el puerto 25:

```
root@SRVCorreo:/#  telnet localhost smtp
```

El servidor se le dejó en:

```
Tratando 127.0.0.1 ...
Connected to localhost.
Escape character is '^]'.
220 ESMTP Postfix mailtest (Debian / GNU)
```

Saludamos al entrar:

```
ehlo central.local
```

Postfix presentará una lista de las características que están disponibles durante el diálogo SMTP:

```
250-mailtest
250-PIPELINING
250 TAMAÑO 10.240.000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

Tras la lista, puede observarse que hay una importante línea que no se encuentra, línea que la autenticación:

250-AUTH PLAIN LOGIN

Le indicamos a *Postfix* que sólo permitiese la autenticación cuando la conexión estaba cifrada, por tanto, no se ofrecerá autenticación a través de texto plano.

Para salir de *Telnet* pulsamos *Ctrl+'5'* y luego escribiremos ***Quit***.

Webmail RoundCube

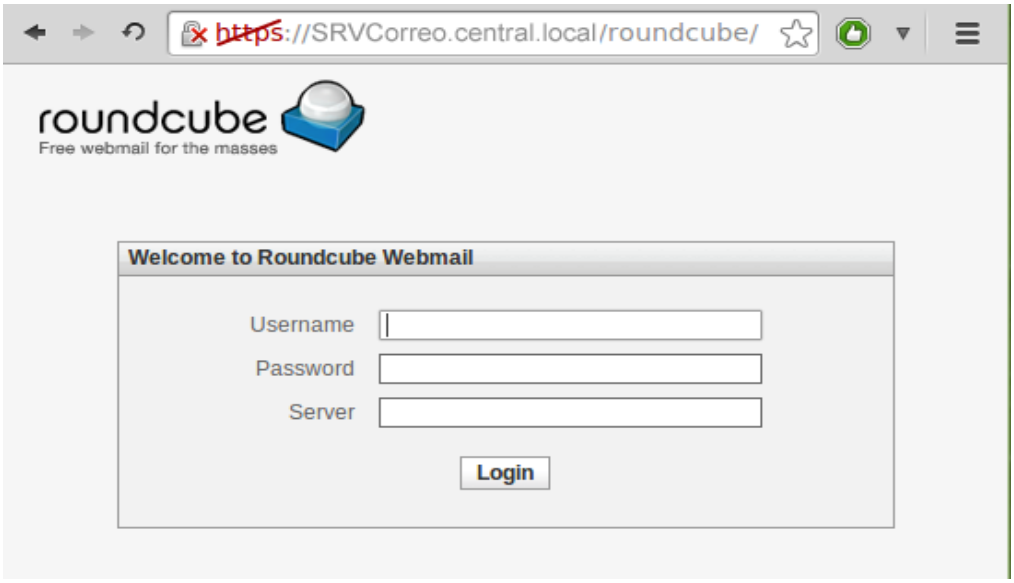
Vamos a configurar *RoundCube* como un software de correo web. Es una aplicación web escrita en *PHP* que ofrece una interfaz web fácil de usar y que se comunica a través de *IMAP* con cualquier servidor de correo.

Si el servidor de correo sólo se va a utilizar para esto, y la única web que tendrá será la del propio webmail, debe descomentar las directivas "Alias" en el archivo ***/etc/apache2/conf.d/roundcube*** y reiniciar Apache:

```
root@SRVCorreo:/# reinicio apache2ctl
```

Probamos la conexión a la interfaz gráfica a través de un navegador web:

https://SRVCorreo.central.local/roundcube/



Podremos acceder con cualquier usuario, por ejemplo, el que hemos creado "*fgomez*".

La configuración para *RoundCube* es la siguiente:

Vamos a editar el archivo de configuración ***/etc/roundcube/main.inc.php*** e incorporan los siguientes cambios:

Desactivar el campo "Servidor" y siempre utiliza el servidor local utilizando IMAP.

```
Rcmail_config ['default_host'] = 'localhost';
```

Asegurar que no dejamos accidentalmente a los usuarios enviar sus datos de acceso a través de una conexión HTTP insegura.

```
Rcmail_config ['force_https'] = true;
```

Configuración Servidor Ficheros

El servidor de ficheros a montar es algo básico.

Ha de tenerse en cuenta que existen multitud de posibilidades en cuanto a software utilizado, medidas de complejidad y seguridad, etc…

Sin embargo, lo explicado aquí marca la configuración de este tipo de equipos para una empresa. Siempre hay posibilidad de ampliar las funcionalidades.

Probaremos con dos ejemplos de clientes: uno bajo *Windows* y otro bajo *Linux*.

Algo que debe tenerse en cuenta es que un servidor de ficheros necesitará sobre todo bastante capacidad de almacenamiento, aunque también memoria *RAM* y procesador suficientes si la empresa consta de muchos empleados.

Hay una serie de servicios necesarios y prácticamente comunes para todas las implantaciones.

Servicio Samba

Como ya hemos visto anteriormente, sin más detalles procedemos a la instalación del servicio Samba:

```
root@SRVFich:/# apt-get install samba
```

Procedemos a crear los usuarios, asignando nombre y número de identificación por usuarios de la siguiente manera.

```
root@SRVFich:/# adduser -system -no-create-home -uid 600 clientexp
root@SRVFich:/# adduser -system -no-create-home -uid 601 clienteubuntu
```

Este comando lo repetiríamos de acuerdo al número de usuarios que queremos crear, con la variante que el número (*uid* incrementaría).

Comprobamos que los usuarios se añadieron correctamente.

```
root@SRVFich:/# cat /etc/passwd | grep clientexp
root@SRVFich:/# cat /etc/passwd | grep clienteubuntu
```

Añadimos los usuarios a samba de la siguiente manera.

```
root@SRVFich:/# smbpasswd -a clientexp
root@SRVFich:/# smbpasswd -a clientexp
```

Le asignamos una contraseña a cada usuario, y se verifica confirmándolo.

Procedemos a la configuración del archivo de samba ***/etc/samba/smb.conf***, dónde se configurara el recurso compartido.

Nos ubicamos en las últimas líneas para poder agregar la siguiente configuración:

```
[repositorio]
comment=Servicio Repositorio corporativo
path=/mnt/repositorio
read only=yes
browseable=yes
write list=clientexp,clientelinux
valid users=clientexp,clientelinux
directory mask=0775
create mask=064
```

Nota

RECUERDEN que pueden agregar cuantos recursos quieran compartir. En este caso únicamente compartimos un directorio principal que hará como repositorio de toda la empresa.

Tras esto, dicho directorio debe existir en el sistema:

```
root@SRVFich:/# mkdir /mnt/sambademo
root@SRVFich:/# chmod 777 /mnt/sambademo
```

Lo siguiente será hacer el testeo del archivo de configuración para ver si está o no correcto, ejecutando el siguiente comando ya conocido:

```
root@SRVFich:/# testparm
```

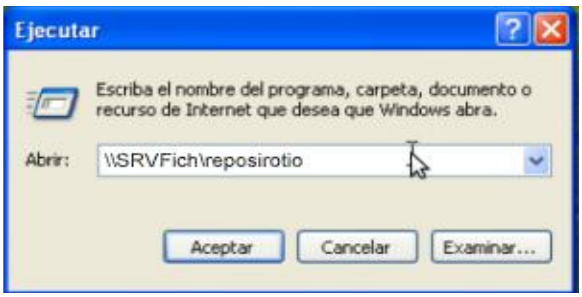
Si no muestra errores, reiniciamos el servicio:

```
root@SRVFich:/# /etc/init.d/samba restart
```

Conexión Cliente: Windows

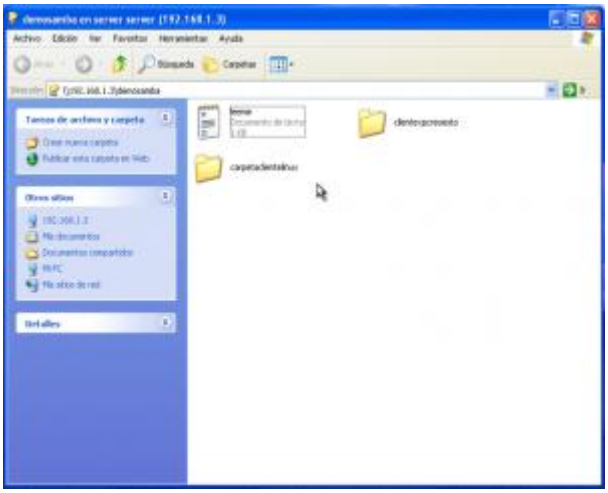
Para ingresar a la carpeta compartida desde samba, hacemos lo siguiente; clic en *Inicio→Ejecutar*

Colocamos lo siguiente en el cuadro de dialogo.



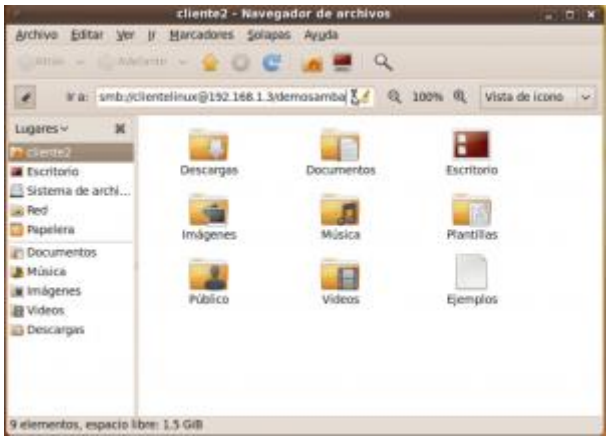
Nos pedirá nombre de usuario y contraseña para poder ingresar (recuerden que es la que establecimos en samba, no la del usuario de Windows)

Ahora podremos ver los archivos de dicha carpeta, así como crear carpetas y documentos.



Conexión Cliente: Linux

Como primer paso abrimos la carpeta personal del usuario y para poder ver la barra de direcciones en el explorador de archivos; hacemos la siguiente combinación de teclas. **[CTRL +L]** y lo veremos tal cual se muestra a continuación, y pondremos lo siguiente.



Escribimos la siguiente sintaxis.

smb://clientelinux@SRVFich/repositorio

Nos pedirá la contraseña.

Nos mostrara la carpeta compartida y montada al lado izquierdo del explorador como cualquier otra unidad.

Servicio NFS

Para los casos de sistemas Linux, otra posibilidad, además de emplear Samba, es acceder al repositorio empleando *NFS*.

NFS (*sistema de archivos de red*: «*Network File System*») es un protocolo que permite acceso remoto a un sistema de archivos a través de la red. Todos los sistemas Unix pueden trabajar con este protocolo; cuando se involucran sistemas Windows, debe utilizar Samba en su lugar.

NFS es una herramienta muy útil, pero debe tener en cuenta sus limitaciones especialmente en cuestiones de seguridad: todos los datos pasan a través de la red sin cifrar (un *sniffer* puede interceptarlos). El servidor fuerza restricciones de acceso basado en la dirección IP del cliente (que igualmente puede ser falsificada por un atacante una vez se encuentra en la red local de la empresa). Además, cuando se provee acceso a una máquina cliente a un espacio NFS compartido mal configurado, el usuario *root* del cliente puede acceder a todos los archivos en el espacio compartido, ya que el servidor confía en el nombre de usuario que recibe del cliente (esta es una limitación histórica del protocolo).

Para mejorar la seguridad del servicio NFS, nos centramos en los ficheros ***/etc/default/nfs-kernel-server*** y ***/etc/ default/nfs-common***.

Si concretamos algo más, el fichero deberá ***/etc/default/nfs-kernel-serve*** quedar:

```
# Cantidad de servidores a iniciar
RPCNFSDCOUNT=8
# Opciones para rpc.mountd
RPCMOUNTDOPTS="-p 2048"
```

Y el fichero ***/etc/ default/nfs-common***:

```
# Opciones para rpc.statd.
#   ¿Debería rpc.statd escuchar en un puerto específico?
#   En ese caso, defina esta variable como un parámetro de statd como: "--port 1000".
STATDOPTS="-p 2046 -o 2047"

# ¿Está _seguro_ que su núcleo necesita o no un demonio lockd?
# En ese caso, defina esta variable como "yes" o "no".
NEED_LOCKD=
```

Reiniciamos ambos servicios:

```
root@SRVFich:/# /etc/default/nfs-kernel-server restart
root@SRVFich:/# /etc/ default/nfs-common restart
```

Una vez que realizó estos cambios y reinició los servicios, ***rpc.mountd*** utilizará el puerto *2048*; ***rpc.statd*** escuchará en el puerto *2046* y utilizará el puerto *2047* para conexiones salientes.

El servicio ***lockd*** es gestionado por un hilo de núcleo (proceso liviano). Esta funcionalidad está compilada como un módulo en los núcleos *Debian*. El módulo tiene dos opciones que permiten utilizar siempre el mismo puerto: *nlm_udpport* y *nlm_tcpport*.

Para que se utilicen siempre estas opciones, debe existir un archivo /***etc/modprobe.d/lockd*** como el siguiente:

```
options lockd nlm_udpport=2045 nlm_tcpport=2045
```

Una vez que están definidos estos parámetros resulta más sencillo controlar el acceso al servicio *NFS* desde el firewall de una forma específica filtrando el acceso a los puertos *111* y desde el *2045* al *2049* (tanto *UDP* como *TCP*).

Para finalizar, únicamente necesitamos configurar el directorio compartido NFS.

El archivo de configuración del servidor *NFS*, ***/etc/exports***, enumera los directorios que estarán disponibles en la red (compartidos/exportados). Para cada espacio compartido *NFS*, sólo tendrán acceso las máquinas especificadas.

Puede obtener un control más detallado con unas pocas opciones. La sintaxis para este archivo es bastante simple:

```
<ruta_completa_directorio_compartido> <maquina1>(<opcion1>,<opcion2>,...)  <maquina2>(...) ...
```

Un ejemplo sería:

```
/mnt/repositorio   ubuntu1(fsid=0,rw,root_squash,sync,no_subtree_check)
```

Puede identificar cada máquina mediante su nombre *DNS* o su dirección *IP*. También puede especificar conjuntos completos de máquinas utilizando una sintaxis como *.central.local o un rango de direcciones *IP 192.168.0.0/255.255.255.0* o *192.168.0.0/24*.

De forma predeterminada (o si utiliza la opción ro), los directorios están disponibles sólo para lectura. La opción ***rw*** permite acceso de lectura y escritura. Los clientes NFS típicamente se conectan desde un puerto restringido sólo a *root* (en otras palabras, menor a *1024*). Puede eliminar esta restricción con la opción ***insecure*** (la opción ***secure*** es implícita, pero puede hacerla explícita para más claridad).

De forma predeterminada, el servidor sólo responderá consultas *NFS* cuando se complete la operación actual de disco (la opción ***sync***). Puede desactivar esto con la opción ***async***. Las escrituras asíncronas aumentarán un poco el rendimiento pero disminuirán la fiabilidad debido al riesgo de pérdida de datos en caso de un cierre inesperado del servidor entre que recibió el pedido de escritura y los datos sean escritos realmente en el disco. Debido a que el valor predeterminado cambió recientemente (comparado con el valor histórico de *NFS*), se recomienda configurarlo explícitamente.

Para no proveerle acceso de *root* al sistema de archivos a ningún cliente *NFS*, el servidor considerará todas las consultas que parezcan provenir de un usuario *root* como si provinieran del usuario *anonymous*. Este comportamiento corresponde a la opción ***root_squash*** y está activado de forma predeterminada. La opción ***no_root_squash***, que desactiva este comportamiento, es riesgosa y sólo debe ser utilizada en entornos controlados. Las opciones ***anonuid=udi*** y ***anongid=gid*** permiten especificar otro usuario falso que será utilizado en lugar de *anonymous*.

Existen otras opciones disponibles que están documentadas en la página de manual ***exports***(5).

Nota

OJO: El script de inicio ***/etc/init.d/nfs-kernel-server*** sólo inicia el servidor si el archivo ***/etc/exports*** incluye al menos uno o más espacios compartidos *NFS* válidos. En la configuración inicial, una vez que editó este archivo para que contenga elementos válidos, deberá iniciar el servidor *NFS* ejecutando lo siguiente:

root@SRVFich:/# /etc/init.d/nfs-kernel-server start

Hasta aquí la configuración del lado del servidor.

Ahora explicamos el caso de los clientes NFS.

Como con cualquier otro sistema de archivos, incorporar un espacio compartido *NFS* en el jerarquía del sistema es necesario montarlo. Debido a que este sistema de archivos tiene sus peculiaridades fueron necesarios algunos ajustes en la sintaxis de ***mount*** y en el archivo ***/etc/fstab***.

Si lo montamos manualmente desde consola:

```
root@SRVFich:/# mount -t nfs -o rw,nosuid SRVFich:/mnt/repositorio /compartido
```

Si lo automatizamos para que se monte al arranque del sistema:

```
SRVFich.central.local:/mnt/repositorio /compartido nfs rw,nosuid 0 0
```

Servicio FTP

Además de la conexión mediante Samba y NFS, puede dotarse de otra funcionalidad más.

Un servidor *FTP* permite compartir archivos de un manera simple. Es el sistema ideal para almacenar archivos que requieran acceso en modo lectura como, por ejemplo, archivos de audio, *PDF*, videos, *drivers* de hardware, etc.

Además, cuando se configura con soporte *TLS/SSL*, puede accederse desde el exterior de una forma segura.

La instalación del servicio, al igual que en otras ocasiones no genera mayor inconveniente:

```
root@SRVFich:/# apt-get aptitude install proftpd
```

En la instalación aparecerá una ventana que nos preguntará en qué modo queremos instalar proftpd, "*standalone*" o "*inetd*", la diferencia es en la velocidad de ejecución y en la carga que soportará nuestro servidor:

- ***Inetd*:** En cada conexión nueva que realicemos al servidor, se crea un nuevo proceso.
- ***Standalone***: Cada conexión se ejecuta como un proceso independiente del mismo.

En nuestro caso vamos a escoger la opción de "*Standalone*".

Por defecto, *proftpd* crea un usuario llamado *ftp* y un directorio que almacenaremos los archivos para compartir, en ***/home/ftp/***.

A continuación se detalla la configuración que lleva este servicio:

El archivo de configuración de proFTPD es ***/etc/proftpd/proftpd.conf***.

Para dejar correctamente en funcionamiento nuestro servidor, editaremos lo siguiente en dicho fichero de configuración:

En nuestro caso, al no usar direcciones ipv6:

```
UseIPv6   off
```

Tal y como se puede ver más abajo, también podemos editar el nombre de nuestro servidor, el tipo, el tiempo de uso de la conexión, usar un mensaje de bienvenida en cuanto te conectas, etc.

Lo siguiente que editaremos del fichero de configuración es el directorio especificado que usará nuestro servicio para compartir los ficheros:

DefaultRoot /home/ftp/

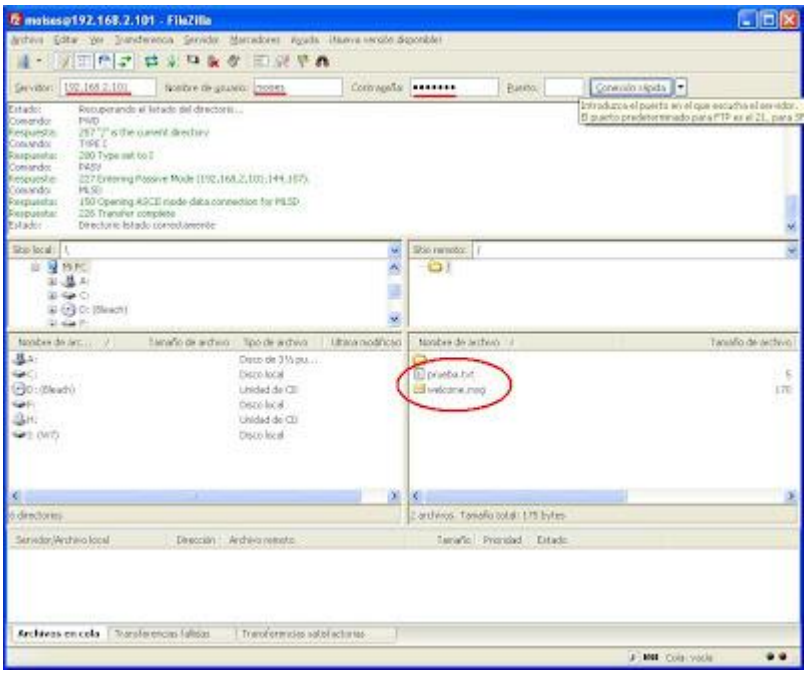
Por defecto viene comentado, descomentamos e indicamos la ruta en el cual solo usaran los usuario que se conecten.

Ahora solo nos quedaría reiniciar el servicio y probar el login.

root@SRVFich:/# /etc/init.d/proftpd restart

Para realizar una prueba, bajo dicho directorio raíz para los usuarios, hemos creado un par de ficheros de prueba.

A través de un cliente FTP, como Filezilla, nos conectamos al servidor, indicando la dirección IP o Nombre DNS del mismo, y los datos la cuenta de usuario para conectar (usuario/contraseña).



Nota

OJO: Cuidado al usar el usuario ya que puede tener una *shell* no válida para conexiones FTP. El servicio puede ser bueno y estable, cuando el problema no procede del servidor.

Podéis ver las *shell* de las cuentas de usuarios del sistema en ***/etc/passwd***.

Configuración Servidor Backup

En este apartado no es necesario explicar nada nuevo.

Los servicios que se utilizarán serán *NFS* o *SSH* para acceder a los ficheros y directorios que salvaguardar, acompañado de un script programado automáticamente, a través del servicio *CRON*, que será el encargado de realizar la copia de copiar los datos en este servidor.

La conexión se realiza a todas las máquinas que se desee guardar datos, entendiéndose que tienen el servicio NFS operativo.

Una vez se tiene conexión, se desarrolla un script que realice automáticamente las copias de seguridad. El siguiente script es un ejemplo:

```
#!/bin/bash
#automated backup of "name" project from server xx.xx.xx.xy DO NOT TOUCH!!!
workingdir=/home/administrator/backup/
checkfile=/home/administrator/backup/checkfile.txt
if [ -d $checkfile ]; then
cat > $checkfile
else
touch $checkfile
fi
echo "backup is done! on" > $checkfile
date >> $checkfile
echo "files saved: " >> $checkfile
rsync -avz -
e ssh administrator@xx.xx.xx.xx:/home/administrator/data /home/administrator/backup/ >> $checkfile
rsync -avz -e ssh administrator@xx.xx.xx.xx:/var/www/webapps /home/administrator/backup/
rsync -avz -e ssh --
exclude "*.log" administrator@xx.xx.xx.xx:/opt/dataserver /home/administrator/backup/
```

Por supuesto, los directorio, direcciones IP o nombres de dominio variarían así como la forma en la que decidamos realizar las copias.

Rsync es un sistema de respaldos incrementales típico en sistemas tipo *Unix* que se caracteriza por hacer respaldos incrementales minimizando el tráfico de datos. Básicamente *rsync* no copiara todos los datos o árbol de directorios cada vez que sincronice sino que solo copiara los archivos modificados del origen conforme a su destino, hace esto mediante un algoritmo de sincronización de directorios. Estas transferencias o sincronizaciones se pueden realizar dentro del mismo disco duro (entre directorios locales) o entre dispositivos en red utilizando protocolos *TCP/IP*.

Este script deberá ir programado con *CRON* en el fichero **/etc/crontab**.

```
00 5 * * 0 /home/administrator/scripts/backup.sh >/dev/null 2>&1
```

El backup será realizado semanalmente los domingos a las 5 de la mañana. Y aseguramos la salida del comando para que no quede colgado el proceso.

Clientes

En el caso de los equipos clientes, se indicará el proceso de instalación y configuración en conjunto, ya que todos ellos llevarán el mismo tipo de utilidades.

Instalación Sistema Base

El proceso de instalación del Sistema Operativo base que llevarán los clientes (Ubuntu 12.04) se encuentra detallado en el documento "***ANEXO II_Instalación de sistema base en Clientes***".

Configuración General

Es importante que los equipos clientes estén con un buen soporte técnico a nivel aplicativo.

Para ello, tras la instalación, marcamos cuales son los útiles más importantes para funcionar con normalidad en el día a día.

Ejecutar el Administrador de Actualizaciones

Es probable que luego de haber sido lanzado Ubuntu 12.04 hayan aparecido nuevas actualizaciones de los distintos paquetes con los que viene la imagen ISO que distribuye Canonical.

Por esta razón, luego de terminar la instalación siempre es recomendable correr el Administrador de Actualizaciones. Puede hacerse buscándolo en el *Dash* (nuevo menú interfaz *Unity*) o ejecutando lo siguiente desde un terminal:

```
# sudo apt-get update

# sudo apt-get upgrade
```

Instalar Idioma español

En el *Dash* escribir *Idioma* y desde allí vas a poder agregar el idioma que prefieras.

Instalar códecs, Flash, fuentes adicionales, drivers, etc.

Debido a cuestiones legales, Ubuntu no puede incluir por defecto una serie de paquetes que, por otra parte, son muy necesarios para cualquier usuario: *códecs* para reproducir *MP3*, *WMV* o *DVDs* encriptados, fuentes adicionales (muy usadas en *Windows*), *Flash*, *drivers* propietarios (para hacer un mejor uso de las funciones *3D* o de la red *WIFI*), etc.

Afortunadamente, el instalador de Ubuntu permite instalar todo esto desde el principio. Sólo hay que habilitar esa opción en una de las pantallas del instalador.

En caso de no haberse hecho, puede instalarse de la siguiente manera:

Driver de la tarjeta de video

Ubuntu debería detectar en forma automática y alertarte sobre la disponibilidad de los *drivers 3D*. En ese caso, se verá un ícono de una tarjeta de video en el panel superior. Hacer clic en ese ícono y seguir las instrucciones.

Si Ubuntu no detecta tu tarjeta, siempre puede instalarse el *driver 3D* (**nvidia** o **ati**) buscando la Herramienta de Configuración de Hardware.

Códecs y formatos propietarios

Si se cree que los ficheros multimedia son necesarios e indispensables para el trabajo del usuario, hay una solución muy sencilla:

```
# sudo apt-get install ubuntu-restricted-extras
```

Para añadir soporte de *DVDs* encriptados (todos los "originales"), abrí un terminal y escribí lo siguiente:

```
# sudo apt-get install libdvdread4

# sudo /usr/share/doc/libdvdread4/install-css.sh
```

Instalar repositorios adicionales

Medibuntu

Es un repositorio de paquetes de software que no pueden ser incluidos en la distribución Ubuntu por motivos como problemas legales de copyright, licenciamiento o restricciones de patentes. Incluye programas como: *Google-Earth*, *Opera*, *Win32codecs*, *Msfonts*.

```
# sudo -E wget --output-document=/etc/apt/sources.list.d/medibuntu.list
http://www.medibuntu.org/sources.list.d/$(lsb_release -cs).list && sudo apt-get --quiet update &&
sudo apt-get --yes --quiet --allow-unauthenticated install medibuntu-keyring && sudo apt-get --quiet
update
```

Para agregar los paquetes de *Medibuntu* en el Centro de Software de Ubuntu:

```
# sudo apt-get install app-install-data-medibuntu apport-hooks-medibuntu
```

Instalar aplicaciones de compresión

Para poder comprimir y descomprimir algunos formatos propietarios y libres populares, es necesario instalar los siguientes paquetes:

```
# sudo apt-get install rar unace p7zip-full p7zip-rar sharutils mpack lha arj
```

Instalar otros gestores de paquetes y de configuración

Synaptic le permite instalar, actualizar o desinstalar paquetes de programas de forma versátil.

No viene ya instalada por defecto.

```
# sudo apt-get install synaptic
```

Encontrar más aplicaciones en el Centro de Software de Ubuntu

En caso de que no encontrar aplicaciones para hacer lo que se desea puede recurrirse al Centro de Software de Ubuntu.

Desde allí vas a poder instalar excelentes aplicaciones con tan sólo unos pocos clics. Algunas elecciones populares son:

AbiWord, editor de textos simple y liviano

Thunderbird, e-mail

Chromium, explorador web (versión libre de Google Chrome)

Pidgin, chat

VLC, video

FileZilla, FTP

GIMP, editor de imágenes (tipo Photoshop)

Cambiar la interfaz

Si no se desea tener *Unity* como interfaz por defecto, siempre es posible volver a usar *GNOME*:

- Cierra Sesión (LogOut)
- Hacer clic en el nombre de usuario
- Buscar el menú de sesión en la parte inferior de la pantalla
- Cambiar de Ubuntu a Ubuntu Clásico
- Hacer clic en Iniciar Sesión.

En caso de que por alguna extraña razón esta opción no se encuentre disponible, puede instalarse lanzando el siguiente comando primero:

```
#sudo apt-get install gnome-session-fallback
```

Tras esto, deberá volver los pasos anteriores.

Clientes: Incorporación a dominio

Los clientes necesitarán apuntar a los nuevos servidores.

Para ello, deberemos acceder a las opciones de red y dejarlo basándose en la siguiente plantilla:

Dirección IP: <IP_cliente>

Máscara de red: 255.255.255.0 (modificar si se cambia el rango y cobertura de la red)

Puerta de enlace: <IP_Servidor_DHCP>

DNS: <IP_Servidor_DNS>

WINS: <IP_Servidor_Directorio>

Para los casos de Windows, una vez se configuren los nuevos datos de red, deberemos de incorporar el cliente al dominio.

Windows XP/2000

Para ello, accederemos a las Propiedades de Mi PC → Pestaña "Nombre de equipo" → Pulsamos sobre "Cambiar".

Cambiaremos de Grupo de Trabajo a Dominio, y escribiremos este último.

Una vez aceptemos, deberemos introducir el usuario root del dominio y su contraseña. De hacerlo correctamente se recibirá un mensaje confirmándonos la incorporación al nuevo dominio.

Reiniciamos el equipo.

A la hora del Login tras el reinicio, deberemos cambiar la opción de "Concectarse a" de nuestro equipo local al nuevo dominio.

Introducimos los datos de la cuenta de usuario de dominio y accedemos.

Windows Vista/7/8

En este caso, es algo más avanzado las modificaciones a realizar:

En la configuración del adaptador de red, además de indicar los valores arriba puestos, se debe de marcar la casilla "Activar Netbios sobre TCP/IP".

Ir a Panel de control → Sistema y Seguridad → Herramientas Administrativas → Directiva de seguridad local → Directivas locales → Opciones de seguridad.

En Seguridad de red: *nivel de autenticación de LAN Manager*, establecer enviar respuestas LM y NTML.

En Seguridad de red: *seguridad de sesión mínima para clientes NTML basados en SSP* y *Seguridad de red: seguridad de sesión mínima para servidores NTML basados en SSP*, deshabilitar Requerir cifrado de 128-bit.

Opcionalmente, se puede aplicar también un parche, provisto por Microsoft, para evitar una molesta ventana con una advertencia, misma que se muestra invariablemente tras registrar exitosamente el equipo en el dominio del PDC con Samba, la cual que dice:

«*No se pudo cambiar el nombre DNS de dominio principal de este equipo a "". Se mantendrá el nombre "DOMINIO". Error: El dominio especificado no existe o no se pudo poner en contacto con él*»

Esta advertencia se puede ignorar con toda tranquilidad. Si se desea aplicar el parche que elimina esta advertencia, ir a la siguiente dirección y seguir las instrucciones:

http://support.microsoft.com/kb/2171571

Reiniciamos sistema para poder iniciar sesión en el nuevo dominio.

Linux

En caso de los sistemas bajo Linux, varia el inicio de sesión.

La utilidad del dominio no va a nivel sistema operativo cliente, como ocurre en Windows, sino a nivel aplicativo.

Por tanto, en Linux no existe la posibilidad de Iniciar sesión en el sistema dentro del dominio. Sin embargo, podrá configurarse el equipo en la base de datos del directorio como equipo del dominio, así como poder usar en distintas aplicaciones los accesos al dominio (lectura o escritura).

Clientes: Perfiles móviles

En el caso de los perfiles móviles, y tal como se ha configurado en el controlador de dominio con *Samba*, todo lo que se cree en el entorno del usuario en la estación cliente (Documentos del usuario) será almacenado en la carpeta del servidor.

Esto hará que el usuario pueda rotar de equipo si es necesario e igualmente accederá a sus ficheros.

Nota

HA DE SABER que el concepto de perfiles móviles únicamente atañe a entornos de clientes *Windows*, y no *Linux*.

Para *Linux* se emplea el servicio y protocolo *NFS*.

La idea principal de esto sería tener un script automático que arranca al inicio y configura el directorio del /home del usuario en el cliente como un punto de montaje apuntado al servidor.

Para configurarlo podemos tirar de lo documentado anteriormente en los servicios de *NFS* del servidor de *backup*.

RESULTADOS Y ANÁLISIS DEL PROYECTO

En esta última fase del proyecto se pretende analizar técnica y económicamente la resolución del proyecto implantado.

Análisis Técnico

Antes de considerar los objetivos conseguidos y los que no, ha de tenerse en cuenta el tiempo establecido para el proyecto así como la extensión del mismo.

Muy importante es destacar que **absolutamente todo el proyecto ha sido llevado a cabo en un entorno virtual completo**, no solo realizando una completa documentación al respecto, sino simulando lo más cercano a un caso real.

Por supuesto, hay cosas que, por tiempo, no se pueden realizar simuladamente en comparación con una empresa. Ejemplo de ello sería la extensa base de datos de una empresa, referentes al directorio, al correo electrónico, etc… Rellenar una base de datos tan grande llevaría muchos días de aplicación a ello, por lo que finalmente se ha querido centrar en lo más importante del proyecto: la utilidad de apoyo de esta guía de implantación para otros usuarios en un caso real.

A continuación se enumeran los objetivos marcados al principio del proyecto, con el fin de reflejar los superados. En el caso de no haberse podido superar el objetivo, se justificará la causa del mismo.

Objetivo	Implant.	Hitos sin implantar	Causas	Solución (S/N)
Migración de sistemas de autenticación de usuarios a la red corporativa	**90%**	**Migración de usuarios reales de entorno Windows Server (Directorio Activo) a OpenLDAP**	**No se ha podido poblar al completo la base de datos como en un caso real, por ende, no se ha podido migrar desde Windows Server.**	**S**
		Migración de sistemas operativos de equipos clientes a GNU/Linux	**Si se pretende tener centralizados a los usuarios a nivel de sistema operativo, únicamente los sistemas de Microsoft facilitan el inicio de sesión bajo dominio corporativo. GNU/Linux no tiene forma implantada para esta función. Únicamente los aplicativos son los que podrán utilizar las bases de datos de los servidores si se desea.**	**N**
Migración de sistemas de conexión de los equipos clientes a la red corporativa y al exterior de la misma	**100%**	-	-	-
Migración del sistema de impresión	**100%**	-	-	-

Migración de los sistemas de comunicación	**90%**	**Configuración de Antivirus y AntiSpam**	**Falta de Tiempo**	**S**
		Centralización de la base de datos de correo electrónico con el servicio de directorio (OpenLDAP)	**Por falta de tiempo. La única modificación sería el cambio de la base de datos de este servidor de Mysql a OpenLDAP.**	**S**
Migración del servidor de archivos	**100%**	-	-	-
Migración del sistema de backups de la información	**100%**	-	-	-

Todas las tareas sin implantar indicadas arriba tienen solución (a excepción de la migración del sistema operativo de los clientes). La causa principal de su no implantación ha sido la falta de tiempo para abarcar un proyecto, quizás, de demasiada envergadura para el tiempo establecido. Por supuesto, en un caso real esta implantación duraría más tiempo, ya que cada paso debería ser bien comprobado y repetir los pasos de configuración para verificar el proceso completo, además de las numerosas pruebas al finalizar cada fase.

Para el caso de la migración de los sistemas operativos de los equipos de los usuarios hay dos opciones: migrarlos y perder casi todo el control que se tiene sobre ellos cuando están bajo políticas de dominio a nivel de sistema operativo, o mantener un sistema operativo cliente privativo, que utilizan el módulo de inicio de sesión bajo dominio (a excepción de GNU/Linux que solo inicia en local). Esto permite un mayor control sobre la arquitectura de sistemas de la empresa.

Como he comentado en el apartado de problemas encontrados en la parte de implantación, existe una empresa catalana que desarrollo dicho módulo necesario para GNU/Linux y poder iniciar sesión bajo dominio. Sin embargo, dado que no poseo licencia ni permisos para divulgar ningún tipo de información sobre la misma, se opta por tomar la no existencia de dicha solución.

DETALLES PERSONALES SOBRE EL PROYECTO

A continuación se detallan algunos aspectos personales relacionados con este proyecto.

Tras haber afrontado la parte más densa del proyecto (Implantación y Técnica) he de recalcar mi posible desmedida a la hora de analizar los tiempos.

Quizás he querido abarcar más de lo que me hubiera gustado demostrar y/o aplicar en el proyecto final.

Determinadas funciones y servicios, que pueden llegar a realizarse e implantarse en una empresa no serán finalmente detallados ni explicados dado que no hay tiempo material para ello.

Tras descubrir esto, he llegado a la conclusión que es mucho mejor la entrega de un proyecto con menor ambición pero que igualmente siga pudiendo cubrir necesidades en una empresa, en lugar de querer abarcar todo lo propuesto en el análisis y realizar la entrega incompleta y por tanto la descalificación del mismo.

Aunque se explica la puesta en marcha de cada tipo de servidor, y puesto que a lo largo del proyecto se han ido extendiendo el número de páginas, no se ha profundizado en los detalles de cómo conectar una sede con la otra. Inicialmente, en el apartado de análisis, se marcó que ambas sedes tendrían una conexión VPN entre ellas, lo cual significa que dado que la configuración de replicación entre servidores fue explicada más arriba, podrá realizarse igualmente la sincronización entre ambas sedes.

Al igual ocurre con el sistema de seguridad de copias de datos. Tras haber explicado como de implanta uno de ellos, el resto es únicamente cambiar los datos de los servicios (direcciones IP, directorios que copiar, etc.) y utilizar la conexión VPN igualmente para ello.

BIBLIOGRAFÍA CONSULTADA

Información general, historia y conceptos concretos:

http://es.wikipedia.org/

Análisis, estudio e información sobre distribuciones GNU/Linux:

http://www.debian.org/index.es.html

http://www.ubuntu-es.org/

http://www.es.redhat.com/

http://es.opensuse.org/

http://www.linux-es.org/distribuciones

Aplicativos (Información General)

http://www.openldap.org/

http://www.samba.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://www.ubuntu-es.org/forum

Servicios de red (DNS, DHCP,…)

http://cumptrnrd.wordpress.com/2012/02/20/configuring-an-ubuntu-debian-server-for-dns-dhcp-and-wins/

Samba-LDAP:

http://siddou.hd.free.fr/2013/06/install-sambaopenldap-on-debian-7-wheezy/

http://www.tutorial-es.com/sistemas-operativos/fedora-13/40-configurar-ldap-servidor

http://www.ldap-es.org/node/20

Samba y NFS como Servidor de archivos:

http://linux-windows.infonotas.com/nfs-guia-de-5-minutos-tutorial-para-compartir-carpetas-en-red-usando-nfs-en-linux/

http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m4/index.html

Servidor de impresión mediante Samba:

http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-samba-cups.html

https://wiki.samba.org/index.php/Samba_as_a_print_server

Servidor de Correo SMTP, IMAP, Webmail y AntiSpam:

https://workaround.org/ispmail/wheezy

https://help.ubuntu.com/community/Dovecot

http://wiki2.dovecot.org/

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

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

http://www.ehowenespanol.com/configurar-correo-web-roundcube-como_16774/

**** Muchos de los pasos y configuraciones elegidas no han sido consultadas en Internet, sino que han sido utilizados documentos personales que recopilan información acumulada durante mi trayectoria profesional.**