UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

PROYECTO FIN DE CARRERA

PLATAFORMA DE CORREO ELECTRÓNICO CON SINCRONIZACIÓN DE ELEMENTOS PIM MEDIANTE SERVIDOR FUNAMBOL

Héctor Moreno Blanco

NOVIEMBRE 2013

PLATAFORMA DE CORREO ELECTRÓNICO CON SINCRONIZACIÓN DE ELEMENTOS PIM MEDIANTE SERVIDOR FUNAMBOL

AUTOR: Héctor Moreno Blanco
TUTOR: Amalio Francisco Nieto Serrano
PONENTE: Eloy Anguiano Rey

Dpto. de Ingeniería de Telecomunicación
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Noviembre de 2013

RESUMEN:

El presente documento, objeto del PFC, describe el proceso de investigación de diferentes productos y soluciones de software libre para las capas correspondientes a un sistema de correo electrónico, así como su implantación y configuración para un correcto funcionamiento (*Plataforma de correo electrónico con sincronización de elementos PIM mediante servidor Funambol*).

Como consecuencia de las exigencias del mercado potencial, en cuanto a disponibilidad del servicio (7x24) y acceso en movilidad (ubicuidad), se propone como elemento adicional la implantación de un sistema para la sincronización de datos personales de los eventuales usuarios (contactos, calendarios, tareas, notas, etc.).

Por otra parte, como consecuencia de la situación económica actual, los aplicativos a implantar serán de libre distribución. Es decir, el coste de la licencia es gratuito. De este modo, se podrá ofrecer a un mercado más amplio de usuarios.

Además, para que la plataforma disponga de mayor seguridad, se instalarán los productos en servidores Linux, que ofrecen mayor protección ante ataques exteriores y virus.

Antes de comenzar con el informe del estudio del mercado de las aplicaciones de correo electrónico de software libre, se procederá a una breve descripción de los diferentes protocolos y estándares que se mencionan en el mismo y que, en la mayoría de los casos, se emplearán en la infraestructura a implementar.

Se iniciará con un estudio de los aplicativos más destacados en el mercado de Open Source para correo electrónico, basándose en funcionamiento, eficiencia, limitaciones de la versión libre (si procede) y usabilidad por parte de los usuarios y administradores.

Tras este estudio, se seleccionarán las aplicaciones que más se adapten a las especificaciones propuestas (precio, funcionalidades, etc.) y se procederá a la instalación y configuración de los productos seleccionados.

LISTA DE PALABRAS CLAVE:

Correo electrónico, dirección correo electrónico, calendario, agenda, contactos, tareas, transmisión, comunicación, servidor, webmail, estafeta, buzón, protocolo, estándar, red, internet, cortafuegos, lista distribución, virus, SPAM, reputación, sincronización, elementos PIM.

ABSTRACT:

This document describes the whole process of researching different open source products and solutions for the corresponding layers to an email system and its implementation and configuration for correct operation and performance (*Email platform with Funambol synchronization server*).

As a result of potential market requirements in terms of service availability (7x24) and mobile access (ubiquity), an additional element is proposed in order to implement a system for personal data synchronization for potential users (contacts, calendars, tasks, notes, etc.).

Moreover, due to the current economic situation, the applications to be implemented will be freely distributed. That is, the cost of the license is free. Thus, it can offer a broader market of users.

Furthermore, for the platformcan provide even more safety, products are installed on Linux, which offer greater protection against external attacks and viruses.

Before beginning the study of open source email applications, there will be a brief description of the different protocols and standards mentioned therein and mentioned in this infraestructure implementation.

We will start with a study of the most important applications in the Open Source market for email, based on performance, efficiency, limitations of the free version (if applicable) and usability for users and administrators.

Following this study, the most suitable applications for the proposed specifications (price, features, etc.) will be selected and proceed to the installation and configuration of the these products.

KEY WORDS:

Email, email address, calendar, addressbook, contacts, tasks, transmission, communication, server, webmail, relay, mailbox, protocol, standar, network, internet, firewall, mailing list, virus, SPAM, reputation, synchronization, PIM items.

Agradecimientos

En primer lugar, quiero dar las gracias a mi tutor, Eloy Anguiano por haber confiado en mí y en este proyecto, y por la paciencia que ha tenido conmigo por el retraso en finalizar. Por otra parte, también quiero agradecer a todos los profesores de la Escuela Politécnia Superior de la UAM por todos los años de aprendizaje y nuevos conocimientos adquiridos.

También quiero agradecer a toda mi familia todo lo que se han interesado por mí y apoyado a lo largo de toda la carrera y, sobre todo, durante el tiempo de realización del PFC. En especial a mis padres y hermnao, Paulino, Ana y Adrián, a mi abuela, Ángeles, por todos los tirones de oreja y apoyo proporcionado. Siempre han tenido fe en mí, y ahora espero estar a la altura.

Quiero agradecer también:

A todos mis compañeros de la universidad haber compartido todos los buenos (alguno malo) momentos. Sobre todo a Víctor, por su apoyo, ayuda y compañerismo, además de la paciencia que ha tenido conmigo. Tampoco olvidarme de mis amigos *Muñeco, Talón y Alvarito*. Todos ellos han hecho más llevadera la carrera, con las clases, exámenes y alguna que otra fiesta. Un placer y esperemos que siga así.

A mis compañeros de GMV la ayuda que me han prestado para la realización del proyecto, así como la representación de ellos en el mismo.

Y a mis amigos de toda la vida, que también me han dado su apoyo (a su manera) y su compañía durante todos estos años, y los que quedan. Pepe, *Tuchy*, Dani, Mario, Álex, Borja… Siempre han confiado en mí, y después de este proyecto, espero cumplir las expectativas.

¡MUCHAS GRACIAS A TODOS!

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

No se referencian tablas en el presente documento

1 Introducción

1.1 Motivación

El motivo del presente proyecto es la implantación de un sistema de correo electrónico eficaz, potente y fiable, con herramientas puramente de software libre. Además, las nuevas amenazas existentes en la red, hacen que sea una necesidad poder protegerse frente a ataques a través del correo electrónico. Como añadido se propondrá, e implantará un servidor para poder sincronizar los elementos PIM (calendario, contactos, tareas…) de modo que los usuarios puedan tener todo centralizado en un servidor y todos los dispositivos que posea (ordenador, móvil, tablet…) sincronizados.

1.2 Objetivos

El presente proyecto tiene como objetivos principales el aprendizaje de diferentes tipos de protocolos empleados en la comunicación y transmisión de información, su empleo y usos prácticos.

Adicionalente, se persigue la investigación y estudio de diferentes tecnologías y módulos de una plataforma de correo electrónico seleccionar una y proceder a su implantación.

Por otra parte, conocer las exigencias de los usuarios respecto a los datos personales, ya que siempre se quiere estar conectado y con acceso a la información de cada uno. Para ello se ha querido abordar la instalación de un servidor de sincronización de elementos PIM.

Conocida la actula situación de crisis económica, se pretende minimizar los costes de la solución con una plataforma más sencilla y personalizable. Razones, estas, por lo se han seleccionado productos de software libre y gratuitos. Esto quizá puede limitar algunas capacidades de otras plataformas de pago, pero no de manera significativa.

1.3 Organización de la memoria

La memoria de este proyecto, consta de los siguientes capítulos:

- **Estado del arte:** En este primer apartado se hará un repaso breve de la historia de las telecomunicaciones y del correo electrónico, así como una somera explicación de éste y de los diferentes protocolos implicados en la plataforma. También se hará un pequeño estudio de cada capa de la plataforma con los aplicativos más importantes disponibles, y las razones por las que se seleccionan unos en concreto.
- **Diseño:** Aquí se detalla~~n~~ el hardware y software de la plataforma, junto con explicaciones del esquema lógico diseñado. Por otro, se aportarán explicaciones del comportamiento de los diferentes módulos y funcionamiento entre ellos.
- **Desarrollo:** En este apartado se describe la instalación y configuración de todos los elementos de la plataforma. Los extensos ficheros de configuración se encuentran en los Anexos.

- **Integración y pruebas:** Como su nombre indica, este apartado presenta las pruebas realizadas a los diferentes componentes de la plataforma para comprobar el correcto funcionamiento y que cumpla las expectativas de los requisitos iniciales.
- **Concluisiones y trabajo futuro:** Tras una conclusión del trabajo realizado, se propondrán una serie de potenciales mejoras para la plataforma de correo electrónico diseñada y expuesta en este proyecto.

2 Estado del arte

2.1 Historia

Telecomunicación: comunicación a distancia. La comunicación es todo proceso de transferencia de información entre una fuente y un receptor.

Hoy en día, se utiliza el término Telecomunicación cuando la transmisión de la información involucra una propagación electromagnética inducida artificialmente. Así pues, ni el correo tradicional ni las antiguas formas de mensajes enviados mediante señales visuales o sonido se incluyen.

Esta información que se transmite, se define como los datos (símbolos, conjuntos sencillos de formas, imágenes, vídeo, gráficos, órdenes, medidas físicas…) que se han transferido desde el emisor hasta el receptor, diferiendo de la definición tradicional (información: todo aquello que puede incrementar nuestro nivel de conocimiento). Al final de la cadena, el receptor debe ser capaz de manipular esta información para posibilitar su interpretación. [1]

[2] En la antigüedad, la forma más común de producir estas señales para comunicarse era a través de luz (fuego) y sonido (tambores y trompas). Posteriormente fue evolucionando hacia otros medios más visuales, como son los semáforos. Sin embargo, todas estas formas de comunicación eran inseguras y altamente mejorables, ya que no permitían la encriptación del mensaje ni la transmisión de gran cantidad de información.

El salto cualitativo se dio con el descubrimiento de la electricidad. Le energía electromagnética es capaz de transportar información de manera muy rápida (idealmente a la velocidad de la luz). Se podría decir que el inicio de toda comunicación moderna fue con la invención de la célula eléctrica por Alessandro Volta (1800).

Poco después los experimentos comenzaron con sistemas de comunicación más avanzados. En 1809, Thomas S. Sommering propuso un sistema de telégrafos compuesto por una batería, 35 cables (letras y números) y un grupo de sensores fabricados de oro que se sumergían en agua: cuando una señal pasaba por uno de esos cables, la corriente eléctrica dividía las moléculas del agua y pequeñas burbujas de agua eran visibles cerca del sensor. Pronto le siguieron otros experimentos, algunos intentando mejorar el de Sommering (Wheatstone, Weber y Gauss).

Para el siguiente gran cambio, habría que esperar hasta 1843, cuando Samuel Morse propuso un método para asignar a cada letra y número un código ternario (punto, línea y espacio). Esta propuesta mejoraba económica y funcionalmente que la de Sommering, ya que, sobre todo, reducía la circuitería. Mientras tanto, la tecnología avanzaba y se descubrió la forma de convertir estas señales en sonidos. Así nació el código Morse, aún utilizado hoy en día.

El sistema fue mejorado en los siguientes años por Hughes, Baudot y Gray, quienes propusieron otros posibles códigos (el código Gray se emplea en las comunicaciones y en los códigos de barra hoy en día).

Sin embargo, el telégrafo aún se usaba por personal entrenado en ciertos edificios como oficinas, por ello podía seguir empleándose por una cierta cantidad de personas. Se produjo la búsqueda de una manera de transmitir sonidos además de señales. Aquí es cuando se inventaron los transductores que podrían transformar una señal acústica en otra eléctrica y viceversa con pérdidas aceptables (1850).

Siete años después, Antonio Meucci y Graham Bell desarrollaron un prototipo de teléfono y, debido a la falta de financiación de Meucci para regitrar la patente, Bell fue el primero en registralo.

Con los teléfonos y telégrafos, se creó vio necesidad de construir una red de comunicaciónes distribuida y fiable. Los problemas de enrutado se solucionaron por operadores humanos y circuitos de conmutación: nació la Red Telefónica Conmutada (PSTN: Public Switched Telephne Network). Sin embargo, este sistema no garantizaba la privacidad y seguridad de las conversaciones, por lo que se enfocó el desarrollo hacia la creación de un circuito de conmutación automático.

En 1899 Almon Strowger inventó un dispositivo electro-mecánico conocido como *switch* que estaba dirigido por señales eléctricas procedentes del dispositivo telefónico, logrando una selección basada en prefijos geográficos.

La transmisión de mensajes (información transmitida desde un emisor a un receptor) de manera electrónica se podría decir que comenzó con el código Morse (a mediados del siglo XIX), y en la Feria Mundial de Nueva York de 1939 donde IBM remitió una carta de felicitaciones desde San Francisco a Nueva York mediante una máquina de escribir eléctrica (para más información sobre el radiotipo de IBM. [3]

Más tarde, en la Segunda Guerra Mundial, Alemania hizo use de los teletipos [4], cuyo uso se generalizó en los años venideros gracias a la red Telex. A la par que los teletipos, estaban los modelos americanos TWX (Teletypewriter eXchangeService).

Por otra parte, en 1946 comienza la era de la informática con la invención del ENIAC (Electronic Numerical Integrator and Computer). De este modo, la informática y las telecomunicaciones comienzan a interactuar como era de esperar: procesado de datos rápidamente así como el envío de los mismos a larga distancia.

Otras innovaciones que fueron saliendo en el campo de las telecomunicaciones fueron la radio (Guglielmo Marconi, 1895), aparición de válvulas amplificadoras (1920), creación de la televisión (1923), creación de los transistores (1947), primer circuito integrado (1958), primer microprocesador (1969).

Con el último invento, la electrónica se convierte en una parte fundamental del mundo de las telecomunicaciones, al principio sólo en la transmisión, pero rápidamente en el entorno de conmutación de circuitos.

El desarrollo de la microelectrónica y la informática revolucionó las redes de telecomunicaciones y su rendimiento. En 1938 comenzó a usarse una tecnología innovadora, PCM (Pulse Code Modulation). Esta tecnología podía lograr la transmisión de señales de voz codificando y decodificando digitalmente.

Durante la década de los 60, un empleado de la compañía RAND, Paul Baran, ideó el concepto de *intercambio de paquetes de red* (*packet switching network*) como alternativa a la red de conmutación de circuitos. De acuerdo con este modelo, no habría jerarquía en los nodos de red si no que cada nodo se conectaría con otros y sería capaz de decidir y enrutar los paquetes. Cada paquete era un conjunto de datos, dividido en dos partes, las cabeceras (con información del enrutado) y el cuerpo (propios datos).

Dentro de este contexto, Vincent Cerf, Bob Kahn entre otros, desarrollaron en los años 70 el protocolo TCP/IP, que permitía la comunicación ordenadores y otras máquinas a través de una seria de capas lógicas y físicas. La red de intercambio de paquetes y el TCP/IP se seleccionaron para el proyecto militar ARPANET [5]. El resto de la historia es bien conocida: en 1983 ARPANET estuvo disponible para universidades y centros de investigación, entre los cuales estaba NSFNET (National Science Foundation + NET), que dio origen a Internet.

2.1.1 Correo electrónico

El correo electrónico es un método de intercambio digital de mensajes desde un remitente a uno o varios destinatarios. Se basa en el modelo de almacenar y enviar, así pues no se debe confundir con la mensajería instantánea.

[6] El correo electrónico antecede a Internet, y fue una herramienta fundamental para la creación de éste. En 1961 hace su aparición el modelo CTSS (Compatible Time-Sharing System) en el prestigioso MIT. Mediante este sistema los usuarios se conectaban desde un terminal con un ordenador modelo 7094, y almacenaban ficheros en el disco. El objetivo de este modelo era poder compartir información mediante un nuevo mecanismo: los usuarios pasaban mensajes unos a otros, creando mensajes en directorios comunes. El destinatario, al conectarse al sistema CTSS desde cualquier terminal, podía mirar si tenía algo para él, buscando en el directorio personal. A este tipo de correo electrónico, Ian R. Hardy lo denomina *intra-computer email*, en contraposición al *network email* que aparecería posteriormente con el advenimiento de ARPANET.

En 1971, Ray Tomlinson, un ingeniero de la empresa BBN, creó el correo electrónico tal y como se conoce hoy en día. Tuvo la idea de crear un programa que permitiera enviar estos mensajes de un ordenador a otro distinto. Los programas que creó se llamaron originalmente SNDMSG (para el envío de mensajes) y READMAIL (para su lectura).
Se creó la necesidad de separar de algún modo el nombre del usuario del de la máquina desde la que se enviaba el correo. De entre los caracteres que poseía el teclado que Ray utilizaba, un Model 33 Teletype, eligió uno: la arroba, @.

En julio, Larry Roberts crea el primer programa de gestión de correo electrónico, que permite listar, leer, archivar, responder, o reenviar mensajes de correo. El programa se llama *RD*, y ya permite ordenar los mensajes según su asunto o fecha de envío, junto con otras funciones que facilitaban su uso.

Poco después, Barry Wessler, investigador de DARPA, creó *NRD* a partir de *RD*, en el que incluía nuevas características, como la posibilidad de borrar mensajes.

A partir de todas estas aplicaciones, Marty Yonke creó un nuevo programa, que denominó *WRD*, y que permitía enviar y leer mensajes, pero cuyo entorno era mucho más cómodo para el usuario. Más tarde lo renombró como *BANANARD*.

John Vittal mejoró este último, creando *MSG*, que es considerado como el primer programa moderno de gestión de correo electrónico. Entre otras novedades, permitía reenvío de mensajes, o direccionar automáticamente las respuestas, por ejemplo.

Así pues, el inicio de intercambio de mensajes de realizaba mediante el protocolo FTP (File Transfer Protocol). Más adelante, en 1994 aparece el RFC 1725, POP3. Este protocolo permitía al usuario descargarse los mensajes del servidor a su propia máquina. Aunque en 1988 surgió IMAP2 como protocolo (RFC 1064), fue en 2003 cuanto se creó el protocolo IMAP4 (RFC 3501) que permitía leer el correo online y desde cualquier sitio como si se estuvieran manipulando carpetas locales. Por otra parte, para el envío de mensajes, al dejar de emplear FTP, se inventó el protocolo SMTP (RFC 821, RFC 2821, RFC 5321).

Los servidores de correo electrónico aceptan, envían, entregan y almacenan mensajes, con la ventaja de que no es necesario que los participantes en la comunicación estén conectados al mismo tiempo, simplemente con un breve intervalo de tiempo serán capaces de establecer el flujo de comunicación entre ellos.

Un correo electrónico consta principalmente de dos elementos:

- Cabeceras: las cabeceras de los correos electrónicos contienen información de control, como las direcciones de correo del remitente y los recipientes (destinatarios). También pueden contener diferentes tipos de información como etiquetas de antivirus o antispam, y las diferentes estafetas de correo por las que ha pasado con las correspondientes fechas/horas.
- Cuerpo del mensaje: el cuerpo del mensaje es el mensaje en sí mismo, donde está la información a transmitir. Esta información puede ir cifrada o en plano.

En un principio, sólo se transmitía texto plano y sencillo, pero rápidamente salieron estándares RFC para permitir la codificación de caracteres y la inclusión de contenido multimedia y adjuntos, así como redacción/lectura de correos en HTML.

El funcionamiento del correo electrónico es sencillo y se explicará mediante el siguiente diagrama:

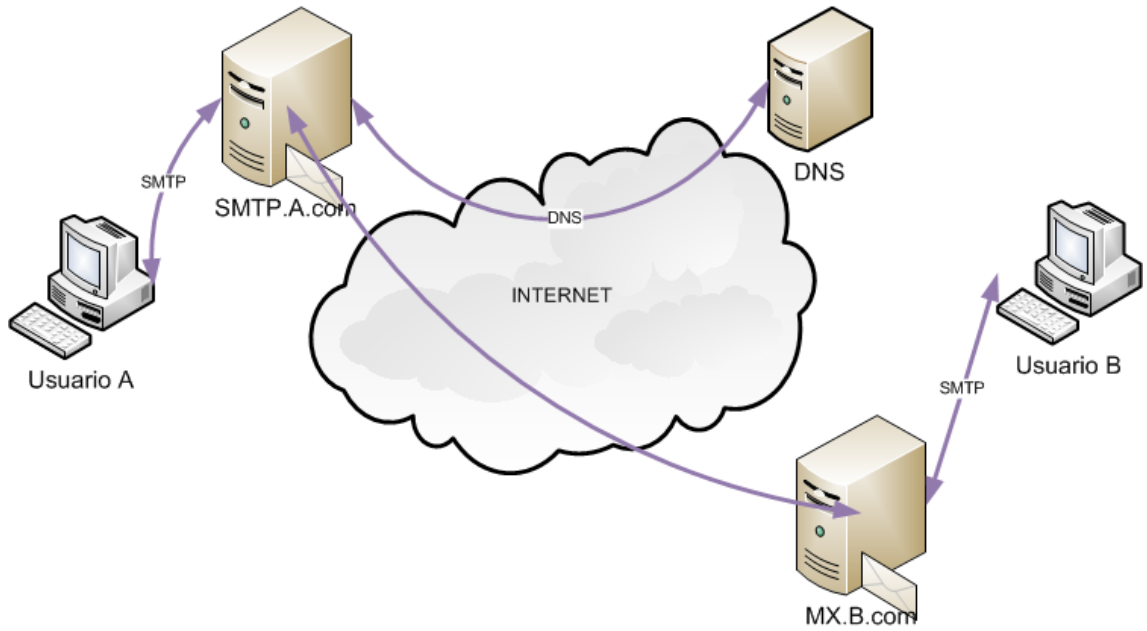

Figura 1 - Ejemplo de tráfico de correo

En este ejemplo, el usuario A mandará un correo electrónico al usuario B. Ambos usuarios con cuentas en servidores diferentes. [7]

A la hora de escribir un correo electrónico el usuario A, ya sea con cliente de correo o por una herramienta de webmail, el aplicativo se pondrá en contacto con su servidor de salida SMTP, transfiriéndole el mensaje a enviar. Este servidor tendrá que conocer dónde mandarlo, para ello se pone en contacto con un servidor DNS para que le conteste cómo encaminar este mensaje. Esto es, le pregunta por el servidor MX del recipiente. El servidor SMTP A recibirá esta información y redirigirá el correo electrónico al MX del usuario B.
De este modo, el mensaje estaría almacenado en el servidor del usuario B para que cuando acceda a su cuenta, ya sea con webmail o cliente pesado, pueda recuperar dicho correo, ya sea mediante POP3 como IMAP4.

En el caso de que los dos usuarios estén en la misma red, el mensaje no se transmitirá a través de internet, si no que, dependiendo de cómo esté estructurada la arquitectura de correo, se redirigirá internamente del servidor de envío SMTP al MX correspondiente.

Otro caso, menos común, que se puede dar en usuarios con sistema operativo basado en Unix, es que el usuario A tenga en su propio ordenador un servidor SMTP y, por tanto, actuaría él mismo como servidor de envío.

Una vez que el usuario B ha recibido el correo, tiene varias opciones para acceder a su información.

La primera es mediante POP3. Éste es un protocolo de descarga de correo. Quiere decir que el usuario, mediante un cliente de correo (Microsoft Outlook, Mozilla Thunderbird, Evolution, KMail…) accederá al servidor haciendo uso del protocolo POP3 y descargará sus mensajes a su ordenador local.

También mediante cliente de correo, puede hacer uso del protocolo IMAP. De este modo sólo consultará el correo sin descargarlo del servidor. Es decir, podrá acceder a él desde cualquier máquina siempre y cuando se autentique.

La última manera de consultar el correo sería mediante los aplicativos de Webmail. El usuario se conecta a una página web en la que, después de autenticarse con sus credenciales, tiene acceso a todo su correo. Esta manera hace uso de protocolo IMAP.

2.1.1.1 Peligros y amenazas del correo electrónico

En la era actual, hay una gran preocupación por la seguridad informática, confidencialidad e integridad de los datos. El correo electrónico es muy propicio a sufrir diferentes ataques de este tipo. Se van a destacar los 3 grandes principales problemas/amenazas:

En primer lugar destacar el envío de virus a través del correo electrónico. Los virus informáticos son un *malware* que alteran el funcionamiento del ordenador. Los más comunes son los troyanos (programa dañino que se oculta en otro programa legítimo), gusanos (programa que van consumiendo cada vez más memoria), virus de macros (como los *keylogger*), etc.

Para evitar que se reciba (o envíe, en caso de estar ya infectado) un virus, existen muchos sistemas de antivirus, tanto de pago como gratuitos. Sin embargo, en muchas plataformas de correo, los propios servidores ya contienen un sistema antivirus, que tratarían de desinfectar el mensaje o, en caso de no poder, no entregarlo y eliminarlo (o ponerlo en cuarentena). Pudiendo, o no, avisar de esto al usuario.

Otro problema bastante grave se trata del correo no deseado. Se trata de mensajes electrónicos no solicitados y que son enviados en cantidades masivas, generalmente de tipo comercial. También denominado SPAM. En ocasiones, es un virus el que propicia que desde una cuenta se envíen estas cantidades de correo, provocando la entrada en listas negras (se le prohíbe el envío) a los servidores.

Frente al SPAM, existen numerosas herramientas también, tanto de pago como gratuitas. Muchas veces, son los propios antivirus los que tienen también esta funcionalidad. Sin embargo, en esta ocasión, sí que es más frecuente que sea el propio servidor el que determine si es SPAM o no. Existen muchas palabras clave para determinar el SPAM. Si los servidores contienen la funcionalidad de listas grises, proporciona una oportunidad en caso de que se haya tenido un falso positivo de SPAM.

Las listas grises, de primeras, meten cualquier dirección (o dominio) nueva en una lista, sin distribuir el mensaje. Activando un contador. Si se vuelven a recibir más correos de esa dirección de manera sospechosa (muy seguidos o mucha cantidad), esa dirección se añadirá a la lista negra, prohibiendo el envío a ese servidor. Por el contrario, saldría de esa lista gris y permitiría el paso siempre (a menos que sea susceptible de ser SPAM).

Existe otro problema, también muy crítico, que se denomina *phising*. Los mensajes de *phising* son correos electrónicos, a priori pueden parecer legítimos, que solicitan al usuario credenciales o datos privados del mismo, con el fin de robar la identidad y usarlo para acceder a cuentas de correo, cuentas bancarias, etc.

Ante esta amenaza, a pesar de que los antivirus actualizados mantiene una base de datos con posibles plantilla de *phising*, la mejor manera de prevenir es que el usuario sea capaz de discernir si el correo es legítimo o no. Como norma general, cualquier entidad (bancaria, empresa…) NUNCA solicitará por correo electrónico datos personales, y mucho menos financieros o contraseñas. Tampoco es recomendable, si no se está seguro del correo electrónico, seleccionar ningún enlace contenido en el mismo.

2.1.2 Sincronización de elementos PIM

Según avanza la tecnología, avanza también la movilidad de las personas. Esto obliga a los usuarios estar prácticamente conectados todo el tiempo. Además de poder disponer del correo electrónico en cualquier lugar, surge la necesidad de tener también siempre disponible datos de calendarios, libretas de direcciones, tareas, etc. en diferentes dispositivos allá donde se encuentre.

Para llevar a cabo este tipo de sincronizaciones, existen muchos tipos de protocolos que han ido surgiendo los últimos años (SyncML, ActiveSync, Z-Push…).

2.2 Protocolos y estándares

2.2.1 SMTP:

[8] El objetivo de SMTP (Simple Mail Transfer Protocol) es transmitir correo de una manera eficiente y fiable. Principalmente, estas conexiones para enviar los correos electrónicos se realizan sobre TPC/IP (capa de aplicación).

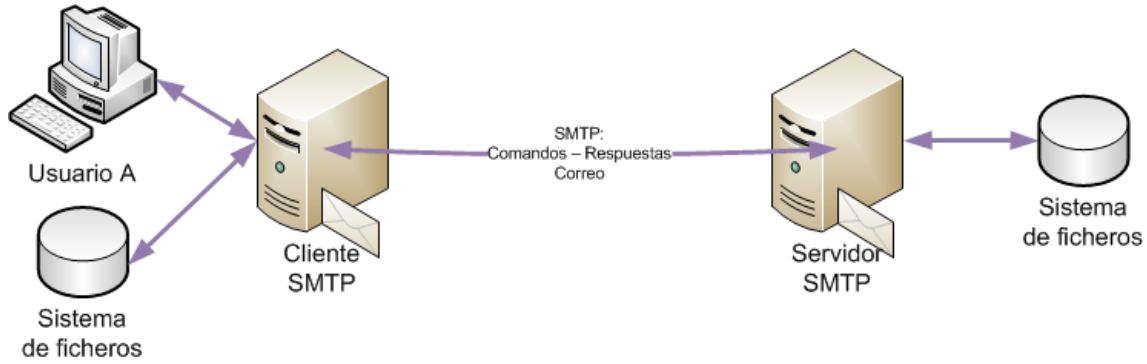

Figura 2 - Ejemplo de Envío de correo

Cuando un cliente SMTP tiene un mensaje que transmitir, se establece un canal de transmisión bidireccional hacia un servidor SMTP. La responsabilidad del cliente es transferir los mensajes de correo a uno o más servidores o reportar en caso de fallo.

Una vez que el mensaje está en el cliente SMTP, deberá localizar el servidor SMTP. Para ello hace uso de los servidores de nombres DNS. Una vez que el cliente obtiene la ruta, envía el correo al servidor y éste se encargará de entregarlo al resto de capas internas de la plataforma de correo.

El servicio SMTP se puede dar en los puertos TCP 25, 465 y 587.

Cuando se trata del 25, no hay identificación ninguna por parte del usuario. No está controlado el acceso por ese puerto.

Los puertos de presentación (o *submission*), el 587, y el securizado (SMTP over TLS), 465, son más seguros, y recomendables, ya que solicitan autenticación y comprueban si los usuarios están autorizados a mandar o no.

2.2.2 POP3

[9] Inicialmente, el servidor comienza el servicio POP3 (Post Office Protocol versión 3) escuchando en el puerto TCP 110. Cuando un cliente quiere hacer uso de este servicio establece una conexión IP con el servidor. El cliente y el servidor intercambian comandos y respuestas respectivamente hasta que la conexión finaliza.

Mientras esta conexión está activa, el cliente recupera la información que le interesa, los correos electrónicos, y la descarga del servidor.

POP3 tiene una gran ventaja, una vez que todos los correos electrónicos se han descargado al cliente, es posible la interacción con ellos sin conexión. Sin embargo, estas conexiones que realiza al servidor son muy lentas.

Por otra parte, el hecho de descargar el correo en el cliente, sólo te permite el acceso a esta información desde dicho cliente, es decir, tiene poca movilidad. Últimamente, muchos clientes tienen la opción de dejar una copia en el servidor, de modo que se los descargan pero continúan en el servidor. Esto es una mejora ya que en caso de que el cliente se corrompa (o deje de funcionar por cualquier motivo), podrán recuperar los correos del servidor, que en la mayoría de los casos hacen copias de respaldo (*backup*).

Como se ha comentado, tradicionalmente POP3 hace uso del puerto TCP 110. Mediante este puerto el acceso no es seguro y es propicio para que algún malware capture credenciales o sea capaz de leer correo del usuario. Por ello, los servidores de POP3 ofrecen la posibilidad de hacer que la conexión sea segura mediante TLS y SSL, a través del puerto 995.

2.2.3 IMAP4

[10] El protocolo IMAP (Internet Message Access Protocol) versión 4 revisión 1 permite al usuario acceder y manipular los mensajes de correo electrónico en un servidor, sin necesidad de descarga de los mismos. También permite la manipulación de los buzones como si estuvieran en carpetas locales. Además, ofrece la posibilidad de una conexión offline para resincronizar con el servidor.

IMAP4 incluye operaciones como crear, borrar y renombrar carpetas, comprobar correo nuevo, eliminar de manera permanente mensajes, crear y eliminar banderas, buscar atributos de mensajes…

Al no descargar los correos en local, permite al usuario acceder a su correo desde cualquier localización. Además, las conexiones son efímeras, sólo hace una pequeña conexión cuando se consulta un correo, el resto del tiempo permanece offline. Esto hace que no se consuma ancho de banda y que sea notablemente más rápido que POP3. Por otra parte, hace necesaria una conexión a internet cada vez que se quiera recuperar información, aunque sea por breve período de tiempo, aunque muchos clientes de correo cachean los

correos (cabeceras o cabeceras y cuerpos) para que, en caso de que se pierda la información, poder acceder al contenido de correos.

El puerto por defecto de IMAP es el TCP 143. Mediante este puerto el acceso no es seguro y es propicio para que algún malware capture credenciales o sea capaz de leer correo del usuario. Por ello, los servidores de IMAP ofrecen la posibilidad de hacer que la conexión sea segura mediante TLS y SSL, a través del puerto 993.

2.2.4 FTP

[11] Los objetivos de FTP son: promover la compartición de archivos/ficheros (programas de ordenador y/o datos), estimular indirecta o implícitamente el uso de ordenadores remotos (mediante programas), asegurar a un usuario de las variaciones de los sistemas de almacenamiento de ficheros entre los servidores, y transferir datos de manera eficiente y fiable. Aunque muchos usuarios hacen uso de FTP, está diseñado principalmente para que sean los programas quienes lo utilicen.

El servicio de FTP es ofrecido por la capa de aplicación del modelo TCP/IP, utilizando normalmente los puertos 20 y 21.

Está diseñado para ofrecer la máxima velocidad en la transferencia, pero no la máxima seguridad (la autenticación de los usuarios se realiza en texto plano, sin cifrado), por lo que es vulnerable a ataque para capturar tráfico y, con ello, credenciales y archivos.

Para solucionar este problema, se puede hacer uso de SCP y SFTP, incluidas en SSH, que permiten transferir archivos pero cifrando todo el tráfico.

2.2.5 HTTP

[12] El HTTP (Hyper-Text Transfer Protocol) es un protocolo del nivel de aplicación para sistemas de información distribuidos y colaborativos. Es un protocolo genérico y sin estado (no guarda información sobre conexiones anteriores) que puede ser empleado más allá de su uso para el *hipertexto*, como para servidores de nombres o sistemas de administración de objetos distribuidos, a través de los métodos de petición, códigos de error o cabeceras.
HTTP se ha estado empleando por la iniciativa World-Wide Web (WWW) desde 1990.

Muchas aplicaciones web requieren frecuentemente mantener el estado sobre conexiones anteriores, pero al ser HTTP un protocolo sin estado, se hace uso de las cookies (información que un servidor puede almacenar en el sistema cliente).

Este protocolo opera a través del puerto TCP 80. Estas transacciones que se lleven a cabo mediante este puerto, pudiendo ser víctimas de algún ataque para hacerse con información. Por ello, se creó una versión segura de este protocolo, HTTPS, sobre el puerto TCP 443. Con ello, se logra que toda la información sensible que se haya intercambiado en las transacciones esté cifrada y no pueda ser utilizada por un atacante que haya interceptado datos de la conexión.

2.2.6 HTML

[13] El HTML (Hyper-Text Markup Language) es un simple lenguaje de marcado (uso de etiquetas) usado para crear documentos de *hipertexto* independiente de las plataformas que se usen. Son documentos con una semántica genérica apropiada para la representación de

información. El marcado HTML puede representar noticias, correo, documentación, menús de opciones, resultados de consultas a bases de datos…

HTML ha sido empleado por la World-Wide Web (WWW) desde 1990, y dedicado a estandarizar casi todas las tecnologías ligadas a la web, sobre todo en lo que se refiere a su escritura e interpretación.

Basa su filosofía en la referenciación. Es decir, no añade directamente un elemento en el código de la página, si no que se hace una referencia a su ubicación.

Su compatibilidad con los diferentes dispositivos y navegadores está sujeta a las actualizaciones de HTML con la de dichos dispositivos y navegadores. Así pues, un navegador no actualizado no será capaz de interpretar correctamente una página web escrita en una versión de HTML superior a la que pueda interpretar, obligando a los desarrolladores a aplicar técnicas y cambios que permitan corregir problemas de visualización e incluso interpretación de código HTML.

2.2.7 WWW

Sistema de distribución de información basado en *hipertexto* accesible desde Internet.

2.2.8 MIME

[14] MIME (Multipurpose Internet Mail Extensions) es una especificación para dar formato a mensajes no ASCII de manera que puedan ser enviados a través de Internet. La mayoría de clientes de correo electrónico soportan MIME, lo que les permite enviar y recibir gráficos, audios y vídeos a través de Internet. Además, MIME soporta otros tipos de codificación de caracteres a parte de ASCII.

Hay muchos tipos de MIME predefinidos, como los archivos gráficos GIF o los ficheros PostScript. Además permite que un usuario defina sus propios tipos MIME.

Los navegadores Web también soportan varios tipos MIME. Esto permite al navegador mostrar o imprimir ficheros que no están en formato HTML.

Esta especificación se definió en 1992, aunque existe una nueva versión que soporta mensajes cifrados/encriptados, S/MIME.

2.2.9 Sieve

[15] Sieve (‘colador’ en español) es un lenguaje para el filtrado de mensajes de correo electrónico en tiempo de entrega final del mensaje, al buzón. Está diseñado para implementarse tanto en el cliente de correo como en el servidor. Trata de ser extensible, simple e independiente del protocolo de acceso, arquitectura de correo o sistema operativo. Es apropiado para ejecutarse en un servidor de correo donde los usuarios no estén autorizados a correr programas para filtrar mensajes.

Como está orientado a los usuarios, ofrece facilidad de uso. Este lenguaje se ha creado lo suficientemente simple como para que la gran mayoría de usuarios lo utilicen, pero también rico para poder usarse de manera eficaz. Sin embargo, un gran número de usuarios prefieren editar los filtros con editores gráficos (GUI).

2.2.10 SSL

[16] SSL (Secure Sockets Layer) es un protocolo desarrollado por Netscape para transmitir documentos privados a través de Internet. Hace uso de sistemas criptográficos que emplean dos claves para encriptar la información: una clave pública conocida por todos y una clave privada conocida sólo por el receptor de los datos.

2.2.11 TLS

[17] TLS (Transport Layer Security), protocolo sucesor de SSL cuyo principal objetico (mejorando SSL) es proporcionar integridad y privacidad de los datos entre dos aplicaciones conectadas. El protocolo está compuesto por dos capas: el registro de protocolo TLS y el protocolo de "apretón de manos" (*handshake*).

Una ventaja del TLS es que no depende del protocolo de la aplicación. Sin embargo, el estándar no especifica cómo añaden la seguridad con TLS los protocolos, las decisiones de cómo iniciar TLS y cómo interpretar el intercambio de certificados se dejan a juicio de los diseñadores de los protocolos que corren por encima de TLS.

2.2.12 LDAP

[18] El LDAP (Lightweight Directory Access Protocol) es un protocolo de Internet para un acceso a servicios de directorio distribuidos siguiendo el modelo X.500. Entendiendo directorio como un conjunto de objetos con atributos organizados en una manera lógica y jerárquica denominada DIT (árbol de información de directorio).

Cada entrada en el directorio LDAP corresponde a un objeto, abstracto o real. Estas entradas están compuestas por un conjunto de atributos que permiten caracterizar el objecto que la entrada define. Las entradas se indexan mediante un nombre completo (DN) que permite identificar de manera única un elemento de la estructura del árbol.

El conjunto de definiciones de objetos y atributos que un servidor LDAP puede administrar se denomina esquema. Esto permite definir si un atributo puede poseer uno o más valores. Además, existe un atributo llamado *objectClass* que permite definir si los atributos son obligatorios u opcionales.

LDAP tiene un formato de fichero (LDIF: LDAP Data Interchange Format) con el que se pueden realizar diferentes acciones sobre un directorio LDAP (añadir, modificar, eliminar…).

En el presente PFC se empleará la versión libre OpenLDAP.

2.2.13 SyncML

[19] SyncML (Synchronization Markup Language) es un protocolo de la familia de XML usado para proveer sincronización remota para dispositivos móviles. Al ser XML, todos los dispositivos compatibles podrán entender este estándar.

Se usa para sincronizar datos entre diferentes dispositivos (teléfonos, ordenadores…), como contactos, agendas, tareas…

Funciona sobre diferentes tipos de conexiones, Wireless, Bluetooth o Infrarrojos.

2.2.14 ActiveSync

Es un software para móviles Windows que permite sincronizar Windows Mobile y otros dispositivos Windows CE con un PC con Windows o un servidor Exchange.

2.2.15 TCP/IP

[20] El modelo TCP/IP (Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos utilizados para conectar hosts en Internet. TCP/IP usa varios protocolos, los dos principales con el TCP y el IP. Está desarrollado en sistemas operativos UNIX y es usado por internet, haciendo que sea el estándar para la transmisión de datos entre redes.

Describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse con otra red. Provee conectividad extremo a extremo, especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el usuario.

Consta de 4 capas de abstracción [21] similar al modelo OSI [22].

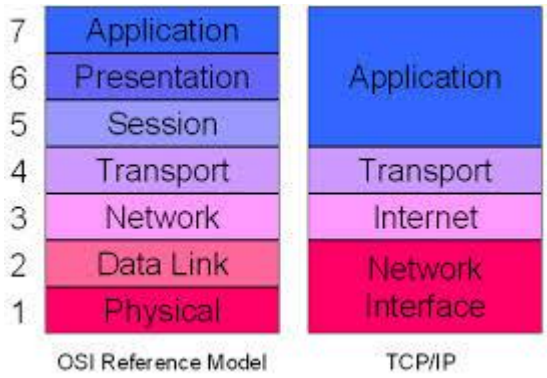

Figura 3 - Capas OSI vs Capas TCP/IP

Estas capas están jerarquizadas, y cada una se construye sobre su predecesora. Cada capa debe proveer servicios a las capas superiores de manera transparente. Así, cada capa debe ocuparse exclusivamente de su nivel inmediatamente superior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

2.2.16 DNS

[23] DNS (Domain Name Server/Service) es un servicio de Internet que traduce nombres de dominio a direcciones IP. Esto se hace porque los nombres de dominio son alfabéticos y son más fáciles de recordar que las direcciones IP, que es en lo que está basado Internet. Por tanto, cada vez que se introduce un nombre de dominio, un servidor DNS deberá traducir ese nombre a la correspondiente dirección IP. Por ejemplo, el nombre *smtp.uam.es* se traduce a la dirección IP *150.244.214.241*.

El sistema DNS tiene su propia red, es decir, si un DNS no sabe cómo traducir cierto nombre en particular, preguntará a otro DNS, hasta que le conteste uno con la dirección IP correcta.

2.2.17 NAT

[24] El NAT (Network Address Translation) es un estándar de Internet que permite a una red local (LAN) hacer uso de un rango de direcciones IP para tráfico interno y un segundo rango de direcciones para el tráfico externo. Permite mapear direcciones IP de un rango/grupo a otro, siendo transparente para los usuarios finales.

Las principales características de un servicio de NAT son: ofrecer un comportamiento parecido a un cortafuegos escondiendo direcciones IP internas, permitir a las compañías utilizar diferentes direcciones IP internas (para no entrar en conflicto con otras redes privadas de otras compañias) o permitir a una compañía múltiples conexiones RDSI en una sola conexión a Internet.

2.2.18 Listas blancas/negras/grises

En el tráfico de correo electrónico, existen las llamadas listas negras, listas blancas y listas grises, que definirán el comportamiento de los servidores de correo hacia determinadas direcciones de correo electrónico y/o direcciones IP.

Una lista blanca es una lista de servidores, direcciones de correo electrónico o direcciones IP que automáticamente se considerarán emisores válidos y, por tanto, aceptarán todo el correo de esas fuentes. Por ejemplo, no se actuará con estas direcciones con listas grises, o chequeos de virus/SPAM… Aunque sí se recomienda hacer estos últimos.

Una lista negra es una lista de clientes a los que se les deniega el acceso a un cierto servicio. En el caso de un servidor de correo, esto es una lista de direcciones de correo, servidores y direcciones IP a las que el servidor automáticamente rechaza toda conexión.

Las listas grises no se mantienen automáticamente por una persona, sino que es una lista de servidores, direcciones de correo y direcciones IP que recientemente han intentado acceder/mandar correo al servidor. Aunque el correo parezca correcto, para estar seguros, se solicita al servidor que vuelva a enviar el correo electrónico, de este modo se evita que sean errores temporales o de SPAM, pues este tipo de correo no es enviado con MTAs convencionales y, por tanto, no hará el reintento de envío (se asume que no reintentarán el envío).

Así pues, en un principio, y hasta que las diferentes fuentes de envío de correo entren en las listas blancas, todos los correos se retrasarán un corto período de tiempo, configurable.

Por otra parte, existen las llamadas listas de reputación (RBL). Son listas albergadas en servidores de confianza que contienen sitios web o dominios con mala reputación debido a su alto contenido de SPAM, virus… Muchos servidores de correo consultan estas listas para saber si deben o no aceptar las conexiones de un determinado sitio.

2.2.19 Antivirus

Un virus informático es un programa o trazas de código que se cargan en el ordenador o dispositivo sin conocimiento del propietario y se ejecuta de manera transparente. Además, los virus pueden replicarse a sí mismos. Todos los virus informáticos son creados por técnicos con alta experiencia en desarrollo de software.

Un simple virus puede hacer copias de sí mismo todo el rato es fácil de crear. Incluso el virus más simple es peligroso pues rápidamente carga la memoria y la carga de la máquina

llevándola a colapsarla. Aún son más peligrosos los que son capaces de transmitirse a través de las redes saltándose los sistemas de seguridad.

Desde 1987, cuando un virus infectó ARPANET, se han desarrollado numerosos programas antivirus. Los antivirus son una utilidad que buscan en los sistemas estos virus y los eliminan cuando son encontrados. La mayoría de los antivirus incluyen una actualización automática de su base de datos para permitir que se descarguen información y eliminación o neutralización de nuevos virus, con el fin de mantener la protección ante nuevas amenazas.

En los últimos años, han proliferado unos ciertos tipos de virus, denominados troyanos, que recopilan información de usuario a través de su conexión a internet sin su conocimiento ni consentimiento, principalmente para propósitos comerciales. Suelen estar alojados en aplicaciones gratuitas o de prueba.

Existen numerosas soluciones de antivirus, algunas más efectivas que otras, y con la posibilidad de decantarse por programas de pago (Kaspersky, Panda, Norton, Sophos…) o gratuitas (AVG, Avast!, ClamAV, AD-Aware...). Lógicamente, las de pago ofrecen más posibilidades de protección.

2.2.20 Anti-SPAM

El SPAM es comúnmente conocido como correo electrónico no deseado o correo basura. Normalmente trata sobre productos comerciales.

El SPAM, al ser enviado masivamente, puede llegar a consumir ancho de banda de las conexiones, así como aumentar la carga de los servidores considerablemente.

[Como curiosidad, el término SPAM proviene del corto homónimo de los Monty Python, pues se trata de texto repetitivo y sin interés].

En cuanto a sistemas anti-SPAM, como se ha comentado antes, la mayoría de los antivirus poseen esta característica. Sin embargo, para servidores de correo y software gratuito, se pueden destacar dos grandes aplicativos: DSPAM y SpamAssassin (que también pueden trabajar juntos en un mismo servidor).

[25] DSPAM es un software anti-SPAM que puede almacenar información de clasificación en bases de datos, empleando filtros *bayesianos* entre otros, para aprender y adaptarse a los correos de SPAM.

SpamAssassin es un programa anti-SPAM de Apache basado en reglas de equivalencia de contenidos. Es fácilmente integrable con los servidores de correo e incluye detección por DNS, filtros bayesianos, listas negras, etc. [26]

Estos sistemas anti-SPAM siempre requieren un cierto entrenamiento. Esto es, crearse una base de datos de plantillas y cadenas que suele haber en este tipo de correos. Este entrenamiento suele completarse con la ayuda de usuarios de la plataforma, catalogando correo legítimo como SPAM.

2.2.21 DKIM

[27] DKIM (DomainKeys Identified Mail) es un método de autenticación de correo electrónico que permite a un usuario u organización responsabilizarse del envío de un mensaje, de manera que éste pueda ser validado en el destinatario.

DKIM utiliza criptografía de clave pública para permitir al origen firmar electrónicamente correos legítimos de manera que puedan ser verificados por los desinatarios.

También protege contra la manipulación de correo electrónico, proporcionando integridad extremo a extremo.

2.2.22 SPF

[28] SPF (Sender Policy Framework) es una extensión de SMTP que detiene los correos SPAM de crear el campo *From* de los mensajes. Como SMTP en sí no contiene mecanismos de autenticación, esta extensión provee de cierta autenticación especificando qué servidores están autorizados a enviar correo de determinados dominios. Para poder hacer uso de SPF, se deberán registrar estos servidores en los DNS. Entonces, cuando se envía un correo, se comparará el registro con los almacenados en los DNS y se comprobará si está autorizado o no. En caso de que no encuentra tal registro, el correo no se redirigirá a ninguna estafeta.

SPF puede utilizarse para para evitar que se mande SPAM desde dominios no autorizados.

2.3 Elementos software de la plataforma de correo

2.3.1 MUA

El Agente de Correo de Usuario (MUA: Mail User Agent) hace referencia a los propios clientes de correo electrónico, que permiten la visualización y envío/recepción de mensajes. Este software se instala en la máquina cliente y habrá que configurarlo para que sea capaz de recuperar/leer el correo de los servidores. Además, en la mayoría de los casos, también se deberá configurar el servidor de correo saliente.

Los más comunes son KMail, Evolution, Mozilla Thunderbird, Microsoft Outlook… Entre estos clientes no existen sustanciales difrerencias y su uso dependerá de las preferencias de los usuario (funcionalidades, coste…).

2.3.2 MTA

El Agente de Transferencia de Correo (MTA: Mail Trasnfer Agent) es el software encargado de transmitir mensajes de correo electrónico de una máquina a otra haciendo uso del estándar SMTP. Los MTA proporcionan bidireccionalidad, es decir, son capaces de enviar y recibir dichos mensajes.

Aunque la entrega de mensajes entre máquinas puede parecer simple, todo el proceso de decisión si un MTA particular puede o debería aceptar un mensaje para la entrega es bastante complicado. Además, debido a los problemas de SPAM, el uso de un MTA particular, por lo general está restringido por la configuración del MTA o la configuración de acceso a la red en la que reside el MTA.

Numerosos clientes de correo modernos pueden actuar como un MTA para enviar correo electrónico. Sin embargo, esta acción no debe confundirse con un verdadero MTA. La única razón de que los clientes de correo son capaces de enviar mensajes como un MTA se debe a que el servidor que ejecuta la aplicación no tiene su propio MTA. Esto es particularmente cierto para los programas cliente de correo electrónico en los sistemas operativos que no están basados en UNIX. Sin embargo, estos programas clientes sólo envían mensajes salientes a un MTA para el cual están autorizados a utilizar y no entregan el mensaje directamente al servidor de correo electrónico del destinatario.

Como Red Hat Enterprise Linux instala dos MTAs, Sendmail y Postfix, a menudo no se requieren MTA para los clientes de correo electrónico. Red Hat Enterprise Linux también incluye un MTA de propósitos especiales llamado Fetchmail.

A menudo se integran dos capas de MTA (o más), para darle más granularidad y seguridad, pero también aumenta considerablemente la dificultad de una configuración. Además de que de este modo se introduce un punto más de fallo.

A continuación se van a repasar los MTA más usados: Sendmail, Postfix, Exim y Qmail.

2.3.2.1 Sendmail

Figura 4 - Logo Sendmail

[29] [30] MTA compatible con sistemas UNIX y responsable de la mayoría de envío de correo electrónico a través de internet. Sin embargo, es criticado por el alto número de alertas de seguridad, así como la dificultad de configuración, en caso contrario habría muchos mensajes legítimos rechazados o rebotados.

2.3.2.2 Postfix

Figura 5 - Logo Postfix

[31] [32] Se trata de un MTA que se creó como alternativa a Sendmail. Es rápido, fácil de administrar y seguro. El comportamiento es muy similar a Sendmail, pero por dentro es completamente diferente.

Es compatible con AIX, BSD, HP-UX, IRIX, LINUX, MacOS X, Solaris, Tru64 UNIX y otros sistemas UNIX. Requiere librerías ANSI C y sockets BSD, además de otros requisitos dependiendo de las características que se usen.

En cuanto a las características, se puede controlar el correo basura (listas blancas DNS, Greylisting, control SPF, control de acceso por tasas de cliente…), gran cantidad de protocolos soportados (HAProxy, Nginx proxy, DKIM, DSN, SASL, IPv6, TLS…), formatos mailbox y Maildir, dominios virtuales, enmascaramiento, gran cantidad de bases de datos soportadas (LMDB, Memcache, SQLite, CDB, PostgreSQL, LDAP, MySQL…), reescritura de direcciones…

2.3.2.3 Exim

Figura 6 - Logo Exim

[33] [34] MTA desarrollado para sistemas UNIX. Es muy flexible en cuanto a la manera en la que el correo electrónico puede ser enviado, y hay amplias opciones para tratar el correo entrante. Se puede instalar también en lugar de Sendmail, pero la configuración de Exim es muy diferente.

A pesar de que su diseño monolítico se considera menos seguro y lento, los registros de seguridad de Exim son mucho mejores que Sendmail en comparación con Qmail y Postfix, así como su velocidad. Su rendimiento en el manejo de colas, enrutado de direcciones y pruebas es espectacular.

Exim es altamente configurable, y por tanto tiene características de las que otros MTA carecen. Tiene muchas opciones para controles de política, así como introducen ACL permitiendo un control muy flexible del sistema. Esta configuración es bastante extensa, y permite la creación de los llamados "router" que se encargan del procesado de mensajes, si cumplen ciertas condiciones, los "transport" que se encargan de encaminar el correo dependiendo de qué políticas haya o no pasado, la sección de reintento define qué hacer con los mensajes que han fallado en el primer intento, la sección de reescritura describe cómo reescribir las direcciones de correos electrónicos entrantes, la sección de autenticadores contiene información relativa a SMTP AUTH para cada mecanismo de autenticación.

El único inconveniente no rinde muy bien en entornos donde la cola crece mucho. Pero no está diseñado para esto, ya que los correos encolados no suelen (o no deberían) ser normales en el funcionamiento normal de una plataforma de correo.

2.3.2.4 Qmail

Figura 7 - Logo qmail

[35] [36] MTA seguro, fiable, eficiente y simple desarrollado también para sistemas UNIX. En 2001 era el segundo servidor SMTP más común en Internet, habiendo crecido y evolucionado considerablemente desde entonces. A continuación se especifican las principales características:

La seguridad no es un objetivo sino un requerimiento absoluto. La entrega de correo es crítica para los usuarios, al no poderse desconectar debe ser completamente seguro.

En cuanto a fiabilidad, la filosofía de Qmail es garantizar que el mensaje, una vez que se acepta en el sistema, no se pierde. Soporta Maildir, además de mbox y MH, que garantiza que el buzón no se corrompe si el sistema falla durante la entrega. Aún más, no sólo los usuarios pueden leer de manera segura su correo por NFS, si no que varios clientes NFS pueden entregar el correo a un buzón al mismo tiempo.

Qmail es bastante más simple que otros MTA. Otros agentes tienen mecanismos separados de forwarding, aliasing y listas de distribución. Qmail sólo un sencillo mecanismo de forwarding que permite a los usuarios administrar sus propias listas de distribución.

Mientras otros MTA tienen muy diversos tipos de entrega de correo (desde rápido-inseguro hasta lento-encolado), Qmail trata de manera inmediata los elementos de la cola, teniendo por tanto un único modo de entrega, rápido-encolado.

Además, el diseño de Qmail hace que la carga de la máquina esté limitada así que puede ejecutarse de manera segura desde el *inetd* (demonio que atiende las solicitudes de conexión, cuantas menos conexiones menos carga) del sistema.

El gran problema de Qmail es que ya no tiene soporte y el creador no permite que otros desarrolladores saquen nuevas versiones. Además, no es completamente OpenSource.

2.3.2.5 Comparativa MTA

Una vez que se han analizado a grandes rasgos los 4 principales MTA existentes, se va a proceder a la elección de uno (o varios) para implantarlo en la plataforma de correo electrónico.

Sendmail se rechazará debido a los problemas de seguridad que presenta y porque según se profundiza más en él, más complicado se pone.

Postfix es una muy buena opción debido a su nivel de seguridad, la fácil administración y eficiencia. Además de las grandes posibilidades de configuración, así como su integración con sistemas antivirus (ClamAV) y anti-SPAM (DSPAM y/o Spamassassin). Postfix dispone de una amplia y clara documentación sobre su configuración y administración.

Exim es una buena solución ya que es muy genérico y se puede implantar en prácticamente todos los servidores (en Windows tiene la posibilidad de implantarlo en Cygwin). Además, las posibilidades que ofrece con los "router" y "transport" son muchas y variadas. Exim dispone de una amplia y clara documentación sobre su configuración y administración.

Qmail es muy seguro, pero a la vez antiguo y muy complicado de configurar si se quieren todas las características de forwarding y listas de distribución.

Por tanto, y una vez revisados estos agentes, se optará por una solución de dos capas: una primera que será Postfix, y una segunda que será Exim. Además, de este modo evitamos que Exim encole muchos correos.

2.3.2.6 Ironport

Figura 8 - Logo Ironport

A pesar de que Ironport no es en sí misma un MTA ni es de software libre, se va a comentar a grandes rasgos sus principales características puesto que será un elemento importante de la plataforma de correo electrónico a implantar en el presente PFC. La empresa Ironport fue adquirida recientemente por Cisco.

La pasarela de mensajes Ironport es un aplicativo diseñado para satisfacer las necesidades de una plataforma de correo de las redes más exigentes. Ironport elimina el SPAM y los virus, aplica la política corporativa, asegura la entrada/salida de la red y reduce el coste total de una infraestructura de correo electrónico, debido a que incluye muchos productos en uno (MTA, antivirus, anti-spam, políticas…).

El sistema Ironport combina hardware, un sistema operativo robusto (AsyncOS), la propia aplicación de Ironport, y servicios de auto-soporte para administrar fácilmente la estructura implementada.

Incluye las siguientes características:

- Anti-Spam, con ayuda de filtros de reputación basados en remitente único de Ironport, incorporando sistemas de anti-spam tanto de Ironport como de Symantec Brightmail Anti-Spam
- Anti-Virus, con los motores de escaneado de Sophos y McAfee.
- Filtros de intrusiones de virus, que es un sistema único de Ironport, ofrece protección preventiva contra nuevos ataques de virus que pueden poner en cuarentena mensajes peligrosos hasta nuevas actualizaciones de anti-virus, reduciendo así la vulnerabilidad contra nuevos virus.
- Cuarentena de Spam, ofreciendo acceso al usuario final de acceso a este correo en cuarentena.
- Autenticación de un email mediante DomainKeys y DKIM, firmando correo saliente y verificando correo entrante.
- Encriptación de correo de Ironport. Se pueden cifrar los correos salientes para abordar HIPAA (EEUU), GLBA (EEUU) u otras entidades reguladoras.
- Administrador de Seguridad de Correo, mediante una interfaz simple se puede administrar todos los servicios de seguridad de correo y los diferentes módulos de la aplicación. Se pueden configurar reglas de seguridad a correos basadas en grupos de usuarios, para administrar los filtros de reputación, anti-spam…
- Áreas de cuarentena on-box, para mantener los mensajes que violan las políticas de correo.
- Seguimiento de mensajes on-box. Esta propiedad es muy útil a la hora de encontrar rápida y fácilmente el estado del mensaje que se ha procesado.
- Monitorización del flujo de correo, de todos los correos entrantes y salientes, ofreciendo una completa visibilidad de todo el tráfico de la organización.
- Control de acceso, para los remitentes de correo entrante, basados en la dirección IP, rango de IP o dominio.
- Filtrado de mensajes extensivo, permitiendo aplicar políticas corporativas e interactuar con los diferentes correos que entran o salen de la organización. Las reglas del filtro identifican mensajes basándose en el mensaje o adjunto, información de la red, cabeceras, cuerpo… Las acciones del filtro, permiten descartar los mensajes, rebotarlos, archivarlos, enviar notificaciones…
- Cifrado de mensajes vía SMTP seguro sobre TLS, asegurando que los mensajes se envían entre la organización y el destinatario de manera cifrada.
- Pasarela Virtual. Esta tecnología de Ironport permite que el servidor actúe como varias pasarelas dentro de un mismo servidor, facilitando así el tratamiento de correo electrónico de diferentes fuentes o para ser enviados a IP diferentes. Asegurándose que si ocurre algún problema de entrega con cierta IP no afecte a las demás.
- Verificación SPF y SIDF. SPF y SIDF son métodos para verificar la autenticidad del correo electrónico basándose en registros DNS. SPF permite al propietario de un dominio de internet usar formatos especiales de registros DNS TXT para especificar qué máquinas están autorizadas a transmitir correo electrónico en ese dominio.
- Los servidores de Ironport son fácilmente integrables con cualquier infraestructura de correo electrónico. Es decir, es compatible con cualquier elemento de una plataforma de correo: MDA, MTA, LDAP…

- La alta disponibilidad está soportada por Ironport. Se puede configurar con la herramienta de interfaz gráfica como por línea de comandos, y soporta tanto activo/activo como activo/pasivo.
- Los Ironport proporcionan un alto rendimiento en el tratamiento de correo electrónico, pudiendo manejar diariamente miles de correos de manera sencilla y sin que el sistema se resienta.
- La centralización de la infraestructura de varios Ironport en clúster es posible siempre que éstos sean la misma versión de servidor y sistema operativo AsyncOS, y tengan nombres que se resuelvan por DNS. Una vez en clúster, se pueden comunicar por SSH o por el Servicio de Comunicación de Clúster (CSS).
- La interfaz gráfica de usuario (GUI) es una alternativa web a la interfaz por línea de comandos (CLI) para la configuración y monitorización del sistema. De este modo, no será necesario el uso de todos los comandos existentes en el AsyncOS. La interfaz gráfica contiene la mayor parte de la funcionalidad necesaria para configurar y monitorizar el sistema. Sin embargo, no están presentes todos los comandos existentes desde línea de comandos, es decir, algunas características están sólo mediante línea de comandos.
- La línea de comandos de AsyncOS de Ironport es una interfaz interactiva diseñada para permitir la configuración y monitorización de la solución Ironport. Dependiendo del comando, puede requerir argumentos. La consola es accesible mediante SSH o Telnet, a través de los puertos previamente configurados. Por defecto, estos servicios están configurados en el puerto de Administración. Mediante el comando *interfaceconfig* se puede deshabilitar estos servicios.
- La solución de Ironport ofrece comandos para permitir la monitorización de las operaciones del correo electrónico sin analizar los logs. Se puede monitorizar mediante la línea de comandos o la interfaz gráfica. La mayoría de los comandos están disponibles en la GUI.
- Una característica importante de la solución de Ironport. AsyncOS puede generar muchos tipos de logs, registrando diferentes tipos de información. Los ficheros de log contienen los registros de las operaciones normales y las excepciones de varios componentes del sistema. Esta información puede ser útil a la hora de monitorizar el aplicativo entero o resolver problemas o comprobar el rendimiento.
- El soporte se puede realizar desde la misma interfaz de red, mediante una herramienta de ticketing, chat con técnicos o por correo electrónico. Incluso, existe la posibilidad de que el técnico se conecte de manera remota para el análisis del servidor. Este soporte entra dentro de la licencia.
- Ironport, con las últimas versiones del sistema operativo AsyncOS, soporta completamente IPv6.
- La solución de Ironport no ofrece la posibilidad de *archiving*.

El reporte de problemas, la monitorización y los comandos de configuración están disponibles a través de la interfaz gráfica web (GUI) mediante HTTP o HTTPS, y a través de línea de comandos (CLI) accediendo por SSH, telnet o por conexión serie.

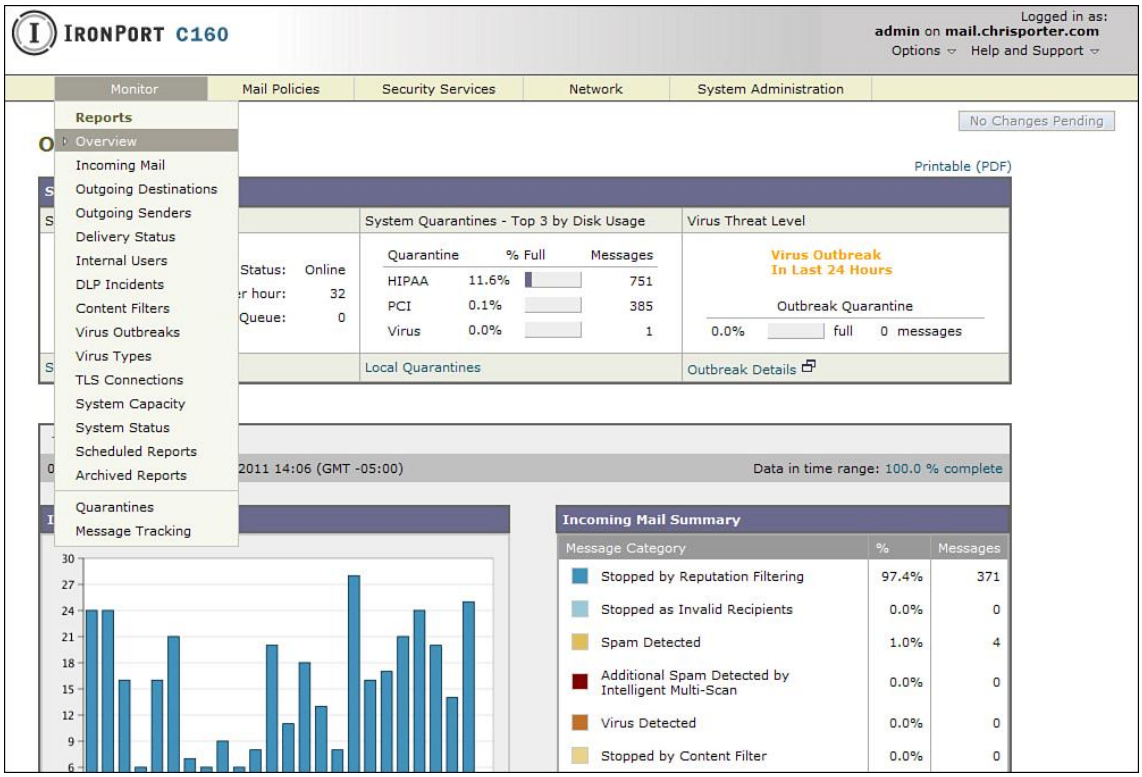

Figura 9 - Ironport GUI

Ironport proporciona herramientas de logging robustas con la posibilidad de seguimiento detallado, de mensajes, IP, ventanas de tiempo…

Documentación: [37] [38] [39] [40]

2.3.3 MDA

El agente de entrega de correo (MDA: Mail Delivery Agent) es un software que se invoca a través del MTA (Mail Transfer Agent) para hacer la entrega de los correos electrónicos a los buzones de usuarios locales. Comúnmente, los MDA actúan por ello también de LDA (Local Delivery Agent).

Todo programa capaz de tratar mensajes para la entrega hasta el punto en el que se pueden leer por un cliente de correo pueden considerarse MDA. Por esto, algunos MTA pueden asumir el papel de MDA cuando añaden los mensajes de correo al archivo de correo spool del usuario.

En general, los MDA no transportan mensajes entre sistemas ni ofrecen ningún tipo de interfaz de usuario. Distribuyen y ordenan los correos en el sistema (local o remoto – SSHFS, NFS… -) para que un cliente de correo electrónico acceda a estos buzones de usuario.

Existen numerosos MDA disponibles. Sin embargo, nos centraremos en los más empleados hoy en día: Dovecot, Courier-Maildrop, Cyrus y Procmail.

2.3.3.1 Procmail

Figura 10 - Logo Procmail

[41] MDA capaz de organizar el correo entrante en diferentes directorios y filtrar mensajes de SPAM. Se ha empleado mucho pero debido a que ya no se mantiene y no hay soporte, los usuarios y administradores de sistema han buscado otras opciones. La más adecuada para este tipo de usuarios es la de Maildrop.

No se ejecuta de manera normal, es decir, no es un proceso que esté siempre corriendo, sino que lo invocan otros agentes de envío/entrega de correo MTA.

El agente Procmail hace uso de recetas, que determinan dónde entregar los diversos mensajes de correo electrónico. Cada receta consta de un modo, condiciones y la acción.

El sistema anti-SPAM de Procmail lo lleva a cabo software de terceros, como puede ser SpamAssassin o DSPAM.

2.3.3.2 Courier-Maildrop

Figura 11 - Logo Courier IMAP

[42] Es un agente de entrega/filtrado de correo electrónico utilizado por Courier Mail Server. Si se tiene instalado este tipo de servidor, el agente viene por defecto con dicha instalación. Sin embargo, se puede integrar con otros servidores de correo electrónico.

Maildrop se encarga de leer los mensajes de correo entrantes y entregarlos en los buzones de usuario. Puede trabajar tanto con buzones MBOX como Maildir.

Tiene capacidades de filtrado. Esto lo realiza mediante la lectura e interpretación de un fichero donde se describen las diferentes reglas a aplicar al correo entrante. Estas reglas pueden guardar el correo en determinados buzones o reenviarlo hacia otra cuenta. Al contrario que en Procmail, Maildrop emplea un lenguaje de filtrado estructurado.

Está escrito en C++ y es significativamente más grande que Procmail. Sin embargo, es mucho más eficiente en cuanto a recursos se refiere. Por ejemplo, Maildrop no leerá mensajes de 10MB en memoria, sino que lo guarda temporalmente en un archivo. Esto no será necesario en el caso de que en lugar de que la entrada sea un archivo sea una tubería.

Maildrop comprueba la sintaxis de instrucciones de entrega de correo desde el archivo de filtros/reglas, antes de intentar entregar un mensaje. A diferencia de Procmail, si el archivo de filtros contiene errores de sintaxis, Maildrop terminará sin entregar el mensaje. El usuario puede corregir el error sin causar pérdida de correo.

2.3.3.3 Cyrus

Figura 12 - Logo Cyrus

[43] Sistema de correo altamente escalable diseñada para uso en entornos de empresas de diversos tamaños que utilizan tecnologías basadas en estándares. Se diferencia de otras implementaciones del servidor IMAP, ya que se ejecuta en los servidores "cerrados", donde los usuarios no suelen estar autorizados a autenticarse. La base de datos de buzón de correo se almacena en partes del sistema de ficheros que son privadas al sistema de IMAP Cyrus. Todo el acceso del usuario a través de correo electrónico es mediante los protocolos IMAP, POP3 o KPOP.

El servidor Cyrus IMAP (Internet Message Access Protocol) permite el acceso a correo electrónico personal y los tablones de anuncios de todo el sistema a través del protocolo IMAP.

Al tener una estructura individual para cada buzón, se le otorgan grandes ventajas de eficiencia, escalabilidad y administración. Además, se permiten lecturas/escrituras concurrentes en el mismo buzón. El servidor soporta ACL (Access Control Lists) en los buzones y control de cuotas.

Cyrus hace uso del estándar IMAP4. Este estándar es una mejora de otros protocolos de correo cuando se trata de escalabilidad y disponibilidad. El protocolo POP3 y similares son menos útiles cuando la base de datos de usuario es grande ya que está pensado para almacenar y redireccionar. Los clientes descargarán todo el correo del servidor en la máquina local. De este modo los mensajes no estarán disponibles en el servidor para que se pueda acceder desde otros clientes.

El protocolo IMAP4 añade a IMAP soporte para trabajo sin conexión. Esto permite al cliente descargar parte de un mensaje y mantenerlo en la máquina local.

Cyrus tiene la posibilidad de hacer uso de filtros para los correos entrantes mediante el lenguaje de filtrado denominado Sieve.

2.3.3.4 Dovecot

Figura 13 - Logo Dovecot

[44] Es un servidor de correo que soporta IMAP y POP3 para servidores Linux/Unix. Es rápido, fácil de configurar y no requiere una especial administración así como hace uso de muy poca memoria.

Es uno de los servidores IMAP con mejor rendimiento, soportando formatos de buzón mbox, Maildir y mdbox (formato propietario de Dovecot que permite un alto rendimiento de lectura/escritura en los buzones y potentes herramientas de administración). Estos buzones de indexan de manera transparente lo que le da a Dovecot un gran rendimiento así como gran compatibilidad con las herramientas de administración de buzones. Estos índices puede que se corrompan, pero Dovecot intenta solucionar todos estos tipos de problemas por sí mismo, aunque queden registros en los logs para el administrador.

Permite el acceso a los buzones e índices desde múltiples máquinas al mismo tiempo con gran rendimiento. Esto es, Dovecot funciona bien en sistemas de ficheros en clúster.

La autenticación de Dovecot es muy flexible y con muchas características, soportando diferentes directorios de autenticación y mecanismos. Además, permite que otros elementos de una plataforma de correo se autentiquen a través del backend de autenticación de Dovecot.

La implementación de Dovecot está muy orientada a la seguridad. Como curiosidad, decir que los desarrolladores ofrecen 1000€ a quien encuentre un agujero de seguridad [45].

Las posibilidades de Dovecot aumentan considerablemente debido a la gran cantidad de plugins existentes para este MDA.

2.3.3.5 Comparativa MDA

Tras haber realizado un repaso sobre las principales características de los MDA más famosos y usados, se procederá a hacer una última comparativa y seleccionar el que se empleará en el presente proyecto.

La opción de Procmail se descarta, debido a que ya no se da más soporte y es antigua. Se ha mencionado por historia.

Courier-Maildrop sería una buena opción pero si se integra con el resto de servidor Courier. Pero lo que se quiere es tener cierta dependencia de módulos dentro de la plataforma. Hay que decir que cuando el servidor Courier está bien configurado (es tedioso, ya que reparte ficheros de configuración por el sistema de ficheros, son complicados de administrar…) consta de muchas características únicas y muy funcionales.

Cyrus es un servidor IMAP bastante potente, y las opciones de las que consta son múltiples. Sin embargo, esto último hace que su configuración sea bastante complicada. Además, tiene muchos elementos no estándares, lo que le hace en ocasiones difícil la integración con otros módulos de la plataforma de correo electrónico.

Dovecot es el que mejor funciona para una organización con muchos usuarios (entre 15000 y 20000). Además, su implementación es muy sencilla, así como su administración. Funciona con los formatos mbox y Maildir, y con un nuevo formato propio mdbox que permite una amplia gama de herramientas de administración de buzones. El gran rendimiento y velocidad de Dovecot se debe al indexado de los buzones. Esto evita que cada vez que se abra un cliente para la consulta de correo, recorra todos los buzones para hacer un escaneo.

Otra ventaja de Dovecot frente al resto es la facilidad de interpretación de los logs que deja en el sistema.

Por esto, y las razones expuestas anteriormente, se implantará Dovecot en la plataforma de correo electrónico.

2.3.4 WEBMAIL

Una vez que se han seleccionado los diferentes agentes de la comunicación y transferencia de los mensajes de correo electrónico en la plataforma, hay que hacer la elección del front-end de la plataforma. Además del posible acceso mediante MUA, también se tiene que poder hacer vía web, esto es, Webmail.

Existen numerosas soluciones de Webmail. En este proyecto se revisarán Zarafa, Horde, RoundCube, Open Xchange, eGroupWare y Zimbra. [46]

2.3.4.1 Zarafa

Figura 14 - Logo Zarafa

[47] Zarafa es una solución de grupo de trabajo basada en la apariencia de Microsoft Outlook. El software se posiciona como un sustituto basado en web para Outlook, y por lo tanto ofrece características comunes, tales como un sistema de borrado parcial para recuperar correos electrónicos eliminados después de 30 días, y un mensajes de ausencia o "fuera de la oficina". Cuenta con una trabajada interfaz que incluye AJAX, visualización de pantalla dividida, y posibilidad de arrastrar y soltar.

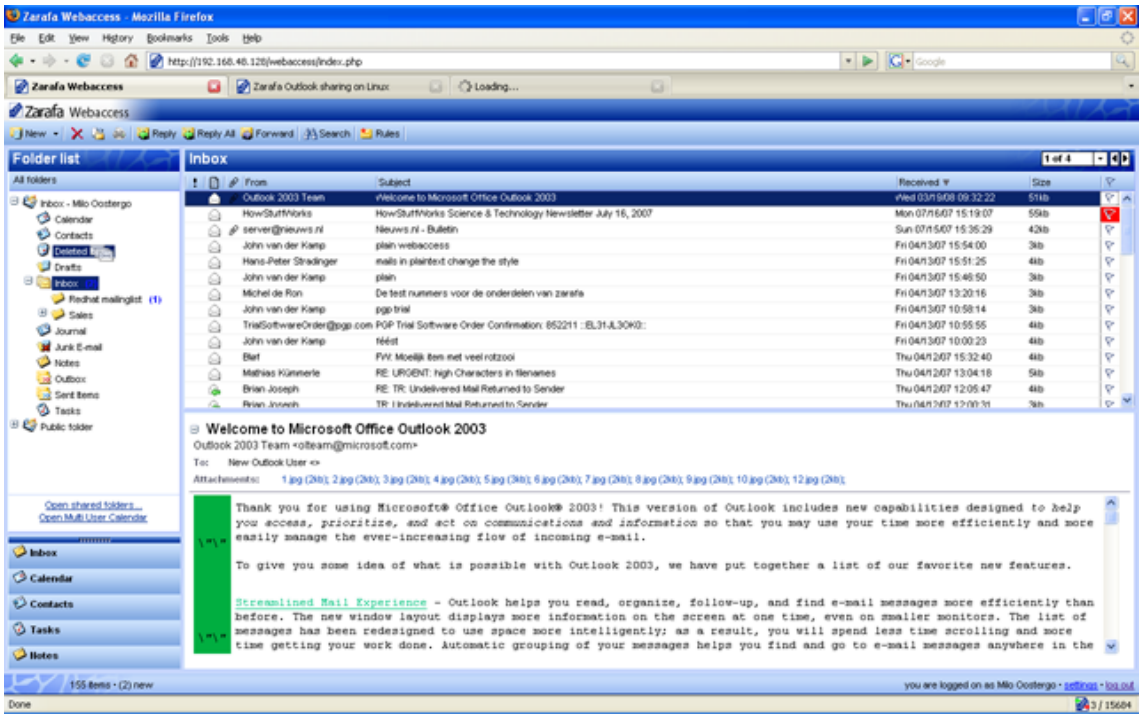

Figura 15 - Zarafa: Bandeja Entrada

Zarafa es bastante práctico para dar soporte a grupos. Justo debajo de la lista principal de la carpeta se encuentran hipervínculos para acceder a la información colaborativa en forma de carpetas compartidas o calendario multi-usuario.

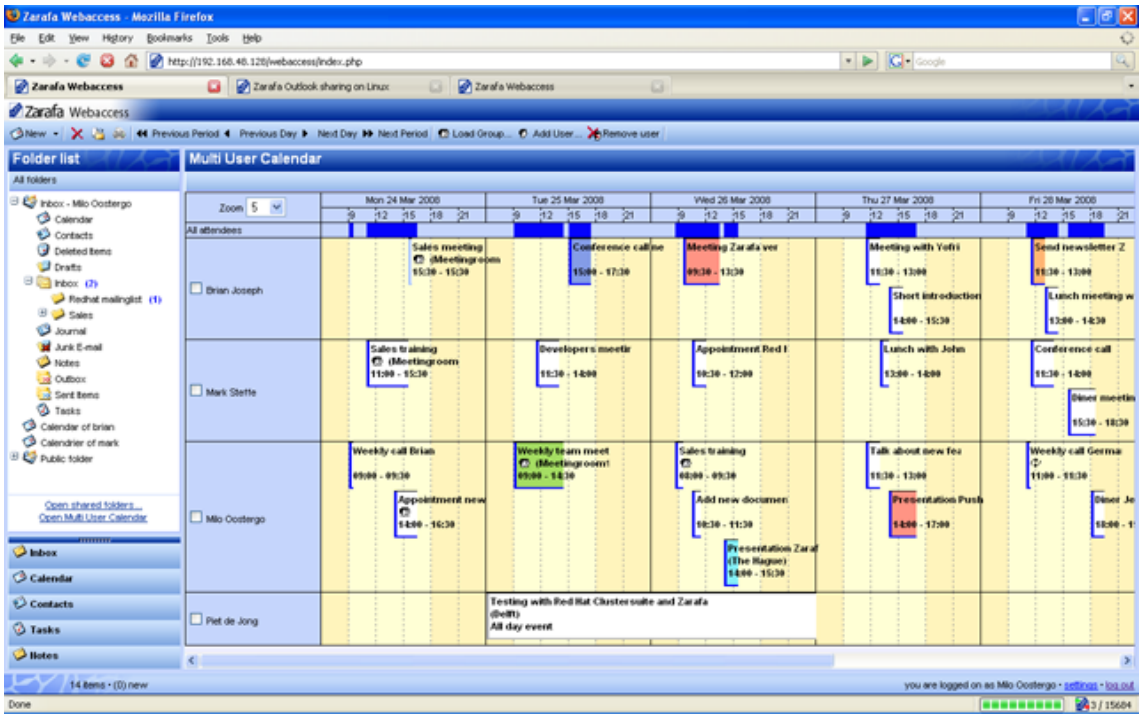

Figura 16 - Zarafa: Calendario

Proporciona un acceso rápido y fácil, seleccionando el enlace de carpetas compartidas muestra una ventana pop-up de los usuarios con carpetas públicas disponibles. Después de seleccionar un usuario, se añaden todas las carpetas públicas de ese usuario a su lista de carpetas. Sin embargo, actualmente, Zarafa sólo proporciona servicios de intercambio de mensajes de correo electrónico, calendarios y contactos, no los documentos, por lo que ofrece pocas opciones de colaboración.

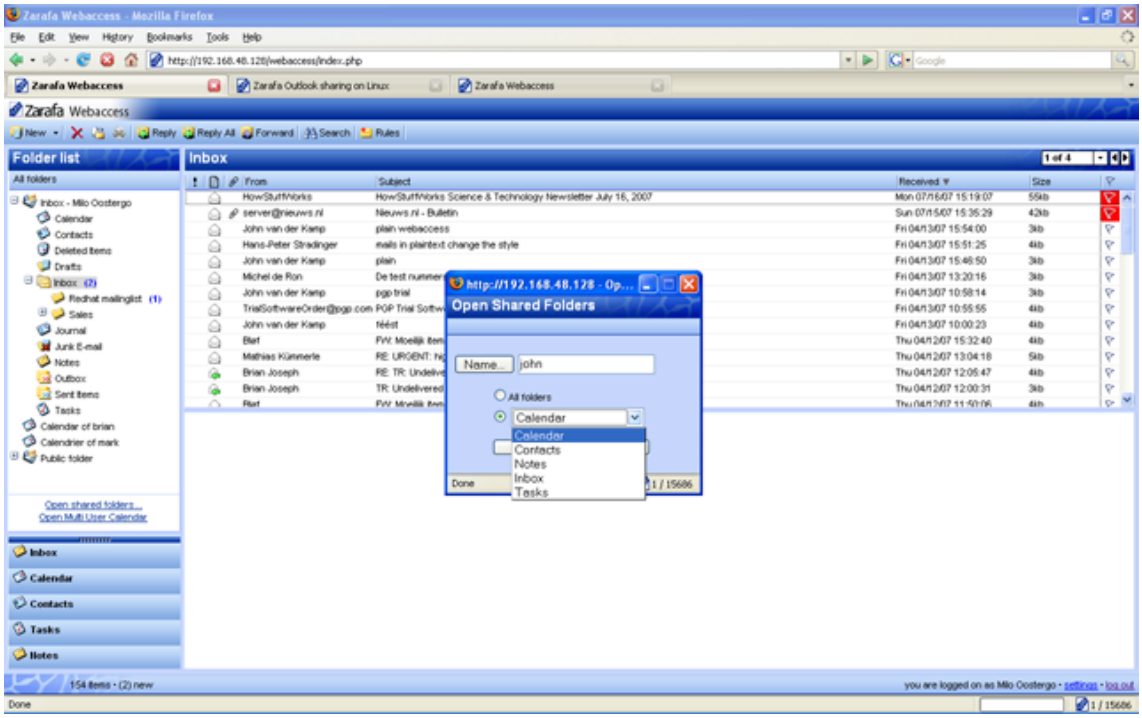

Figura 17 - Zarafa: Carpetas Compartidas

En cuanto a configuración y extensiones, Zarafa no tiene la posibilidad de añadir módulos, como los de Zimbra y Open-Xchange. El software está escrito en PHP, satisfaciendo la mayoría de los desarrolladores. Zarafa ofrece una herramienta de administración de línea de comandos que se utiliza para administrar usuarios y grupos, pero sin interfaz gráfica, la administración del Zarafa groupware puede llegar a ser tedioso e incómodo.

Un inconveniente del software Zarafa es que no lleva incorporado ningún sistema anti-SPAM ni antivirus, así que, para garantizar la seguridad, la solución tienen que estar integrados con software de terceros de anti-SPAM y antivirus (esto se hará en las estafetas de entrada/salida). A pesar de esto, Zarafa permite la conexión con el servidor mediante el protocolo HTTPS, lo que garantiza que todas las conexiones en la red se cifran antes de enviarse. Zarafa utiliza "AirSync", lo que le hace compatible con dispositivos móviles modernos.

A pesar de que en los foros existentes en la comunidad de Zarafa no son muy numerosos comparados con otras soluciones, las respuestas suelen ser bastante rápidas. La documentación es suficiente, con bastantes manuales, una wiki, y documentos técnicos. Sin embargo, en relación con el mantenimiento del software, existen numerosos parches para arreglar pequeños fallos elaborados por particulares.

Aunque Zarafa no dispone de una completa herramienta de sincronización con otros dispositivos, existe la posibilidad de la instalación de un servidor de sincronización Z-Push, basado en ActiveSync.

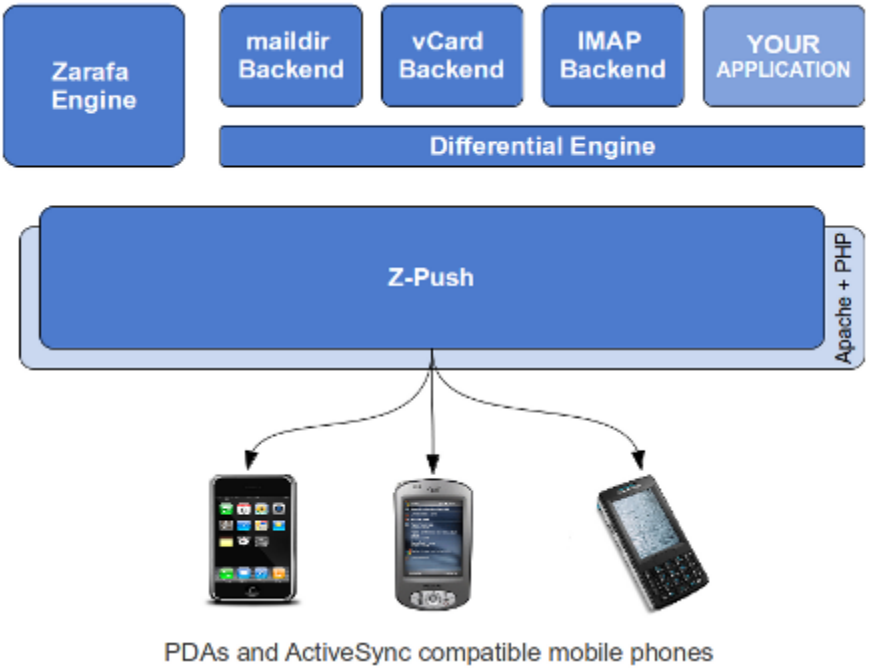

Figura 18 - Zarafa y Z-Push

2.3.4.2 Horde

Figura 19 - Logo Horde

[48] Solución de correo totalmente comunitaria (no tiene versión de pago), por lo que es muy activo. Las aplicaciones y módulos de Horde se desarrollan por toda la comunidad así como los desarrolladores. Los principios de Horde son crear aplicaciones sólidas y basadas en estándares empleando una programación orientada a objetos inteligente que permitirá ejecutar dichos módulos desde una gran variedad de plataformas y backends.

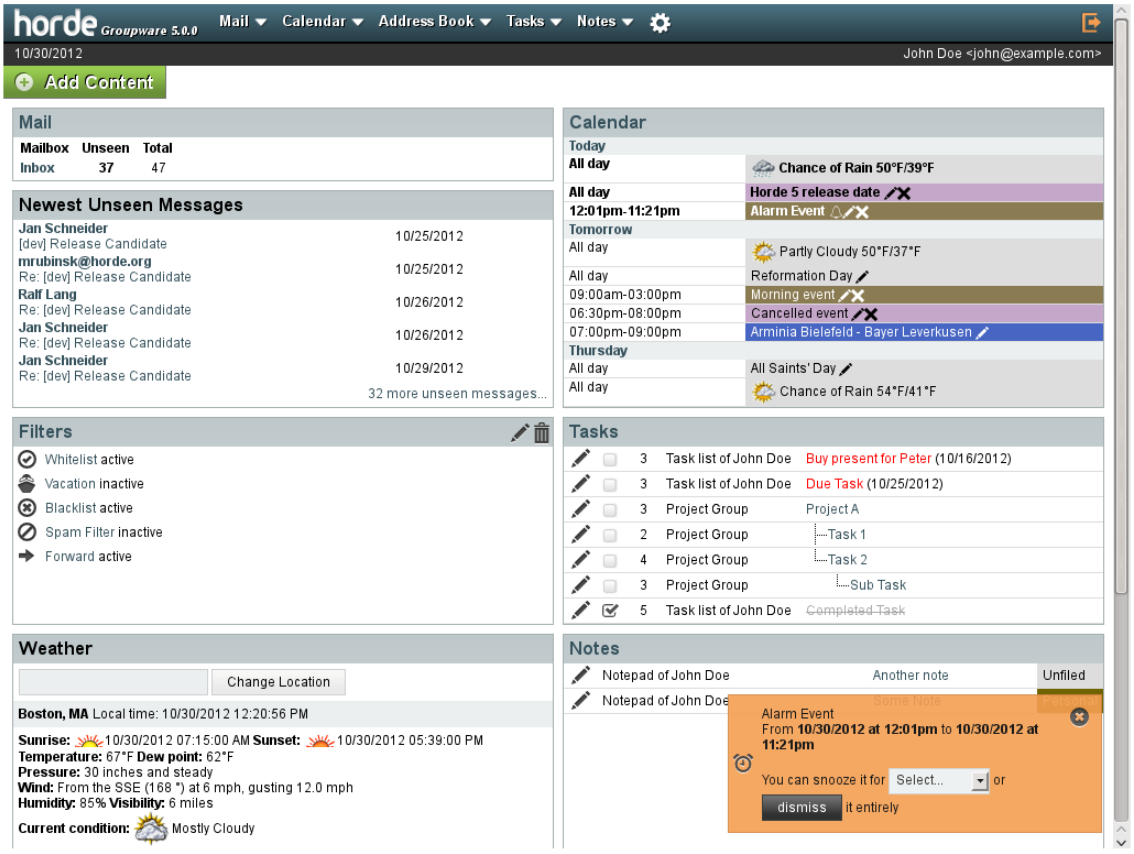

Figura 20 - Horde: Portal

Está escrito en PHP, lenguaje diseñado específicamente para páginas web. Disponible para Apache, IIS, Sun Web Server, Lighttpd, etc.

Horde GroupWare Webmail Edition es una solución gratuita, para empresas y basada en web. Los usuarios pueden leer, mandar y organizar su correo y administrar y compartir los calendarios, contactos, tareas, notas, archivos y marcadores. Tiene la una modularidad bastante variada y completa: IMP (Internet Messaging Program, permite el acceso a cuentas IMAP y POP3), Ingo (administrador de reglas de filtrado de correos electrónicos), Kronolith (aplicación de calendario), Turba (aplicación de administración de contactos y libretas de direcciones), Nag (aplicación de tareas), Mnemo(módulo de notas y memos), Golem (administrador de ficheros basado en web), Trean (administrador de marcadores), así como otros que se encuentran en desarrollo pero con versión beta (Wicked – wiki –, Ansel – administrador de fotos – …).

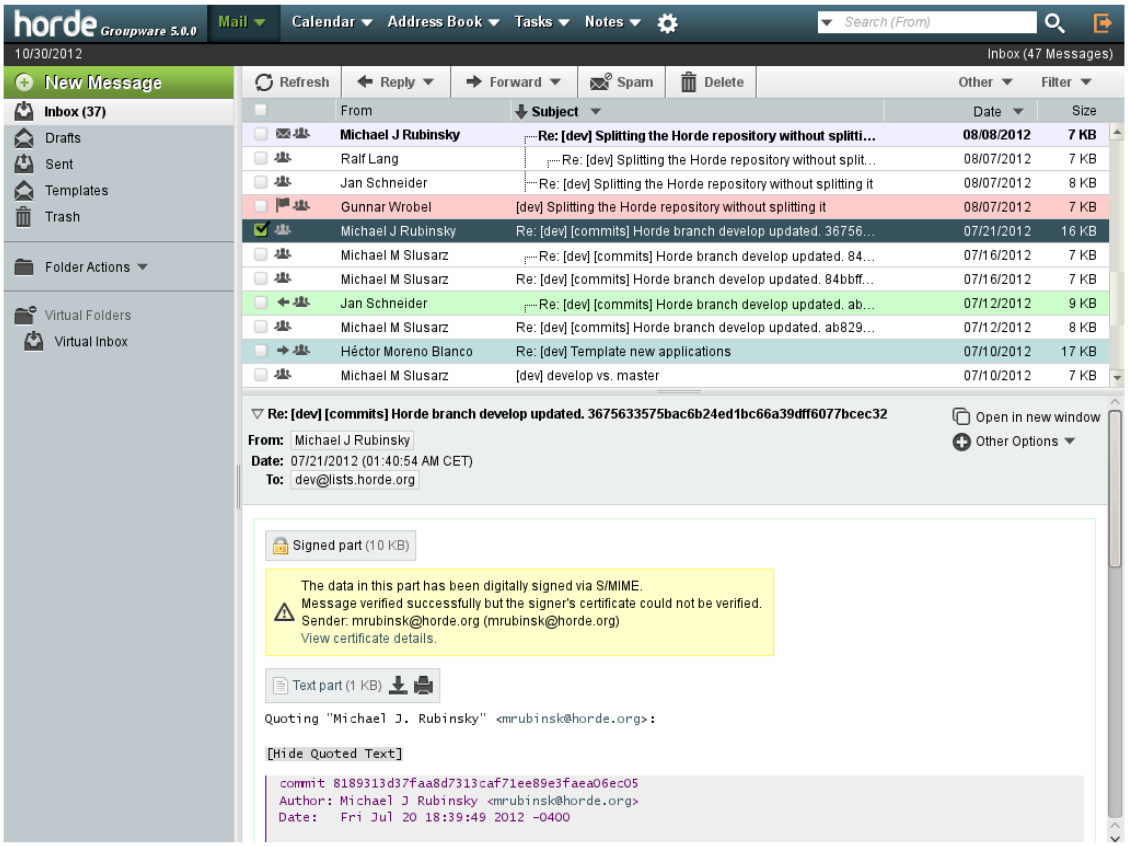

Figura 21 - Horde: Bandeja Entrada

Con las últimas versiones de los módulos, se han añadido capacidades de CalDAV, CardDAV, WebDAV, diferentes soportes con tipos de filtros de correo, firmas HTML, integración con AJAX para modo dinámico en todos los módulos (siempre y cuando el navegador lo permita), sistema de ticketing, gestor de recursos…

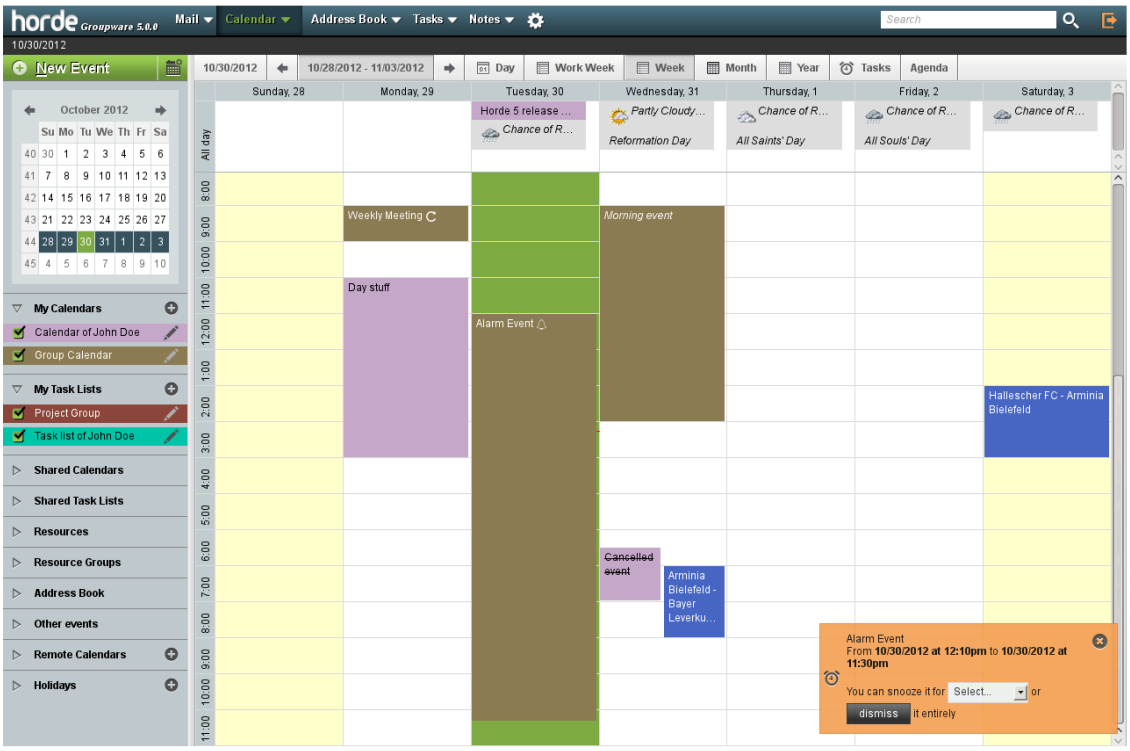

Figura 22 - Horde: Calendario

Dispone de una vista dinámica del correo (AJAX), otra vista básica para navegadores antiguos y una vista para interfaces móviles (tanto smartphones como normales).

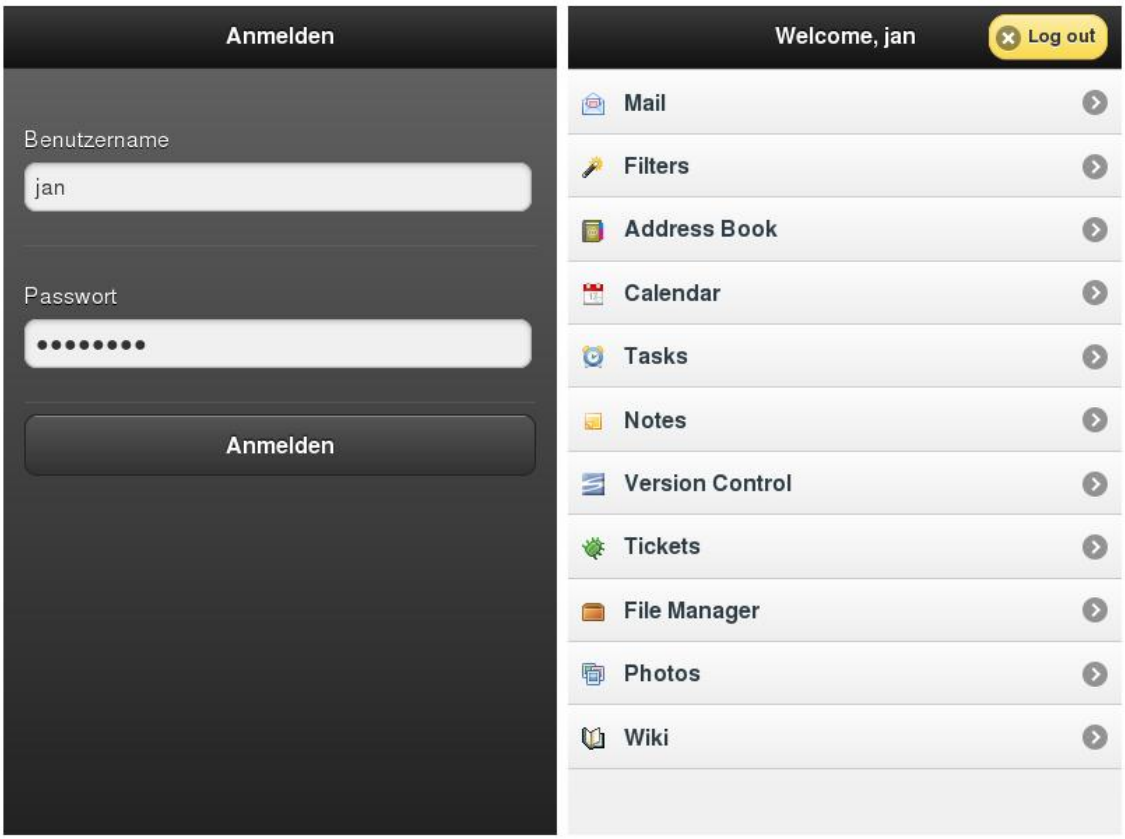

Figura 23 - Horde: Móvil

Funciona con toda plataforma que disponga de las librerías PHP.

2.3.4.3 Roundcube

Figura 24 - Logo Roundcube

[49] Este proyecto es una solución de webmail gratuito y de código abierto con una interfaz de usuario con apariencia de cliente pesado fácil de instalar/configurar y que se ejecuta en un servidor LAMPP estándar (Servidor LAMPP o XAMPP para Linux: Cross-platform, Apache, MySQL, PHP y Perl). Los temas de apariencia utilizan los últimos estándares web como XHTML y CSS 2. Roundcube incluye otras sofisticadas bibliotecas de código abierto como PEAR, una biblioteca IMAP derivado de IlohaMail del TinyMCE texto enriquecido, Googiespell biblioteca para la corrección ortográfica o WasHTML.

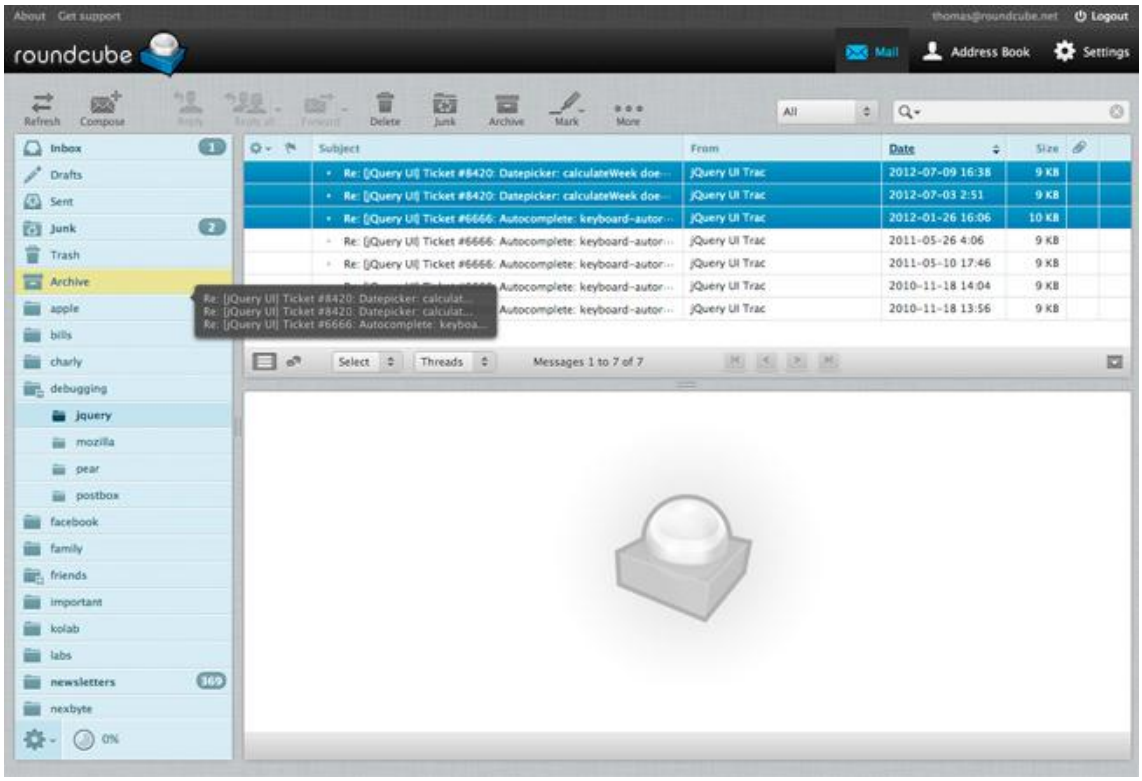

Figura 25 - Roundcube: Bandeja Entrada

Tiene la opción de arrastrar y soltar, con soporte para MIME y mensajes HTML, además de la composición de mensajes con lenguaje enriquecido (HTML). La gestión de carpetas IMAP es sencilla y permite la compartición de carpetas, así como carpetas globales.

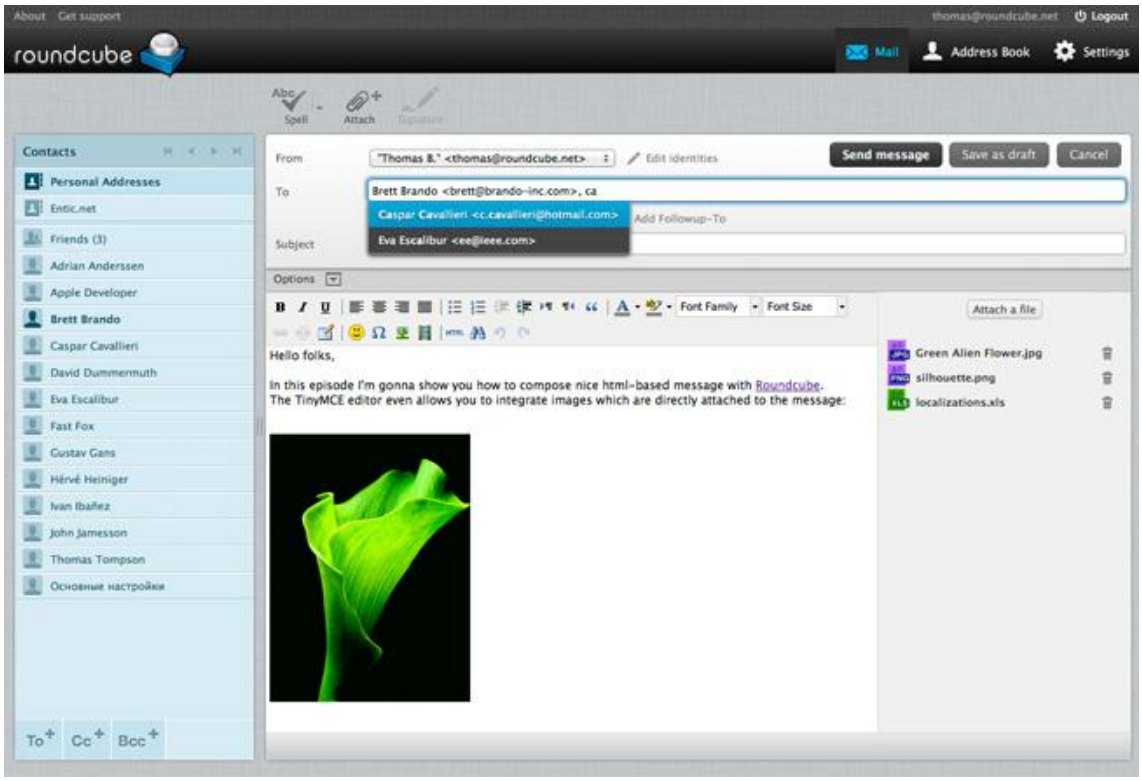

Figura 26 - Roundcube: Directorio

En cuanto a la privacidad y protección, tiene mecanismos sofisticados. Soporta ACL.

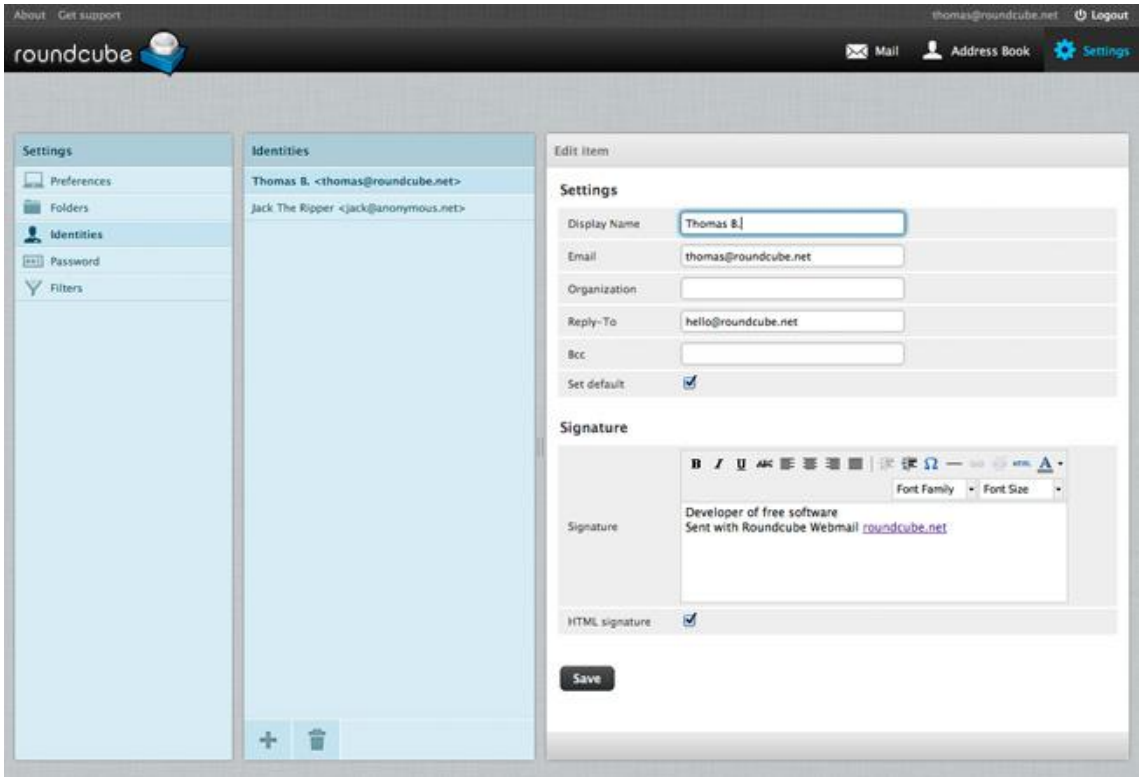

Figura 27 - Roundcube: Opciones

Permite también la integración con LDAP para las libretas de direcciones.

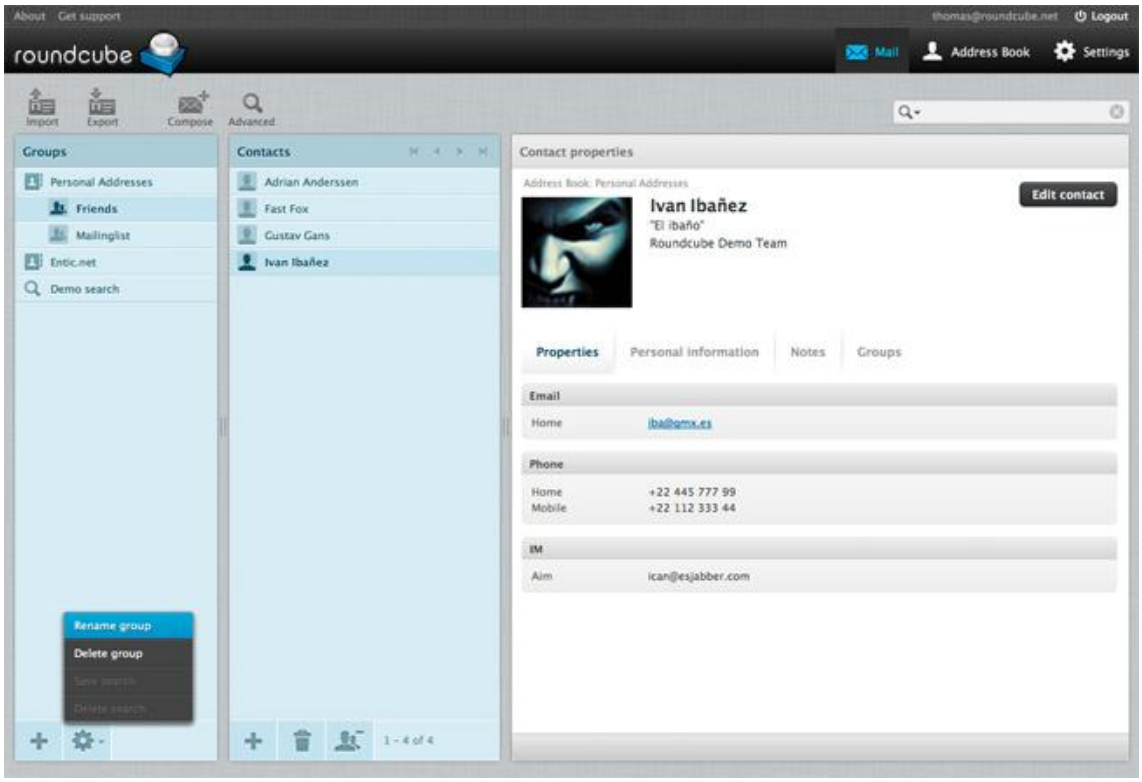

Figura 28 - Roundcube: Libretas y LDAP

En las últimas versiones han añadido características nuevas como el corrector ortográfico, importación/exportación de la libreta de direcciones, autoguardado en borradores cuando se está redactando un mensaje…

Además, Roundcube tiene la posibilidad de aumentar sus funcionalidades debido a la variedad de plug-in disponibles en un repositorio. [50]

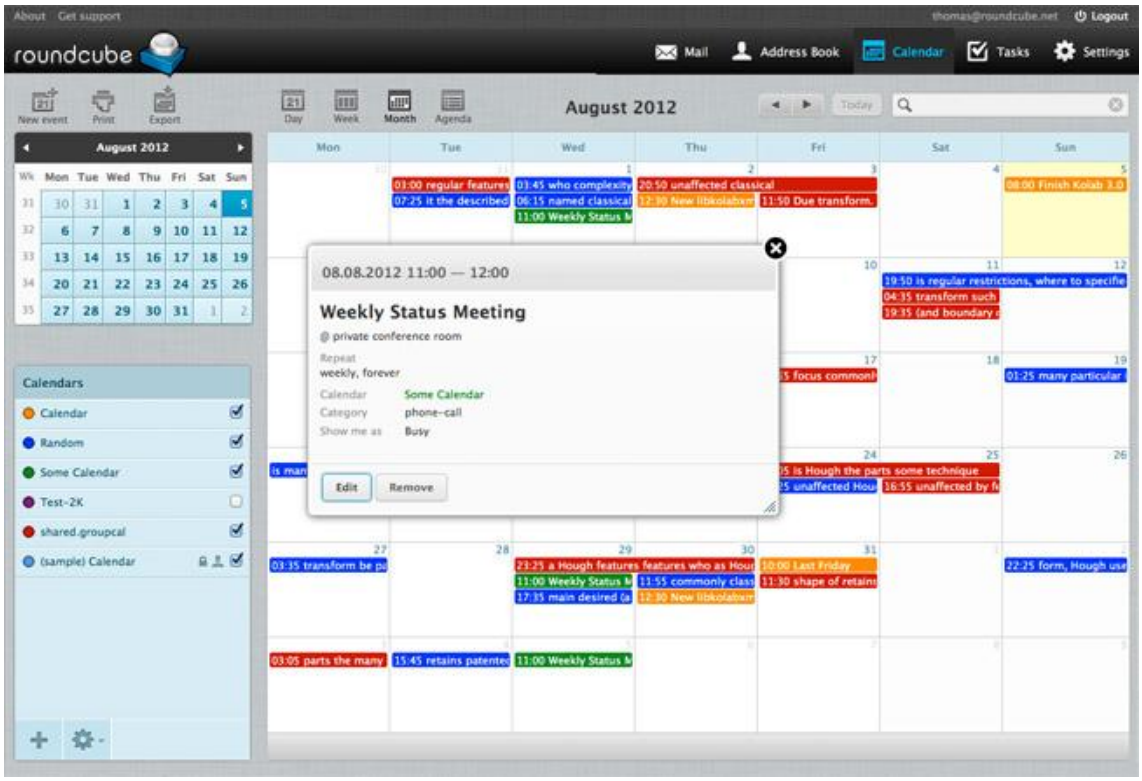

Figura 29 - Roundcube: Calendario

Esta solución es relativamente nueva, ya que la primera versión estable salió en 2008.

2.3.4.4 Open Xchange

Figura 30 - Logo Open-Xchange

[51] Open-Xchange es una aplicación de correo electrónico web y la solución de groupware dirigido a pequeñas y medianas empresas.

Al igual que Zimbra, Open-Xchange tiene una interfaz limpia con características de la interfaz de usuario avanzado, tales como arrastrar y soltar (AJAX), vistas configurables, y la función de autocompletar. Las características colaborativas avanzadas permiten a los usuarios compartir, delegar, establecer prioridades y tareas, y medir el progreso. El "infostore" actúa como un repositorio de archivos para el intercambio de datos e información.

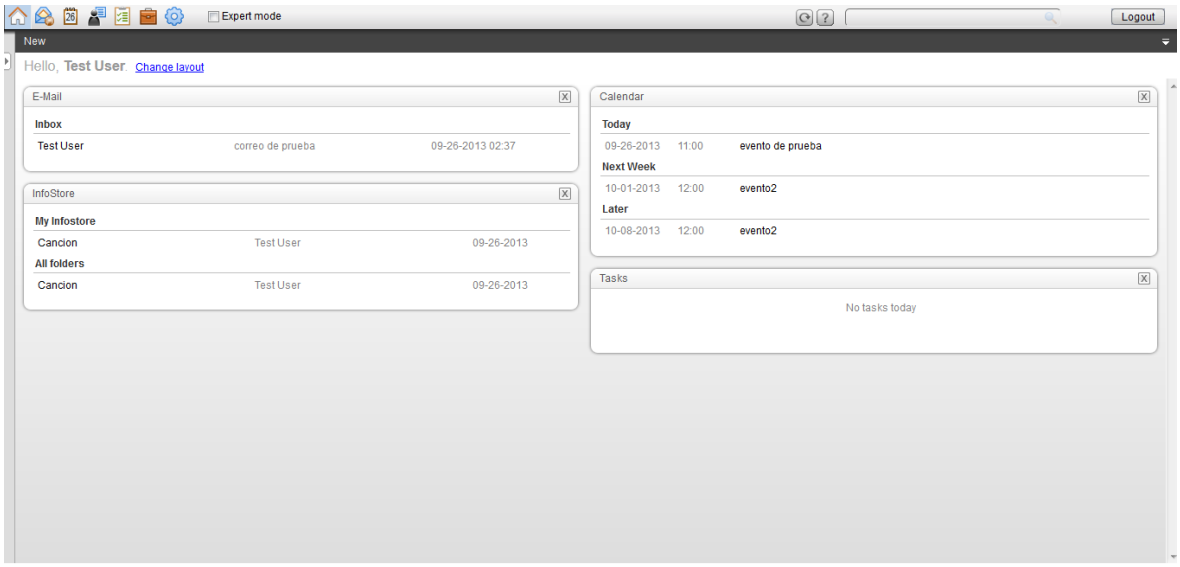

Figura 31 - Open-Xchange: Portal

Esta solución se completa con los módulos UWA, que son herramientas externas similares a los zimlets de Zimbra, pero más personalizables. Al estar escritos en Java, se pueden crear y personalizar.

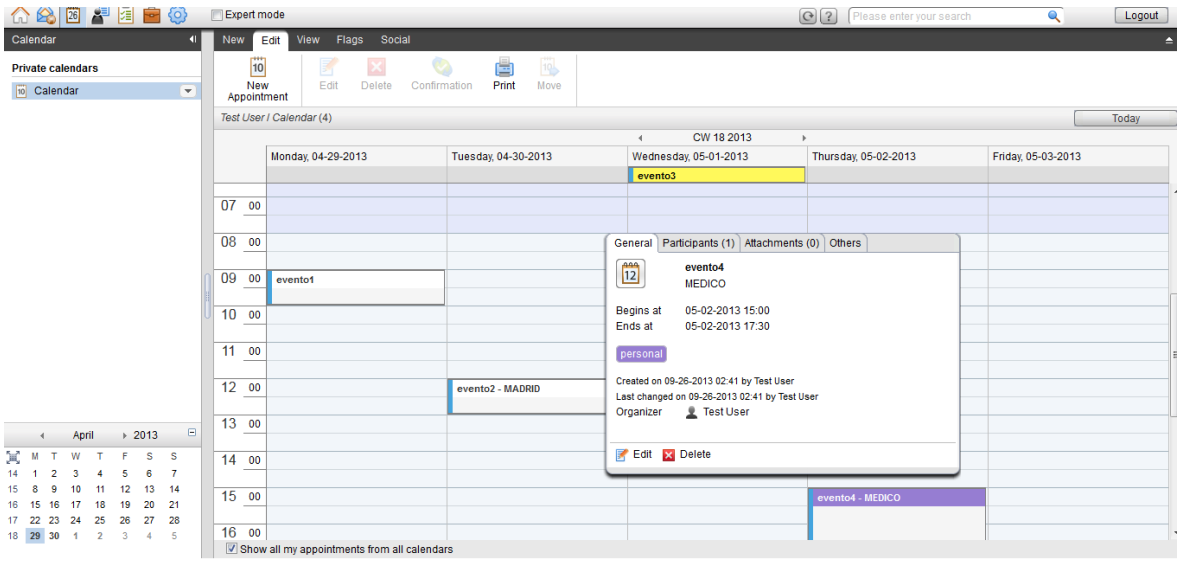

Figura 32 - Open-Xchange: Calendario

Existen conectores de Open Xchange para sincronizar con Outlook y Thunderbird, se denomina OXtender. Sin embargo, la versión para Outlook no está disponible en la versión comunitaria.

Dispone de bastante información, así como una Wiki [52] donde se encuentran diversas guías y documentos y FAQ. Los foros de la comunidad no son muy numerosos (comparado con Zimbra o eGroupWare), pero las respuestas son rápidas y diversas.

La versión de la comunidad (Open Source) no está protegida con antivirus o anti-SPAM, ni dispone de actualizaciones ni ningún tipo de soporte.

2.3.4.5 eGroupWare

Figura 33 - Logo Egroupware

[53] A pesar de que se trata de una solución basada en PHP perdiendo características visuales y funcionales propias de AJAX, ofrece una buena estructura colaborativa de Webmail.

Existe una Base de Conocimiento bastante amplia incluida en los repositorios con manuales, FAQ… Dispone de un potente calendario para la coordinación de grupos, recursos, contactos y noticias (para mantener a empleados informados). Además, eGroupWare es el único que posee un listado de proyectos y seguimientos para fortalecer la relación con el cliente y la administración del proyecto. Esto es una característica muy útil para cualquier compañía.

Figura 34 - Egroupware: Calendario

eGroupWare se puede sincronizar fácilmente mediante módulos con Outlook y smartphones mediante SyncML. Al igual que el resto de soluciones colaborativas Open Source no dispone por sí misma mecanismos de antivirus ni anti-SPAM.

La documentación es extensa, con manuales y Wiki con instalación y configuración detallada. El soporte está disponible a través de un amplio foro con miles de hilos. Sin embargo, y en comparación con otras soluciones, las respuestas suelen ser más lentas.

Algunas características interesantes son: ACL, WebDAV/CalDAV/CardDAV, calendarios y libretas de direcciones muy completos y con muchas funcionalidades, múltiples cuentas IMAP, chat, Wiki, Administrador de archivos (File Manager)…

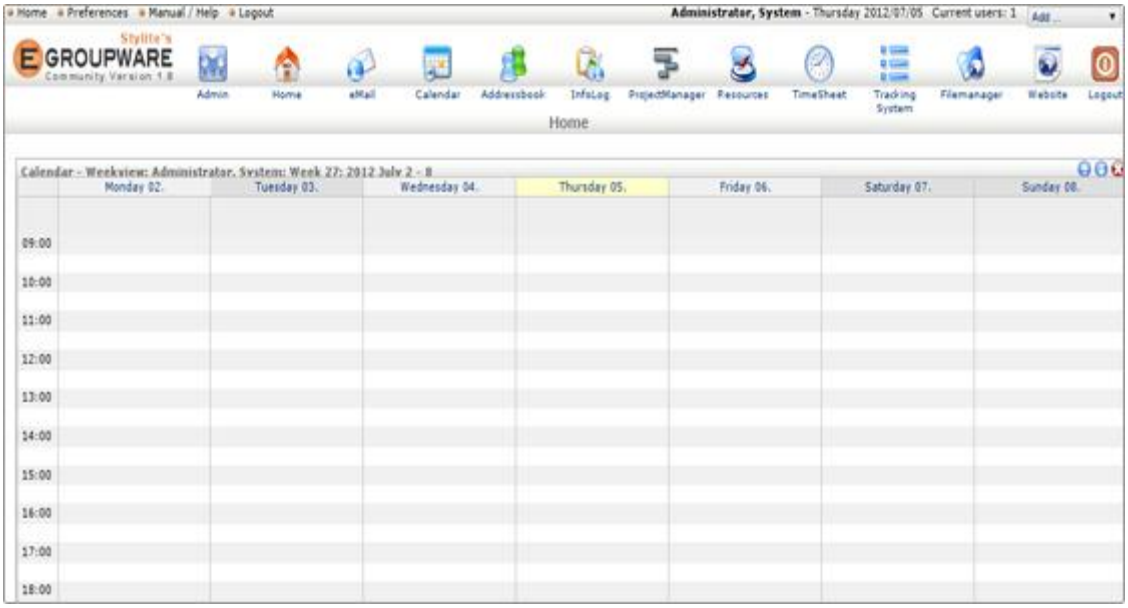

Figura 35 - Egroupware: Calendario 2

2.3.4.6 Zimbra

Figura 36 - Logo Zimbra

[54] Esta herramienta colaborativa ofrece al usuario una interfaz amigable, con muchas mejoras de rendimiento, como AJAX, arrastrar y soltar, un potente mecanismo de búsqueda, formato HTML para archivos Word o PDF. Dispone de zimlets, que son plug-in que permiten una personalización modular y fácilmente administrada para el usuario. Además, los usuarios pueden modificar zimlets ya creados para ajustarlos a sus necesidades (*mashups*).

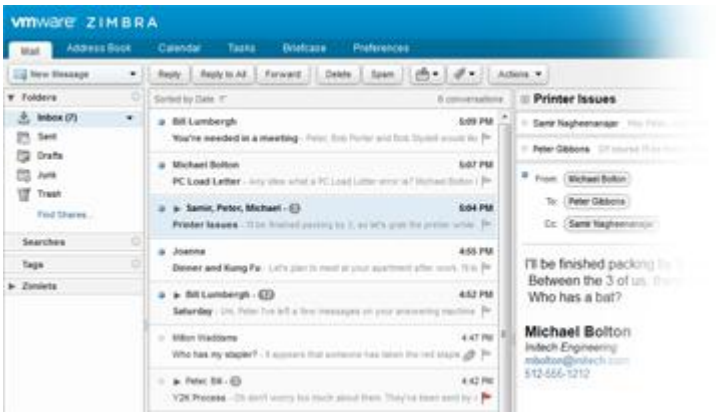

Figura 37 - Zimbra: Bandeja Entrada

Los usuarios pueden crear y compartir documentos web. Éstos se guardan en libretas personales que actúan como repositorios de documentos que se pueden compartir dentro del dominio. La aplicación de Maletín permite a los usuarios almacenar gran cantidad de documentos de diferentes formatos en distintas carpetas, que se pueden acceder remotamente y compartir con otros usuarios, cuyos permisos se editarán en la interfaz.

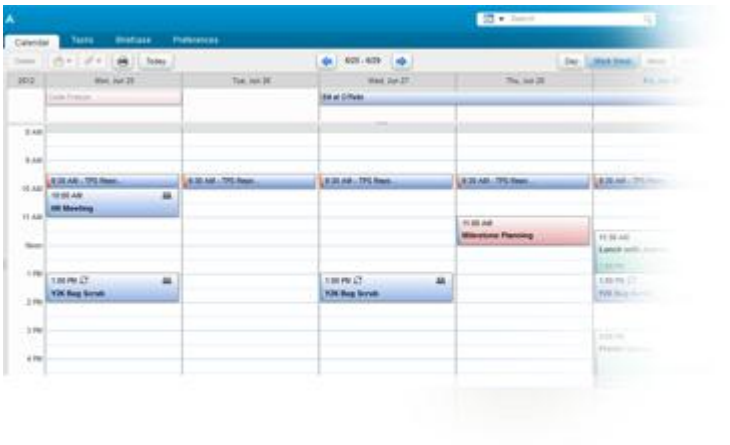

Figura 38 - Zimbra: Calendario

La administración basada en roles de Zimbra permite al administrador delegar derechos y tareas, así como buscar a través de buzones, determinar cuotas a usuarios y buzones, personalizar la interfaz, etc.

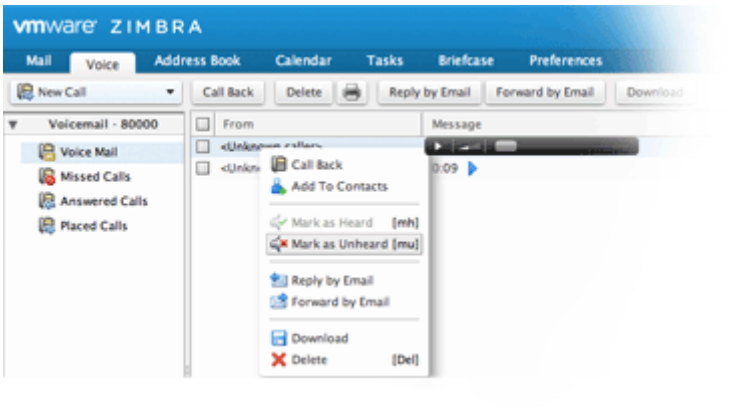

Figura 39 - Zimbra: Llamadas

Zimbra posee algunas características de seguridad, como filtrado de mensajes, marcas (flags), anti-SPAM y antivirus configurable, interfaz de sistema, y posibilidad de forzar la autenticación SMTP en el envío de correo.

El soporte de Zimbra es bastante bueno, con gran número de hilos y publicaciones en los foros y una alta velocidad de respuesta en los mismos. La documentación que se ofrece también es extensa, con varios manuales (administración, de usuario, how-to's…).

Aunque Zimbra no dispone de una completa herramienta de sincronización con otros dispositivos/aplicaciones, existe la posibilidad de la instalación de un servidor de sincronización Z-Push, basado en ActiveSync.

Figura 40 - Zimbra: Móvil

2.3.4.7 Comparativa Webmail

Zarafa es una buena solución de Open Source, complamente gratuita y fácil de usar para los usuarios finales, debido a su parecido con Outlook. Es útil para empresas por el fácil manejo de grupos y compartición de calendarios, correos y contactos. Sin embargo, no ofrece la posibilidad de compartición de documentos/archivos. Además, no tiene plug-in o conectores que mejoren las funcionalidades de la solución.

Horde ofrece múltiples funcionalidades altamente configurables. Ése es su punto fuerte, que al ser completamente abierto y bastante activo, se puede personalizar tanto cualquier característica de interfaz como de acciones. Además de ser el punto fuerte, es también su

desventaja, está siempre con bugs o fallos del sistema o características que no llegan a funcionar del todo, aunque la comunidad de Horde es muy activa en este sentido y se suelen solucionar rápidamente. Por otra parte, si se personaliza demasiado esta solución puede ser un problema a la hora de actualizar, ya que se perderán muchas de las configuraciones/personalizaciones.

eGroupWare tiene tanto solución comunitaria como Enterprise. Esto quiere decir que en la versión libre no se dispone de todas las funcionalidades, aunque sí la gran mayoría [55]. Su gran variedad de características la hacen muy ventajosa frente a otras soluciones.

Zimbra no tiene simplemente Webmail, si no que se instala la herramienta con todos los módulos de backend incluidos (MTA, MDA, base de datos…), esto hace que no sea del todo modulable, aunque sí se puede personalizar bastante. Para aquellos administradores que quieran una instalación *standalone* es una buena solución. Sin embargo, y al igual que otras soluciones, dispone de una versión comunitaria y otra appliance (de pago).

Con Open Xchange ocurre lo mismo, existe una versión comunitaria y otra appliance. Sin embargo, la versión comunitaria es muy completa, si bien hay detalles que no contempla, como alto número de licencias, soporte de alto nivel, etc. Por otra parte, al disponer de características avanzadas (compartición de archivos, contactos, correos…), la interfaz sencilla a la vez que completa y posibilidad de implantar conectores, la convierten en la opción más deseable para el entorno de este PFC. Su gran desventaja sería la sincronización de elementos PIM (Personal Information Manager), pero gracias a un servidor de sincronización Funambol, esto será posible.

2.4 Servidor de Sincronización

Para la sincronización de calendarios, tareas y contactos se ha escogido Funambol, al ser la única solución posible a la integración mediante software libre con Open-Xchange y una gran cantidad de dispositivos y sistemas operativos.

El único inconveniente de Funambol, es que desde los clientes sólo se puede configurar una cuenta. Es decir, si un usuario quiere sincronizar 2 cuentas en su dispositivo no podrá realizarlo mediante estos plugins.

2.5 Listas de distribución

Una lista de distribución es una agrupación de usuarios de correo electrónico que basa su trabajo en un software de envío simultáneo de mensajes, de modo que todos los suscriptores de un grupo reciben cada mensaje remitido por cualquiera de los participantes al servidor en el que se encuentra instalado este programa de difusión masiva de correos electrónicos. Como se deduce de estas líneas, en las listas de distribución intervienen cuatro agentes: los suscriptores, la tecnología del correo electrónico, el programa de distribución de mensajes y el servidor al que llegan y del que salen los mensajes enviados por los miembros de una lista. Por lo general, los suscriptores suelen ser miembros de una misma comunidad científica o profesional, quienes se unen a estas listas para compartir informaciones con los miembros de estos grupos; para ellos el uso del correo electrónico es cotidiano y emplean las listas como una fuente más de información. [56]

Las listas de distribución pueden ser configuradas conforme a unos parámetros establecidos por el administrador de la lista en función del programa empleado y de la política de la lista. El administrador o persona encargada del mantenimiento de la lista y de su buena marcha puede optar por una lista abierta, en la que se suscriba quien lo desee, o bien por una lista cerrada, es decir limitada a aquellas personas que cumplan una serie de requisitos: pertenencia a grupo profesional, interés demostrado por la temática de la lista, etc. Las listas cerradas suelen partir de un formulario en el que se pregunta a los interesados por cuestiones laborales. Muchas de las listas requieren una renovación anual, cuya misión es dar de baja a aquellos suscriptores que no están interesados en pertenecer a la lista, pero que se mantienen en la misma. Los programa de distribución permiten otra serie de opciones, como descargar directamente documentos depositados en el servidor, así como la consulta a los archivos retrospectivos de los mensajes que se han ido enviado en el transcurso de la lista de distribución. [57]

Muchas listas requieren una moderación para orientar mejor su funcionamiento y hacer cumplir correctamente los objetivos para los que se creó. En estos casos el administrador amplía sus funciones, ya que del mero mantenimiento y supervisión del funcionamiento del grupo, pasa a ser filtro, ya que los mensajes llegarán primero a su buzón y será él quien los reenvíe a la lista o simplemente acepte la distribución de los mismos. Se trata de establecer mecanismos de control para no difundir mensajes inadecuados. [58]

Los software de distribución de listas son variados, sin embargo, los más empleados son Majordomo, Listserv y, últimamente, Sympa. El primero, al ser más arcaico y menos intuitivo para los usuarios, se está dejando de usar en detrimento de los otros dos. A continuación se detallarán a grandes rasgos cada uno de ellos y el que se seleccionará en el presente PFC.

2.5.1.1 Majordomo:

[59] [60] [61] Majordomo es una aplicación de software libre (no por completo) de listas de distribución escrita en Perl y trabaja en conjunto con Sendmail. Al estar escrita en Perl, es muy configurable y personalizable. Además de que su diseño modular permite hacer uso sólo de las características que se necesiten.

Tiene un sistema de subscripción un poco arcaico sin interfaz web y mediante correo electrónico, así como los comandos. Una vez que una lista es creada y levantada, se pueden realizar todos los comandos remotamente, sin la intervención del postmaster del servidor de la lista.

Soporta varios tipos de listas, incluidas las moderadas. También confirmación de subscripciones, para proteger frente a las falsas.

Es una aplicación bastante antigua y sin continuidad ni soporte prácticamente desde el año 2000.

2.5.1.2 Sympa

Figura 41 - Logo Sympa

[62] Sympa es un software de libre distribución que permite la gestión de listas de correo y una muy flexible adaptación a las necesidades de la organización.

Sympa está respaldado por un equipo de la red académica francesa llamado CRU y es usado por una gran cantidad de universidades, centros de investigación, etc.

Sympa 6.1.17 es la última versión de este gestor de listas.

Para más información, se pueden consultar las características de este software [63].

Con Sympa es posible a la creación de subdominios para la creación de distintos grupos. Existiendo la posibilidad de que dos listas se llamen igual pero con distinto subdominio. Por ejemplo, el dominio pruebas.com podría contener listas con subdominio sub.pruebas.com.

Figura 42 - Sympa: Portada

Tiene la opción de incorporar subscriptores a las listas de distribución de manera dinámica a partir de información contenida tanto en LDAP como en una base de datos Oracle.

Tiene una gestión de envío y recepción de listas bastante amplia, en la que desde la interfaz web, el propietario de la lista puede definir cualquier política que quiera. Además, se pueden definir listas con unas características especiales: los subscriptores de una lista pueden enviar a otra lista, siendo ésta cerrada y sólo accesible para los primeros. Por ejemplo, se tendría una lista (lista) a la que pueden enviar sus subscriptores (sA) y los subscriptores (sB) de otra lista (listaB), los sB no podrían mandar a listaB (cerrada). La creación de estas listas se puede simplificar mediante plantillas.

Figura 43 - Sympa: Configuración lista

Se puede configurar la autenticación contra LDAP con cualquiera de los alias de los usuarios. De este modo, los usuarios podrían ver las listas a las que está suscrito con cualquiera de sus alias mediante una pequeña adaptación del código.

La licencia es GPL, facilitando así la instalación y actualización de la plataforma. Por tanto, el soporte es bastante amplio con una gran comunidad de usuarios desarrollando parches y solucionando fallos (bugs).

2.5.1.3 LISTSERV:

Figura 44 - Logo LISTSERV

[64] LISTSERV es también un software de gestión de listas de correo, pero propietario.

La primera versión surgió en 1986 en BITNET y fue el primer programa encargado de automatizar las tareas de gestión de listas de correo.

LISTSERV 16 es la última versión.

Con Listserv es posible la creación de subdominios. Sin embargo, dos listas de diferentes subdominios no pueden llamarse igual.

Al igual que Sympa, permite la adición de subscriptores a partir de la información contenida en una base de datos Oracle.

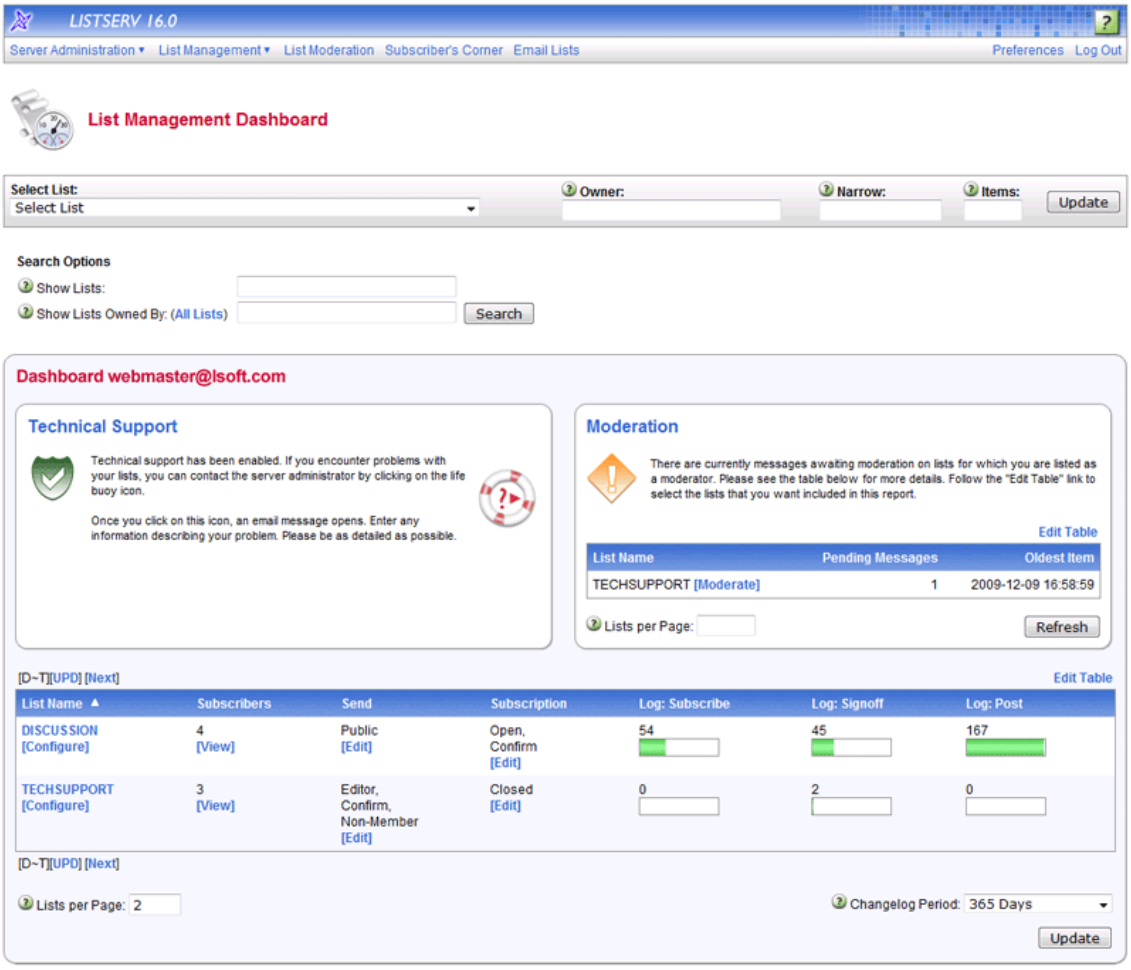

Figura 45 - LISTSERV: Administración

Los usuarios que no sean subscriptores podrían mandar correo a otra lista, aunque según RedIRIS se debería poder realizar mediante algún desarrollo y no se ha llegado a probar.

Este software tiene una versión libre pero con limitaciones importantes: un total de 10 listas de distribución y hasta 500 subscriptores. A partir de ahí, son versiones de pago con licencia propietaria.

Permite también la autenticación por LDAP, pero a diferencia de Sympa, un usuario no podría ver a priori todas las listas a las que está suscrito con todos sus alias. Según RedIRIS se requiere algún tipo de desarrollo.

2.5.1.4 Comparativa listas de distribución

La interfaz gráfica de Listserv es muy sencilla, y el panel de control del estado del servidor es muy completo. Por otra parte, requiere más desarrollo para personalizarlo más para los clientes. Por ejemplo, sólo está en inglés y requeriría traducciones dependiendo de las necesidades.

Almacena menos información en la base de datos, con lo que es más complejo buscar dichos datos en caso de que sea necesario por alguna cuestión de depuración. Además de tener más dificultades durante la instalación.

No permite integración con sistema de SSO ni una completa definición de subdominios para las listas.

Su integración con otros módulos/aplicativos de la plataforma es peor, con LDAP, EXIM… Además de poseer una migración más compleja.

Por otra parte, Sympa no tiene necesario el desarrollo de scripts y es de software libre completamente gratis.

Se integra perfectamente con otros módulos de la plataforma, LDAP, EXIM… Y tiene una migración mucho más sencilla.

Permite una integración son SSO y la creación completa e independiente de subdominios.

La única desventaja importante frente a Listserv es que la interfaz es menos lograda.

Debido a las grandes y numerosas ventajas de Sympa, y, sobre todo, porque es licencia GPL completamente gratuita, se seleccionará Sympa para los servidores de listas de distribución.

3 Diseño

3.1 Hardware

El hardware de la plataforma se encuentra en un BladeCenter de IBM (Blade II), con hojas (blades) HS20 y HS21. Asimismo, se dispone de cabinas de discos administradas por dos controladoras NetApp.

La administración del BladeCenter se realiza tanto desde el propio CPD conectando directamente, o mediante telnet.

La administración de las cabinas de discos se hace por línea de comandos, conectando a la red privada a la que pertenecen, o mediante interfaz web denominada FilerViewer.

La entrada/salida de correo electrónico se realizará a través de los Ironport, donde se encuentran definidos los diferentes registros de correo MX. A pesar de tratarse de una plataforma de software libre, estos elementos serán muy importantes a la hora tratar todo el flujo de correo entrante/saliente de toda la arquitectura. A pesar que se supondrán ya instalados previamente, se tendrán en cuenta durante el diseño del presente PFC.

El acceso a la plataforma (tras los cortafuegos) se realiza a través de unos switches balanceadores Nortel. A los cuales se accede para su administración mediante telnet a través de una red privada.

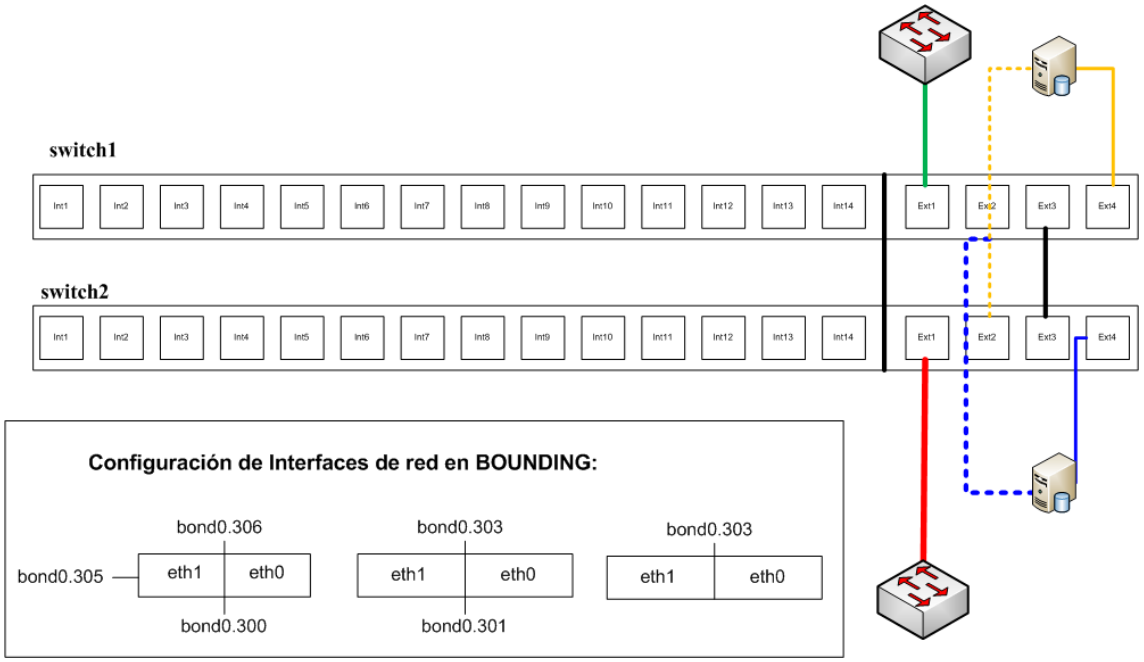

Figura 46 - Arquitectura física

3.2 Software

Como característica común a todas las máquinas, están basadas en Linux en la distribución Scientific Linux 5.x, la cual ha sido instalada y configurada personal y manualmente por

los administradores para garantizar un funcionamiento específico de las herramientas y aplicaciones de la plataforma.

De este modo, también se lleva a cabo la administración, monitorización y configuración de los sistemas desde nivel de sistema operativo hasta usuario final.

Además, todos los servidores tienen sus logs en el syslog, de manera que cuando se vaya a llevar a cabo la centralización de los log en un servidor, sea más sencillo esta migración.

Para un completo funcionamiento de la plataforma, se pueden realizar numerosos scripts (Shell Script) para llevar a cabo diferentes tareas: rotado de logs, chequeos de monitorización, módulos de backup…

3.1 Plataforma de correo

Para facilitar la comprensión de la arquitectura, se procederá a detallarlo en sentido externo a interno.

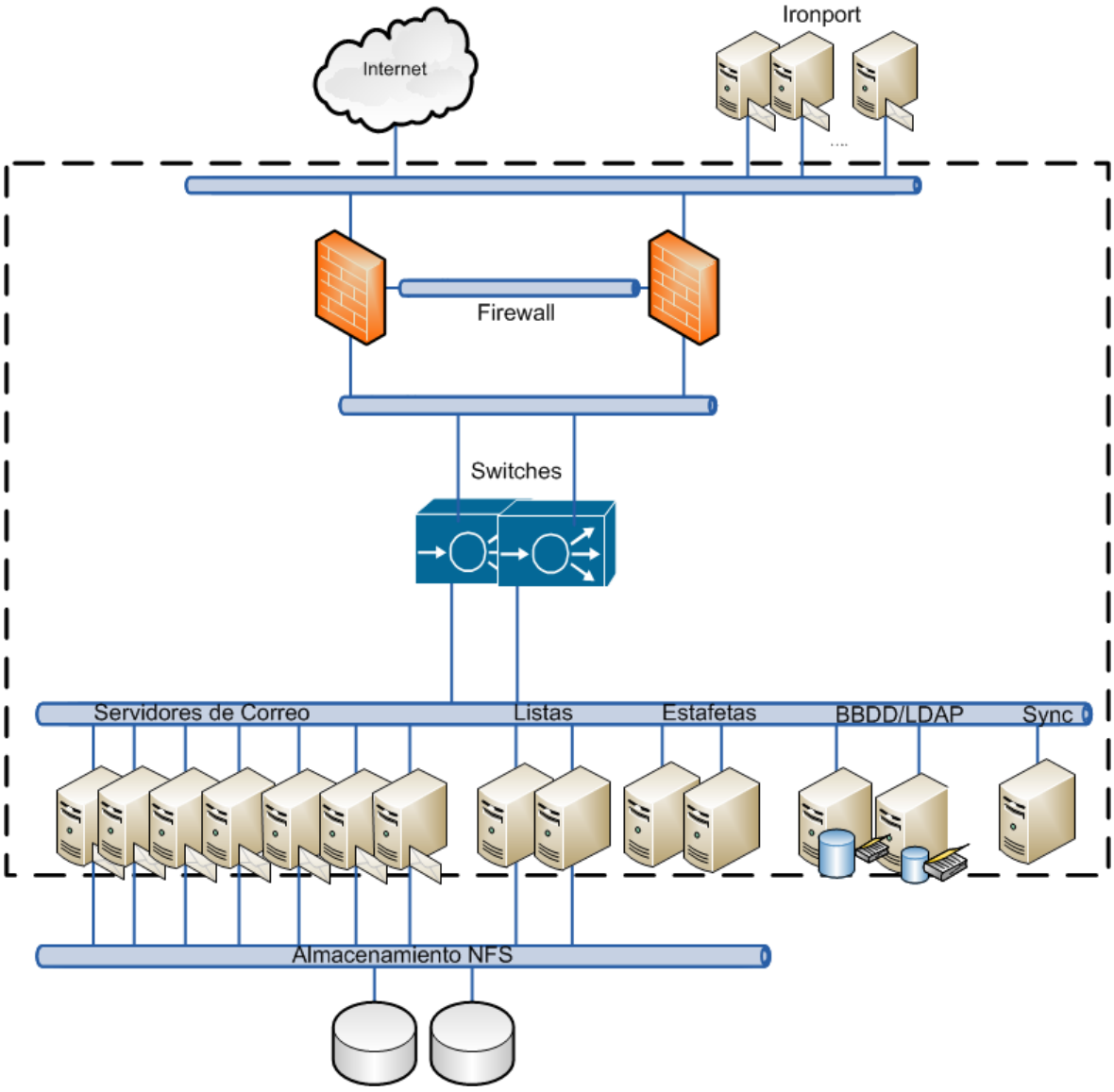

Figura 47 - Arquitectura lógica

3.1.1 Ironport

Los Ironport (Cisco) son dispositivos de alto rendimiento diseñados para las necesidades de infraestructuras de correos en redes con gran cantidad de tráfico. Éstos son capaces de analizar miles de correos en poco tiempo para ver si contienen virus, SPAM, cumplen ciertas políticas…

Estas máquinas son muy potentes y tienen una gran cantidad de posibilidades de configuración. Pueden actuar como Anti-virus, Anti-SPAM, cuarentena para correos, monitorización de correo entrante/saliente, control de acceso a remitentes, puerta de acceso virtual…

Todo el correo de la plataforma, tanto externo como interno, pasa a través de los Ironport para que puedan ser analizados y monitorizados, de manera que la seguridad e integridad de la plataforma no se vea comprometida.

Para la gestión de los Ironport se dispone de una interfaz gráfica muy completa, en la que se pueden administrar todas las características antes mencionadas.

3.1.2 Firewall

El acceso a la plataforma de correo pasa primeramente por un filtro en los cortafuegos. Las políticas de estos cortafuegos están basadas en IPTables, pero para una mejor administración de las mismas, se encuentra instalada una herramienta denominada FW Builder. Con esta herramienta se pueden definir de manera muy intuitiva los grupos e IP que se quieran, así como las redirecciones internas (NAT) y las políticas de acceso/salida de la plataforma.

Además, esta herramienta permite una visualización muy rápida y sencilla de los logs, al loguear todas y cada una de las reglas existentes tal y como se especifique en dicha herramienta. De otra manera, habría que hacerlo manualmente en el fichero de configuración antes de cada regla añadiendo otra línea para indicar que se quiere loguear dicha acción.

Aquí se encuentran definidos todos los servicios que ofrece la plataforma de correo, con los puertos a los que hacen uso y las políticas de acceso a los mismos.

3.1.3 SWITCHES

Los switches, a los cuales se accede desde las máquinas anteriormente mencionadas (‘los cortafuegos), tratan todo el tráfico entrante y lo balancean a las máquinas según una política aleatoria (‘Round Robin’), en la que las máquinas con mayor procesador y memoria tienen más peso para abarcar más tráfico que las demás. Se trata de un balanceo hardware.

En estos switches Nortel se encuentran definidas las IP de los servicios virtuales de la plataforma. Dentro de estos servicios están definidas las diferentes máquinas, cada una con los puertos correspondientes a los que harán uso.

Los switches están interconectados entre sí (véase el esquema de hardware) en estado activo/pasivo, de manera que si el switch activo tiene algún problema o simplemente deja

de funcionar, los servicios balancearán al otro switch, haciendo que la indisponibilidad de la plataforma sea simplemente de segundos.

3.1.4 SERVIDORES DE CORREO

Los servidores de correo son los encargados de entregar el correo a los buzones, mandar el correo hacia fuera (hacia los Ironport) y del webmail.

3.1.4.1 Webmail

La aplicación de Webmail se denomina Open-Xchange. Este Groupware contiene los aplicativos esenciales para el correcto funcionamiento de un webmail. Consta de módulos de acceso a buzones y envío/recepción de correo, libretas de direcciones, agendas, tareas, filtros de correo, almacenamiento y compartición de archivos, cuentas de redes sociales (Facebook, Twitter, LinkedIN).

Open-Xchange es una aplicación basada en AJAX (JAVA). Para su personalización y configuración se requieren conocimientos de este lenguaje, ya que al ser software libre, es posible realizar todas las modificaciones que se deseen.

Es posible la adición de plugins UWA (Universal Widget API). Esto permite la creación y personalización de widgets que harán más único el Webmail de cada usuario, añadiendo partes meteorológicos, minijuegos, datos de bolsa…

El acceso al webmail se realiza mediante HTTP seguro, gracias a los certificados instalados en los servidores HTTP Apache instalados en estas máquinas. Estos certificados son creados dentro de la plataforma y firmados por RedIRIS.

3.1.4.2 Envío/recepción de correo

El envío y recepción de correo en los buzones los realiza la aplicación Exim. Se trata de un agente de transporte de correo (MTA), muy flexible a la hora de configurar el camino de los mensajes según su origen/destino. También puede hacer control de relays, usuarios y dominios virtuales. A su vez, es posible hacer control de SPAM y de virus desde este MTA, pero estos temas los tratarán los Ironport, para evitar que entren en la plataforma correos maliciosos. Este control de caminos posibles se realiza mediante las opciones de configuración del MTA denominadas routers y drivers.

El cometido de Exim es tomar el correo proveniente de las estafetas (exterior → Ironport → estafetas) y transportarlo a la aplicación encargada de guardarla en el buzón. Cuando el correo es saliente, pasa el correo directamente a los Ironport (sea local o no), para que aquí sea tratado de SPAM y virus, y sea enviado directamente hacia internet o hacia dentro de la plataforma si se trata de correo local.

3.1.4.3 Entrega/consulta de correo

Una vez que el correo ha llegado al MTA para ser entregado localmente en un buzón de un usuario, se transporta a la aplicación encargada de ello (MDA), Dovecot. Esta aplicación, además de entregar el correo en buzones y aplicar filtros sieve para clasificar correo entrante así como listas blancas y negras, también es la encargada de realizar la consulta del correo de usuario.

La consulta de correo puede ser llevada a cabo mediante los dos protocolos más importantes para ello: POP3 e IMAP. Desde webmail sólo se puede consultar el correo por

IMAP. Este protocolo (Internet Message Access Protocol) simplemente consulta el correo del servidor, sin eliminarlo del mismo moviéndolo a un cliente. De esta manera un usuario puede ver su correo desde cualquier parte del mundo.

El protocolo POP3 (Post-Office Protocol) funciona de manera distinta a IMAP. Con este protocolo, el usuario descarga del servidor los correos a un cliente que disponga la capacidad para ello (Outlook, Thunderbird…). De este modo, una vez descargados del servidor, sólo es posible acceder a esos correos desde el cliente que los tomó.

Desde los clientes de correo es posible configurar tanto IMAP como POP3.

Para la consulta de correo IMAP y POP3 seguro, se dota a la plataforma con certificados SSL para que la esta consulta se realice sin peligros (IMAPS y POP3S). Al igual que los certificados del servidor HTTP, son creados en la plataforma y firmados por RedIRIS.

3.1.4.4 Listas de distribución

Además de disponer de servicio de correo, también se provee de un servicio de listas de distribución. Este servicio se encuentra en alta disponibilidad activo/activo. La aplicación que se emplea para ello es Sympa.

Esta herramienta permite la creación, administración y un alto nivel de personalización de listas de distribución. Esta personalización consta de: creación de robots por dominio, configuración personalizada de las listas en lo que se refiere a suscriptores, envío/recepción, consulta, moderación, administración… de listas y la creación y uso de listas dinámicas.

3.1.5 Servidor de Sincronización

[66] Funambol es un servidor de aplicaciones móviles que proporciona sincronización de elementos PIM (Personal Information Management), como son los calendarios, las tareas, los contactos o las notas. Está basado en software libre, y consiste en un servidor de sincronización, clientes o programas para dispositivos móviles u ordenadores, y conectores que permitirán la interacción con otros sistemas. La versión comercial de Funambol además añade la sincronización de datos y multimedia.

Está soportado por una gran cantidad de dispositivos móviles y sistemas operativos. La sincronización se puede llevar a cabo en sentido servidor → cliente, viceversa o ambos.

El servidor de sincronización Funambol se integrará perfectamente con la plataforma, haciendo uso de los recursos, como las bases de datos MySQL *bbddX*. También podría emplear el LDAP, pero el aprovisionamiento de usuarios se hará según vayan sincronizando por primera vez en la plataforma.

La integración con Open-Xchange es sencilla, mediante simples conectores.

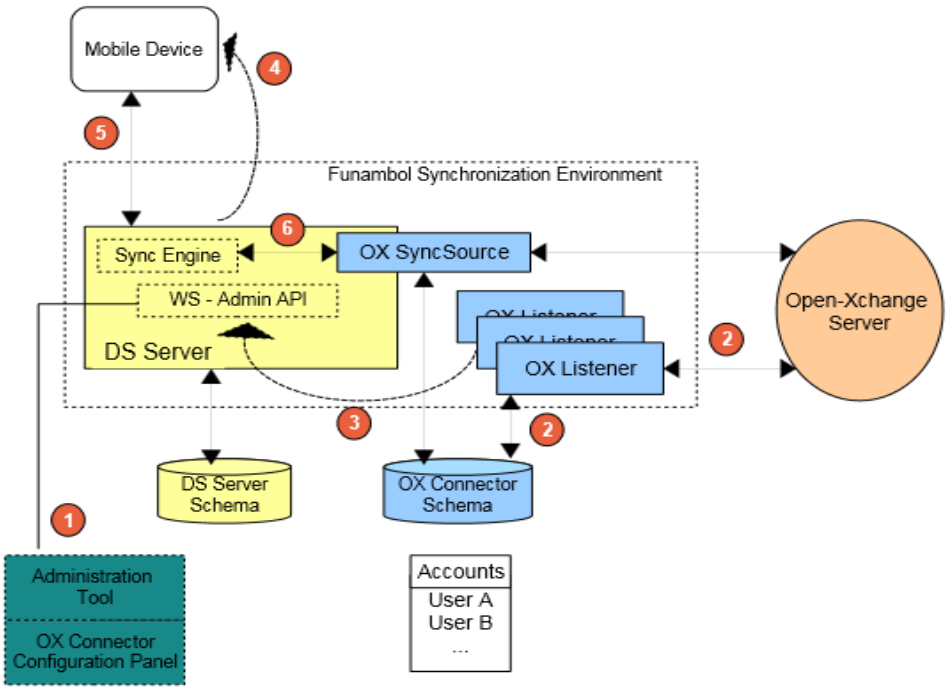

Figura 48 - Open-Xchange y Funambol

El servidor Funambol, cuando recibe las peticiones, conectará mediante el conector *ox-listener* a la información de Open-Xchange.

3.1.6 Almacenamiento

Todos los correos de todos los usuarios locales se encuentran almacenados en unas cabinas de discos, administradas por dos controladoras Netapp. Este almacenamiento sólo es accesible desde los servidores bien de correo y de listas. Desde estas controladoras se han creado diferentes volúmenes para los buzones, listas, configuraciones de aplicaciones y logs de la plataforma.

El acceso a estos volúmenes se realiza mediante el protocolo NFS (Network File System). Así, se exportan estos volúmenes desde las controladoras y se montan (incluidos en el fichero de configuración de sistema fstab) en las máquinas que hagan uso de este almacenamiento.

Estos volúmenes se han creado desde línea de comandos, con cierto tamaño snapshot, y se administran desde la interfaz web FilerViewer. El tamaño es dinámico, es decir, cuando se observa que cierto volumen está cerca de llenarse (sobrepasa el 85% su capacidad), se puede aumentar su tamaño sin tener que parar el servicio (se hace “en caliente”).

3.1.7 BBDD

Estos servidores contienen las bases de datos de las que hace uso la plataforma en MySQL. Tanto Open-Xchange Webmail como Sympa hacen uso de estas bases de datos, para el almacenamiento de preferencias, configuraciones, listas, información de módulos, etc.

Estos servidores se encuentran en activo/pasivo y maestro/maestro. Esto es así porque el acceso simultáneo de escritura a un campo de una base de datos podría corromper la

información. Además, la configuración maestro/maestro permita que cuando el servicio se balancee de un servidor a otro y luego vuelva no haya que hacer una actualización manual de la información del primero.

Para que las aplicaciones puedan acceder a las bases de datos, se tienen que dar los permisos de datos a las bases de datos correspondientes a cada servicio (‘grant’).

Por otra parte, como se ha comentado anteriormente, Sympa hace uso de listas dinámicas. Estas listas dinámicas toman sus datos de usuario de una base de datos Oracle, mediante sentencias SQL de Oracle. De este modo, los usuarios de estas listas se actualizarán automáticamente cada cierto tiempo, configurable desde la herramienta de listas de distribución. La gestión de esta Oracle no se tendrá en cuenta en el presente PFC.

3.1.7.1 LDAP

Los usuarios están almacenados en un LDAP maestro. Los servidores de Bases de Datos (*bbddX*) son réplicas de este LDAP. La consulta a éste se hace mediante la aplicación OpenLDAP. Para llevar a cabo esta réplica de datos entre el LDAP maestro y los esclavos, simplemente es añadir unos parámetros a la configuración de éstos, incluyendo los datos de conexión al LDAP maestro.

Todas las aplicaciones de la plataforma hacen uso del LDAP: Open-Xchange, Dovecot, Exim, Postfix, Sympa, Ironport.

3.1.8 Estafetas

Las estafetas de correo son las encargadas de redirigir todo el correo saliente, ya sea hacia el exterior o locales, pasando antes por los Ironport.

Este transporte del correo desde los servidores hacia los Ironport (o relays externos) se realiza mediante la aplicación Postfix (MTA: Mail Transfer Agent).

Postfix es un servidor de correo de software libre (al igual que el resto de aplicaciones de correo de la plataforma) para el enrutamiento y envío de correo, más rápido, fácil de administrar y segura. Para esta transferencia de correo se emplea el protocolo SMTP.

Al igual que ocurría con la aplicación Exim de los servidores de correo, el MTA (Postfix) de salida tiene una gran variedad de parámetros de configuración. Como la simple definición de hacia dónde mandar correos de ciertos dominios, qué conexiones/usuarios y cómo van a mandar/recibir el correo a través de la estafeta (restricciones de envío, de cliente, de ‘from’…), envío autenticado, comunicación TLS…

3.2 Diseño Lógico

En cuanto al diseño lógico, a continuación se presentan diagramas de los diferentes flujos de comunicación en la plataforma. Los switches no se representan en los siguientes diagramas debido a que se trata de un esquema lógico. Pero se situarían inmediatamente detrás de los cortafuegos.

Existen 3 tipos de flujos de información en la infraestructura de correo electrónico: HTTP, POP3/IMAP y SMTP.

3.2.1 HTTP

Las conexiones HTTP son las destinadas al tráfico de datos por internet. En el caso de esta plataforma de internet, serán las destinadas a el acceso a la aplicación de Webmail y a la interfaz web de listas de distribución.

Así pues, una conexión, ya sea interna de la plataforma o externa (fuera de la compañía, por ejemplo), conectará directamente a estos servicios. Primero pasará por el cortafuegos, donde se hará un *nateo* para traducir las direcciones públicas en privadas. Luego pasarán por los switches donde están definidos los servicios virtuales (en este caso, serán el de webmail y el de listas) que balancearán las conexiones tal y como se comentó anteriormente. Este balanceo se encarga de repartir las conexiones entre los servidores de webmail o listas, dependiendo de la petición HTTP.
4
Cuando se habla de conexiones HTTP (puerto 80), también se incluyen las seguras, HTTPS (puerto 443). De hecho, en todos los servidores se realiza una redirección (o reescritura) en el Apache para que sean todas las conexiones seguras.

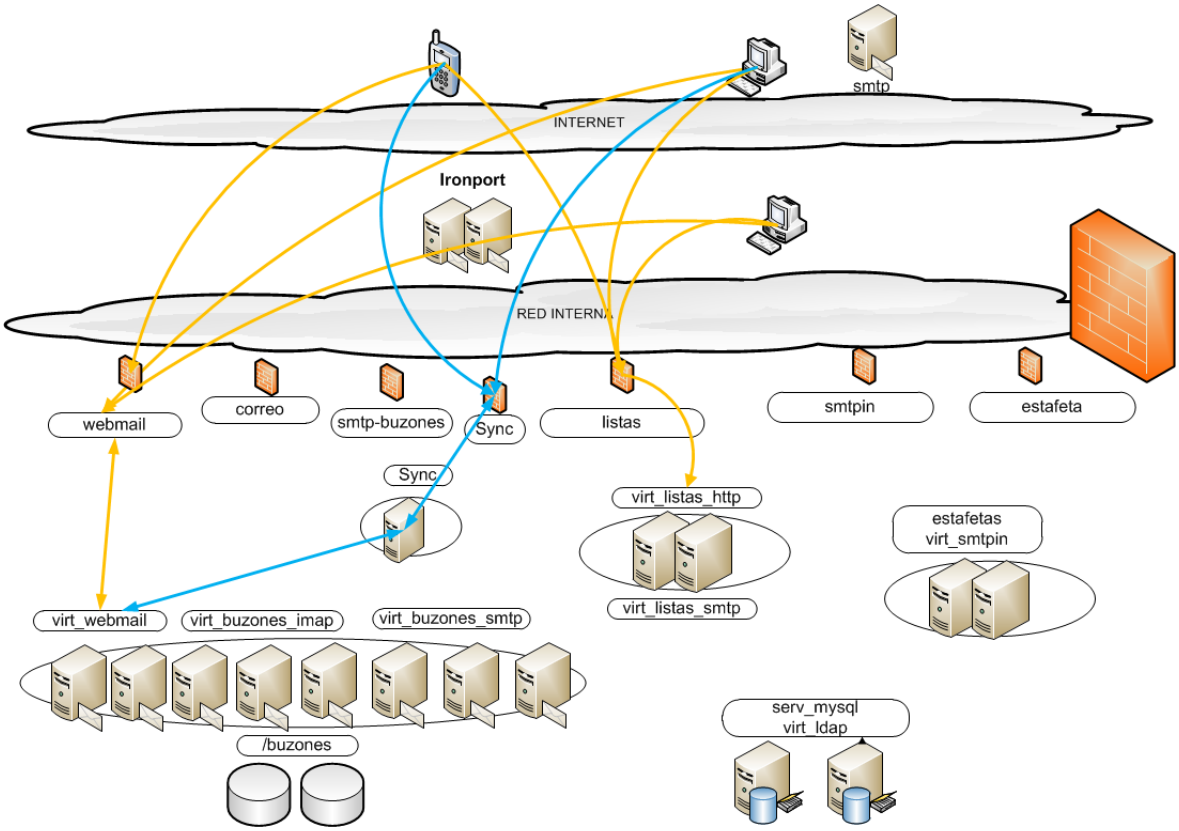

Figura 49 - Flujo HTML

3.2.2 POP3/IMAP

Las conexiones POP3 e IMAP recorren los mismos caminos, pero el funcionamiento es distinto. Estas conexiones, ya sean internas o externas, realizan un recorrido similar al del flujo HTTP, pero a diferentes puertos y servicios.

Los usuarios que opten por conexiones POP3, descargarán todo su correo almacenado en el servidor en el dispositivo/ordenador desde el que ejecuten este protocolo. Mientras que los que se decanten por IMAP podrán acceder a su correo desde cualquier dispositivo y localización ya que el correo se mantiene en el servidor y simplemente se hacen consultas. El flujo de este tráfico, como se ha comentado, es similar al de HTTP: en el cortafuegos se hace el *nateo* de la IP pública a la privada y después, en los switches se realiza el balanceo a los diferentes servidores, que serán en este caso los de correo propiamente dichos donde se encuentra la aplicación de consulta/descarga MDA.

Están disponibles los accesos seguros (POP3S puerto 995, IMAPS puerto 993) y no seguros (POP3 puerto 110, IMAP puerto 143) a estos protocolos, aunque siempre es recomendable habilitar sólo los seguros.

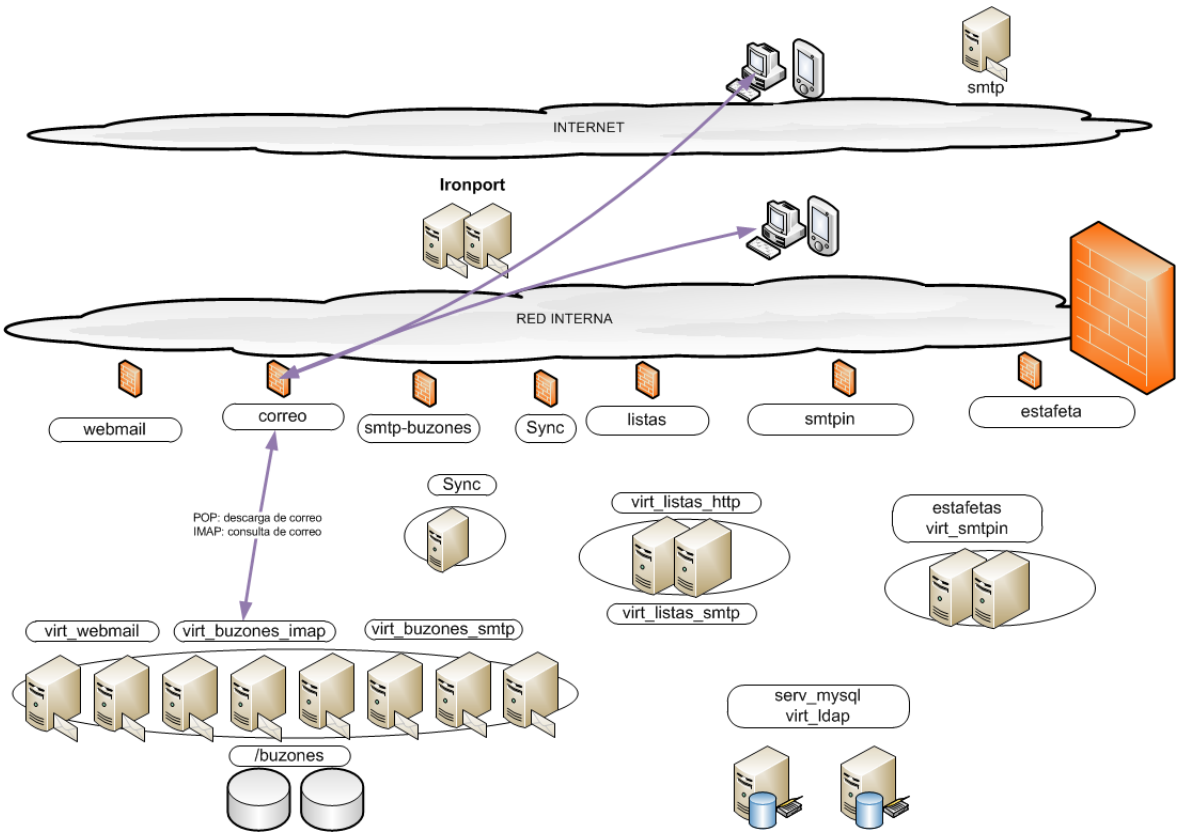

Figura 50 - Flujo POP·/IMAP

3.2.3 SMTP

En cuanto a las conexiones de envío de correo, SMTP, el flujo se complica un poco más, debido a la existencia de listas con subdominios. Se analizarán por orden.

Desde la aplicación de webmail, el correo saliente irá directamente a las estafetas, que mandarán todo este tráfico a los Ironport para que analicen el contenido en caso de haya algún tipo de virus, o si se trata de un ataque de SPAM. Una vez en los Ironport, se decidirá si el correo es local o externo. Si fuera externo, simplemente tienen que enviarlo a los diferentes MX que respondan a los dominios de los recipientes. Si el correo es local, se mandará a la IP de servicio virtual de smtp-buzones, que se encargará de entregarlo a los

MTA de los servidores de correo, que seguidamente entregarán al MDA almacenando así el los mensajes en los buzones locales.

De manera muy similar si se trata de un correo externo para usuarios de la plataforma. Entrarán por los Ironport que, examinarán si ese correo es legítimo y lo entregarán de nuevo al servicio virtual de smtp-buzones, haciendo lo mismo que en el caso anterior.

Como se ha comentado a lo largo del presente PFC, existen dos tipos de listas: las que son directamente dominio de listas y las que constan de algún subdominio. Las primeras, entran directamente, a través del servicio virtual de listas, a los servidores de listas, donde se procederá a distribuir (o no) el mensaje a los suscriptores. En las segundas, al tener subdominios que otros usuarios podrían tener, no se realiza tan directamente, si no que llegan hasta los MTA de los servidores de correo que, mediante el uso de routers y transports harán consultas al LDAP y examinarán cierto campo en la información de la cuenta de correo electrónica en estudio. Si este campo tiene un cierto valor, se sabe que se trata de una lista, y por tanto, se enviará a los servidores de listas, donde se procederá a su distribución (o no).

En ambos casos, si los suscriptores fueran externos a la plataforma de correo, los servidores de listas, que también tienen un MTA, enviarán estos correos a las estafetas que, a través de los Ironport, serán dirigidos a los diferentes MX. Para los suscriptores internos, al tener los servidores de listas un MDA y acceso a los buzones, la entrega es inmediata.

Este flujo SMTP, internamente se realiza mediante protocolo no seguro (puerto 25). Sin embargo, desde fuera se disponen tanto el no seguro, el seguro (465) y el submission (587). La diferencia de estos puertos está explicada en el apartado de protocolos. Como se ha comentado antes, sería recomendable habilitar sólo los seguros, 465 y 587.

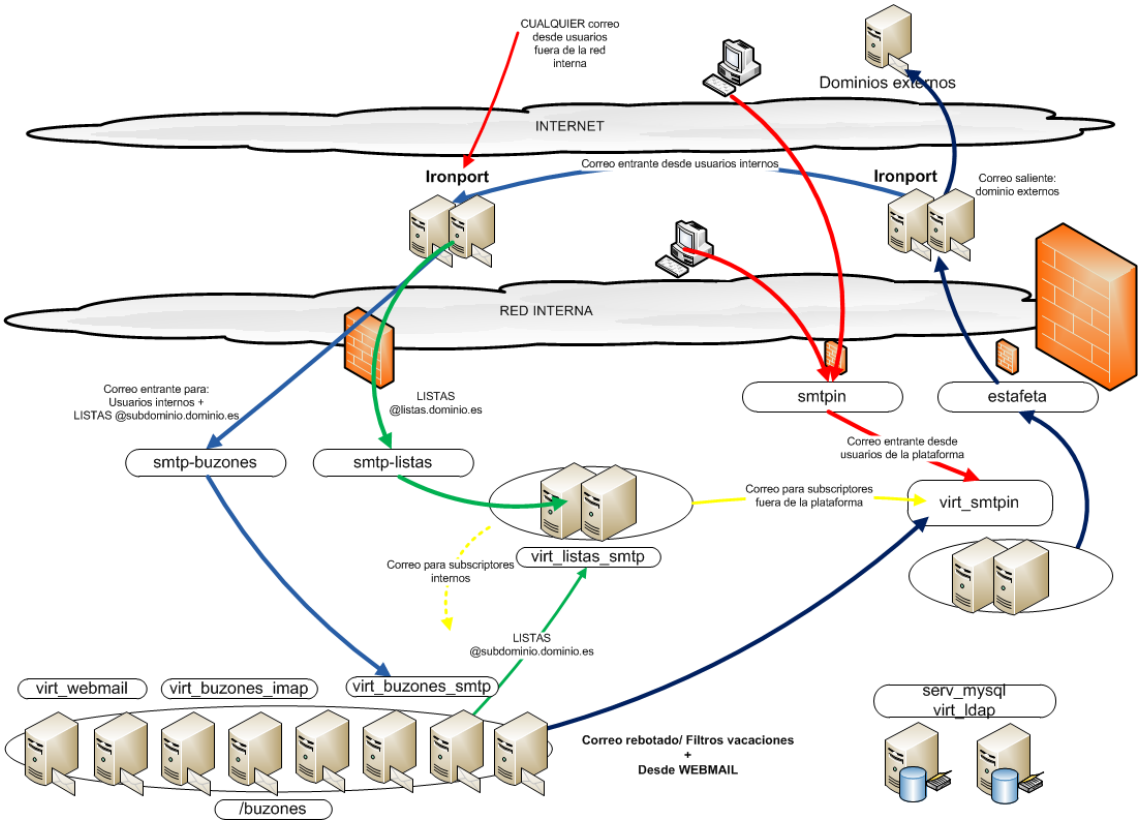

Figura 51 - Flujo SMTP

4 Desarrollo

En esta sección se tratará la instalación y configuración de los elementos de la plataforma de correo electrónico: servidor de correo, estafetas y listas. Además se tratará a grandes rasgos la instalación de los cortafuegos así como su configuración, y la configuración de los switches se comentará (grupos virtuales, balanceo…). Los Ironport ya se han detallado su funcionamiento y características lo suficiente pero no entrarán en el ámbito de este PFC, ya que su instalación y configuración es bastante extensa.

Se comenzará de fuera hacia dentro, tal y como se ha hecho anteriormente en el presente PFC.

Se partirá de una máquina con el software básico de un servidor Linux. Todas con Scientific Linux 5.x. Se omitirán la mayoría de dependencias de los productos, pues no será relevante para el desarrollo de esta memoria.

4.1 Cortafuegos

Los cortafuegos serán la primera capa de la plataforma, restringiendo los accesos a la infraestructura de correo.

Se basan en iptables, programa disponible en el kernel de Linux que permite interceptar y manipular paquetes de red, entrante y saliente. Además, permite realizar la traducción de nombres de red (NAT) y mantener registros de log de dichas conexiones.

Como está incluido en el núcleo de Linux, está disponible para su uso, simplemente habrá que configurarlo para un correcto funcionamiento de la plataforma.

Para administrar las reglas de los cortafuegos, se puede emplear un comando muy útil: *iptables*. Con él se pueden añadir reglas, eliminarlas, visualizarlas… Sin embargo, para hacer que todos estos cambios sean permanentes, habrá que editar directamente el archivo de configuración */etc/sysconfig/iptables* (ejemplo en anexo IPTABLES).

Primero se definirá un nombre para un conjunto de reglas del cortafuegos, así se podrán administrar diferentes conjuntos de reglas, y redirigimos el tráfico a él.

```
# iptables -A INPUT -j RH-Firewall-1-INPUT
# iptables -A FORWARD -j RH-Firewall-1-INPUT
```

Por ejemplo, para aceptar de primeras todo el tráfico entrante a los diferentes puertos de la plataforma, habrá que ejecutar el siguiente comando:

```
# iptables -A RH-Firewall-1-INPUT-p tcp -m multiport --dports
25,80,110,143,443,465,587,993,995 -j ACCEPT
```

Para rechazar el resto de conexiones, al final del apartado INPUT, se pondrá:

```
# iptables -A RH-Firewall-1-INPUT-p tcp -j DROP
# iptables -A RH-Firewall-1-INPUT-p udp -j DROP
```

Y así con todas las diferentes reglas que se quieran añadir.

Por otra parte, tal y como se ha comentado, con *iptables* se procederá a traducir nombres de red. Es decir, se hará la traducción de direcciones públicas a direcciones privadas internas a la plataforma.

Tendremos cuatro IP de servicio, que serán para Webmail, consulta de correo POP3/IMAP, listas de distribución y envío de correo:

```
# iptables -A PREROUTING -i eth1 -d 161.111.10.241 -j DNAT --to-destination
192.168.100.201
# iptables -A PREROUTING -i eth1 -d 161.111.10.242 -j DNAT --to-destination
192.168.100.204
# iptables -A PREROUTING -i eth1 -d 161.111.10.223 -j DNAT --to-destination
192.168.100.205
# iptables -A PREROUTING -i eth1 -d 161.111.10.239 -j DNAT --to-destination
192.168.100.202
```

Tal y como se observa, se hará uso de la herramienta de *forwarding* en el servidor de cortafuegos. Por ello, es importante activar esta propiedad en la configuración de dichos servidor. Esto se realiza en el fichero */etc/sysctl.conf*, habilitando la opción (poniendo valor a 1) en el siguiente parámetro:

```
…
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
…
```

4.2 SWITCHES

Los switches se encargarán de balancear las conexiones según esté la carga en las diferentes máquinas de la plataforma, dentro de grupos de servicio virtuales, además de los puertos de dichos servicios (SMTP, HTTP, IMAP…).

Así pues, se tendrán los siguientes servicios: buzones_webmail, estafetas, buzones_smtp, buzones_imap, listas_http, listas_smtp.
Cada servicio virtual se encarga de proveer una funcionalidad.

En el anexo SWITCHES se encuentra un *dump* de la configuración general de los switches.

4.3 ALMACENAMIENTO

Se encuentran cabinas de almacenamiento NetApp accesibles sólo desde los buzones por NFS. En estas cabinas se encuentran los diferentes buzones de usuario donde se almacenarán todos los correspondientes correos. Estos buzones se dividen en varios volúmenes dentro de las cabinas en un mismo agregado. Estos volúmenes se distribuyen según un identificador que lleva cada usuario en el LDAP, depende del número con el que acabe dicho identificador, irá a un volumen u otro (del 0 al 9).

Para que los servidores de correo puedan montar los volúmenes NFS y acceder a los buzones de usuario, hay que montar los directorios donde se almacenarán y configurar el archivo */etc/fstab* para que los puntos de montaje estén disponibles en cada arranque de la máquina.

```
# --- Netapp

192.168.11.244:/vol/listas                        /listas                        nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.243:/vol/buzon00                       /buzon/buzon0                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.243:/vol/buzon01                       /buzon/buzon1                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.243:/vol/buzon02                       /buzon/buzon2                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.243:/vol/buzon03                       /buzon/buzon3                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.243:/vol/buzon04                       /buzon/buzon4                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.243:/vol/backups                      /config_backup                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.244:/vol/buzon05                       /buzon/buzon5                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.244:/vol/buzon06                       /buzon/buzon6                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.244:/vol/buzon07                       /buzon/buzon7                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.244:/vol/buzon08                       /buzon/buzon8                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
192.168.11.244:/vol/buzon09                       /buzon/buzon9                  nfs
soft,intr,rsize=32768,wsize=32768,timeo=600,retrans=2        0 0
```

4.4 BUZONES

Los buzones de correo se encargarán de varias tareas. La primera será la de recoger los correos entrantes que lleguen desde los Ironport para entregarlos en los correspondientes buzones (aplicando filtros de usuarios en caso de existir). Además, se encargarán de gestionar la consulta del correo mediante los protocolos IMAP y POP3. Tendrán la herramienta de webmail instalada en ellos, que a su vez hará la consulta a los correos mediante IMAP.

El acceso a los buzones de usuario, y correspondientes correos, lo realiza un usuario específico, *vmail*.

```
# useradd -u 501 dovecot
```

4.4.1 Dovecot

La herramienta encargada de la entrega de correo en los buzones, así como de la consulta del correo mediante los protocolos IMAP y POP3 será Dovecot.

Para la instalación de esta herramienta, primero se descargarán los archivos fuentes desde la página oficial:

```
# wget http://www.dovecot.org/releases/2.1/dovecot-2.1.6.tar.gz
```

Hay que tener en cuenta que a partir de la versión 2.x de Dovecot, es necesaria la creación de los usuarios *dovecot* y *dovenull*.

```
# useradd -u 500 dovecot
# useradd -g 500 dovenull
```

Se descomprime el fichero y se accede al directorio para proceder a la configuración e instalación:

```
# tar zxvf dovecot-2.1.6.tar.gz
# cd dovecot-2.1.6
```

A continuación, se procederá a configurar los parámetros de la instalación. Se especificará entre otros la ruta de instalación, la integración con LDAP, el uso de SSL… Y se realiza la instalación sencilla mediante compilación e instalación de la aplicación:

```
# ./configure --prefix=/usr/local/dovecot --disable-dependency-tracking --with-
ldap --with-ssl=openssl --with-ssldir=/etc/ssl
# make
# make install
```

De esta manera ya estaría instalada la aplicación de entrega y consulta del correo con la configuración estándar.

Se procederá a personalizar dicha configuración. Ésta se encuentra detallada y al completo en el anexo DOVECOT.

Para una gestión más centralizada de las configuraciones de las aplicaciones del servidor, se hará un enlace simbólico de la carpeta de configuración de Dovecot en el directorio *etc*.

```
# ln -s /usr/local/dovecot/etc/dovecot/ /etc/dovecot
```

Se especifica el tipo de buzón (*Maildir*), el usuario con privilegios para acceder a ellos, los diferentes plugins de los que se hará uso, mecanismo de autenticación (en este caso es LDAP, y por ello es necesario la creación de un archivo de configuración con los parámetros y atributos de búsqueda para usuarios), puertos de los protocolos, certificados…

Para que el sistema avise de la cuota del usuario en determinados porcentajes, dentro de la definición del plugin de cuota, se ha creado un script que se ejecutará cuando sobrepasen los límites definidos en la configuración (*quota-warning*). Se trata del script */usr/local/dovecot/bin/quota-warning.sh*:

```
#!/bin/sh
PERCENT=$1
cat << EOF | /usr/local/dovecot/libexec/dovecot/deliver -d $USER
From: postmaster@correo.es
To: $USER
Subject: Atención - Su buzón se encuentra al $PERCENT% de su capacidad

Este mensaje ha sido generado de forma automática por el servidor de correo.

Ha superado el $PERCENT% de la capacidad de su buzón de correo.

Cuando llegue al 100% no podrá seguir recibiendo correos.

Se recomienda eliminar mensajes innecesarios y vaciar la papelera.
EOF
```

Ahora, se añadirán al servidor las capacidades de filtrado. Esto se realizará mediante filtros Sieve. Con las versiones 2.x de Dovecot, esto se puede hacer con los paquetes de Pigeonhole.

Primero se descargarán los archivos fuentes:

```
# wget http://www.rename-it.nl/dovecot/2.1/dovecot-2.1-pigeonhole-0.3.5.tar.gz
```

Y de la misma manera, se descomprime, compila e instala. Para que sepa cómo interactuar con Dovecot, hay que especificarlo:

```
# tar zxvf dovecot-2.1-pigeonhole-0.3.5.tar.gz
# cd ../dovecot-2.1-pigeonhole-0.3.5
# ./configure --with-dovecot=/usr/local/dovecot/lib/dovecot/
# make
# make install
```

Por último, hay que completar la configuración de Dovecot para incluir la de los filtros Sieve, además de añadir el servicio al arranque del servidor:

```
# chkconfig --add dovecot
```

Para que la aplicación pueda registrar los logs en el directorio especificado, habrá que crearlo (*/var/log/dovecot/*).

4.4.2 EXIM

La siguiente etapa del correo será el MTA de los buzones, que se encargará de recoger los correos de los Ironport y distribuirlos o a el MDA o a las máquinas de listas de distribución. Además, hace la comprobación de si el usuario es válido o no.

Primero, hay que crear el usuario *exim*:

```
# groupadd -g 93 exim
# useradd -g 93 -u 93 -M exim
```

La opción "-M" es para que no se cree el directorio de usuario.
A continuación, hay que editar el fichero */etc/passwd* de manera que quede:

```
…
exim:x:93:93::/var/spool/exim:/sbin/nologin
…
```

Se descargan los ficheros fuente y se descomprimen:

```
# wget ftp://ftp.carnet.hr/misc/exim/exim/exim4/old/exim-4.77.tar.gz
# tar zxvf exim-4.77.tar.gz
# cd exim-4.77.tar.gz
```

Se copia el fichero *src/EDITME* a *Local/Makefile*. Y se edita este fichero.
Aquí se indican los usuarios que harán uso del aplicativo, los diferentes componentes de los que hará uso (como el LDAP), y otras restricciones y opciones para Exim. Todos estos parámetros luego se pueden modificar directamente en el fichero de configuración.

Una vez que se ha personalizado correctamente el fichero, se compilará e instalará:

```
# make
# make install
```

Hay que crear un enlace simbólico del binario de Exim:

```
# ln -s /usr/exim/bin/exim /usr/sbin/exim
```

Además, habría que borrar el binario de *Sendmail*, o hacer un enlace simbólico de éste a Exim.
A continuación, se crea el fichero de arranque de Exim y se añade al arranque del servidor:

```
# chkconfig --add exim
```

Por último, hay que crear el directorio de logs, darle los permisos, y hacer que apunte a dicho directorio el verdadero de los logs:

```
# mkdir /var/spool/exim/log
# chown -R exim:exim exim/
# ln -s /var/spool/exim/log /var/log/exim
```

En la configuración de Exim, se van a definir los diferentes *routers* para los distintos tipos de correo. Primero se encuentra el *router* que enviará a las estafetas de salida los correos no locales.

Luego está el de listas, que identificará si un correo es de una lista o no y procederá a entregarlo en los servidores de listas de distribución donde se procederá a su procesado.

A continuación se encuentra el de usuarios locales. Éste comprueba si el usuario es local. En tal caso, procederá a entregarlo al MDA (Dovecot) y éste a los buzones.

Por último, en el caso de que el correo en cuestión no se adapte a ninguno de los *router* mencionados, se dará por sentado que Exim no encuentra cómo procesar dicho correo (probablemente tenga un MX diferente al local). Por tanto, se enviará a las estafetas para su envío al exterior.

Una vez que se tienen los *router* definidos, Exim tiene que saber qué hacer con los correos que cumplen las condiciones de estos *router*. Esto se hace en los *transport*. Como sólo un *router* procesa el mensaje hacia dentro (el resto lo manda a otros servidores), se creará un *transport* para él. Se trata el de usuarios locales. En éste se define que los correos locales se enviarán a través de Dovecot y éste se encargará de procesarlo.

El fichero completo de configuración se encuentra en el anexo EXIM.

4.4.3 WEBMAIL – OPEN XCHANGE

[67] Se ha seleccionado Open-Xchange como la solución Groupware de software libre para esta plataforma. Su instalación se llevará a cabo mediante repositorios. Habrá que añadirlos. Para ello, lo primero es crear un fichero */etc/yum.repos.d/ox.repo* que contendrá:

```
[ox]
name=Open-Xchange
baseurl=http://software.open-xchange.com/OX6/stable/RHEL5/
gpgkey=http://software.open-xchange.com/oxbuildkey.pub
enabled=1
gpgcheck=1
metadata_expire=0m
```

Después de añadir el repositorio, es recommendable actualizar el sistema, aunque si no está seguro de las implicaciones que esto conlleva respecto a los demás aplicativos instalados, mejor no hacerlo.

Una vez que se tiene el repositorio activo, se instalará la solución. Como se van a instalar todos los paquetes en un solo servidor, bastará con ejecutar el siguiente comando:

```
# yum install open-xchange-meta-singleserver open-xchange-authentication-imap
open-xchange-mailfilter open-xchange-spamhandler-default java-sun
```

Esto instalará el servidor completo de Open-Xchange (por defecto en */opt/open-xchange/*), el plugin para la autenticación mediante IMAP, el plugin para la creación y uso de filtros de correo, un sencillo programa de anti-SPAM y los paquetes necesarios de JAVA.

Para poder trabajar a partir de aquí más cómodo, se añadirán las rutas de los binarios de Open-Xchange al sistema:

```
# echo PATH=$PATH:/opt/open-xchange/sbin/ >> ~/.bashrc && . ~/.bashrc
```

Además, para aligerar el peso del presente PFC, sólo se mostrarán los parámetros que se van a modificar, el resto serán por defecto. Aquellos ficheros de configuración que requieran una total remodelación o creación, se encontrarán en el anexo Open-Xchange.

Ahora que se tienen todos los paquetes necesarios instalados, se procederá a toda la configuración de la plataforma. En primer lugar, hay que indicar que la base de datos está en otro servidor y las credenciales. Esto se realiza en */opt/open-xchange/etc/admindaemon/configdb.properties*, modificando lo siguiente (en concordancia con las características de los servidores *bbddX*):

```
# readURL holds the database host and the used schema name
readUrl=jdbc:mysql://serv_mysql/configdb
# username for the database user
readProperty.1=user=openexchange
# password for the database user
readProperty.2=password=p4ssw0rd3

# writeURL holds the database host and the used schema name
writeUrl=jdbc:mysql://serv_mysql/configdb
# username for the database user
writeProperty.1=user=openexchange
# password for the database user
writeProperty.2=password=p4ssw0rd3
```

Una vez que se tiene configurada la base de datos, se iniciará la parametrizacion de la misma estableciendo un usuario de administración para la misma:

```
# initconfigdb --configdb-pass=pass_db -a
initializing configdb from scratch... done
```

Ahora se procederá a crear todos los ficheros de configuración del sistema, con todos los valores por defecto. Al ser de software libre, se indicará que no se dispone de licencia.

```
/opt/open-xchange/sbin/oxinstaller --no-license --servername=buzon --configdb-
pass=pass_db --master-pass=master_pass --ajp-bind-port=localhost --servermemory
MAX_MEMORY_FOR_JAVAVM
setting up groupware configuration /opt/open-xchange/etc/groupware
....
skipping configuration of URL in /opt/open-
xchange/etc/groupware/configjump.properties
.....................................
groupware daemon must now be restarted if already running
setting up admin daemon configuration /opt/open-xchange/etc/admindaemon
....................
*** RMI authentication is enabled
using oxadminmaster as master account
admin daemon must now be restarted if already running
```

Donde el parámetro MAX_MEMORY_FOR_JAVAVM será aproximadamente la mitad del máximo de la máquina, debido a que hay más aplicativos implicados en la plataforma en el servidor. Si se quisiera disponer de una configuración en clúster, el parámetro *–ajp-bind-port* deberá ser "*".

A continuación, se configurará cómo accederán los usuarios a Webmail, así como los diferentes parámetros del servidor. Es decir, se va a definir que el servidor IMAP es el propio servidor y el servidor de correo saliente las estafetas.

```
com.openexchange.mail.mailServerSource=global

com.openexchange.mail.transportServerSource=global

com.openexchange.mail.mailServer=localhost

com.openexchange.mail.transportServer=estafetas
```

Como se ha comentado, se va a realizar autenticación IMAP, aprovechando que se tiene Dovecot instalado en la misma máquina, facilitando así el aprovisionamiento de usuarios y la configuración de la solución.

Primero, hay que indicar al plugin de autenticación IMAP que tome sólo la parte de usuario que corresponde al *login*. Esto se realizará en el fichero */opt/open-xchange/etc/groupware/imapauth.properties*:

```
USE_FULL_LOGIN_INFO=false
```

El resto se dejará como está, ya que por defecto autentica a localhost.

A continuación, se configurará para que Open-Xchange haga uso de los filtros sieve. En el fichero */opt/open-xchange/etc/groupware/mailfilter.properties* se encuentran los principales parámetros para su configuración. Al igual que pasaba con el plugin de autenticación IMAP, al encontrarse en el mismo servidor, este fichero funcionará correctamente con los valores de por defecto, salvo el puerto, que habrá que indicarle el correcto (consultar la configuración de Dovecot en caso de duda):

```
SIEVE_PORT=4190
```

Una vez que se tiene configurado el sistema Open-Xchange, se procederá al registro de contextos, almacenamientos, etc. de la plataforma.

Primero hay que registrar el servidor en la base de datos:

```
# registerserver -n oxserver -A master_ox_admin -P master_pass
server 1 registered
```

Después se creará el directorio para intercambio de ficheros. Este sistema permite el intercambio hacia todos los usuarios, a grupos de usuarios, o privado de cada usuario. Y después se registrará en la base de datos:

```
# mkdir /var/opt/filestore
# chown open-xchange.open-xchange /var/opt/filestore
# registerfilestore -A master_ox_admin -P master_pass -t file:/var/opt/filestore
-s 1000000
filestore 2 registered
```

Por último, se registrar la base de datos de la solución entera, donde se almacenarán todos los datos específicos y de cada usuario:

```
# registerdatabase -A master_ox_admin -P master_pass -n openxchange -p pass_db -m
true
database 3 registered
```

Una vez que se tiene configurada toda la solución de Webmail, hay que configurarla para que funcione con el servidor Apache y que funcione correctamente con el módulo AJP. El módulo AJP permite enviar solicitudes desde un servidor web a un servidor de aplicaciones que se encuentra detrás del primero.

Para ello se creará el fichero */etc/httpd/conf.d/proxy_ajp.conf* en el que se encontrará toda la configuración del módulo para que quede integrado perfectamente en el Apache HTTP. Este fichero se encuentra en el anexo Open-Xchange.

Después, hay que modificar la configuración del HTTP para que incluya los accesos y permisos del Open-Xchange. Para no editar directamente la configuración del servidor evitando así también posibles modificaciones no deseadas ante actualizaciones del sistema, se creará el fichero */etc/httpd/conf.d/ox.conf* en el que se definirá por completo un host virtual para la solución de correo.

Ahora se añaden los servicios al inicio del sistema:

```
# chkconfig --level 345 httpd on
# chkconfig --level 345 open-xchange-groupware on
# chkconfig --level 345 open-xchange-admin on
```

Sólo quedaría levantar los servicios y el sistema estaría funcionando:

```
# /etc/init.d/httpd restart
# /etc/init.d/open-xchange-groupware start
```

Se creará un contexto que será el de por defecto del sistema, en el que todos los usuarios se autenticarán, identificando nombre de contexto y administrador. Si se creasen diferentes contextos, los usuarios podrían seleccionarlo en la pantalla de login. Sólo uno puede ser el contexto por defecto.

```
# createcontext -A master_ox_admin -P master_pass -c 1 -u administrador -d
"Administrador" -g Admin -s User -p admin_pass -L correo.es -e
administrador@correo.es -q 1024 --access-combination-name=all
context 1 created
```

Ahora se tendría el contexto para el dominio *correo.es*. Si se quisieran añadir más, basta con ejecutar el siguiente comando:

```
# changecontext -A master_ox_admin -P master_pass -c 1 -L testing.correo.es
```

Comprobando que, efectivamente se tienen los dos contextos (dominios):

```
# listcontext -A master_ox_admin -P master_pass
cid fid fname       enabled qmax qused name lmappings
  1   2 1_ctx_store true    1024     2 1    testing.correo.es,correo.es
```

Ya estaría finalizada la instalación y configuración de la herramienta colaborativa Open-Xchange, con base de datos externa y autenticación mediante IMAP.

4.4.4 FUNAMBOL

Se partirá de un servidor con similares características al resto. Así pues, no se comentarán las dependencias que hagan falta a la hora de instalar los productos.

Para empezar, hay que descargar el archivo binario y lo ejecutaremos para llevar a cabo la instalación.

```
# wget http://downloads.sourceforge.net/project/funambol/bundle/v10/funambol-
10.0.3.bin?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Ffunambol%2Ffiles%2Fbundle%
2Fv10%2F&ts=1380163487&use_mirror=switch
# chmod +x funambol-10.0.3-x64.bin
# ./funambol-10.0.3-x64.bin
```

Ahora saldrá toda la licencia, la cual habrá que aceptar al final, después de leerla:

```
...
Do you agree to the above license terms? [yes or no]
yes
Directory to extract Funambol [/opt] <return to accept>?

Unpacking...
Checksumming...
Extracting... to /opt/Funambol

Do you want to start the server? [yes or no]
yes
```

Para poder trabajar con la base de datos, se deberá crear en los servidores *bbddX*.

```
# mysql -uroot -p
mysql> create database funambol;
mysql> create user funambol identified by 'funambol';
mysql> grant all on funambol.* to 'funambol'@'%' identified by 'funambol';
mysql> flush privileges;
```

El servidor Funambol deberá ser capaz de conectar con la base de datos MySQL, para ello hay que instalar un conector necesario, y copiarlo a una ubicación dentro de Funambol (esto no es necesario, pero recomendable).

```
# yum install mysql-connector-java.noarch
#   cp   /usr/share/java/mysql-connector-java-5.1.17.jar   /opt/Funambol/tools/jre-
1.6.0/mysql-connector-java.jar
```

Una vez que se tiene lista la comunicación con la MySQL por parte de Funambol, hay que indicar los parámetros de la conexión. Esto se realiza en el fichero */opf/Funambol/ds-server/install.properties*:

```
dbms=mysql

jdbc.classpath=/opt/Funambol/tools/jre-1.6.0/mysql-connector-java.jar
jdbc.driver=com.mysql.jdbc.Driver
jdbc.url=jdbc:mysql://serv_mysql/funambol?characterEncoding=UTF-8
jdbc.user=funambol
jdbc.password=funambol
```

Con esto se tendría la configuración básica del servidor Funambol. Sin embargo, antes de completar la instalación del mismo con los módulos o conectores, hay que instalarle el conector para Open-Xchange.

Para la instalación del conector *ox-listener*, primero hay que descargar los ficheros:

```
# wget http://download.forge.objectweb.org/sync4j/funambol-ox-module-7.0.8.zip
# unzip funambol-ox-module-7.0.8.zip
```

Dentro se encuentra el fichero de conector necesario para la instalación del módulo, que deberemos copiar a la ubicación */opt/Funambol/ds-server/modules/*, y otros ficheros de configuración, que deberán copiarse a la carpeta de Funambol.

```
#      cp      Funambol/ox-connector/ox-connector-7.0.8.s4j      /opt/Funambol/ds-
server/modules/
# unzip funambol-ox-listener-7.0.8.zip
# cp -r Funambol/* /opt/Funambol/
```

Ahora, hay que añadir el plugin al fichero de instalación de Funambol (*install.properties*):

```
#
# Modules definitions
#
modules-to-install=content-provider-10.0.0,email-connector-10.0.0,foundation-
10.0.0,phones-support-10.0.0,webdemo-10.0.0,ox-connector-7.0.8
```

Hay que indicar al conector la versión de JAVA instalada. Esto se realiza en el fichero */opt/Funambol/bin/ox-listener*:

```
# Setting the JAVA_HOME to the JRE in the bundle if not set or if not correctly
set
if [ -z "$JAVA_HOME" ]; then
    JAVA_HOME=$FUNAMBOL_HOME/tools/jre-1.6.0/jre
else
    if [ ! -f "$JAVA_HOME/bin/java" ]; then
        JAVA_HOME=$FUNAMBOL_HOME/tools/jre-1.6.0/jre
    fi
fi
```

Además, hay que configurar las URL para que Funambol sepa dónde estarán los servidores Open-Xchange. Hay que realizar modificaciones en dos ficheros del conector:

```
# vi /opt/Funambol/config/com/funambol/oxlistener/task/OXListenerTask.xml
...
        <void property="OXUrl">
            <string>http://servidor_ox:80</string>
        </void>
...

# vi /opt/Funambol/config/ox/ox/OXConnector.xml
...
        <void property="OXUrl">
            <string>http://servidor_ox:80</string>
        </void>
...
```

También hay que configurar la URL en otro fichero, esta vez del servidor:

```
# vi /opt/Funambol/config/Funambol.xml
…
    <void property="serverURI">
     <string>http://servidor_ox:8080/funambol/ds</string>
    </void>
…
```

Una vez que se tiene tanto el servidor como los módulos preparados, se finalizará la instalación mediante el siguiente comando:

```
# /opt/Funambol/bin/install-modules
```

Si se trata de la primera instalación del servidor de Funambol, habrá que recrear todas las bases de datos. Si esto no fuera así, si ya existiese una instalación anterior, si se recrean las bases de datos se perderán todos los datos.

```
...
  [iterate] Do you want to recreate the database?
  [iterate]               (y,n)
y
...
```

Si todo está correcto, se observará al final *BUILD SUCCESSFUL*, y se tendría el servidor Funambol instalado correctamente, atacando a la MySQL y con el conector de Open-Xchange configurado.

4.4.5 SYMPA

Sympa es la aplicación encargada de las listas de distribución. Al hacer entrega y envío de correo, estos servidores también disponen de MDA (Dovecot) y MTA (Exim). Así pues, en esta sección se detallará la instalación de Sympa, además de su puesta en alta disponibilidad, un añadido más al balanceo ofrecido por los switches.

La instalación de Sympa es sencilla, pero hay que tener en cuenta que muchos paquetes de PERL serán necesarios para su correcto funcionamiento. Como se ha comentado, estas dependencias no serán discutidas aquí [68].

Antes de nada, habrá que crear el usuario *sympa*, que será el encargado de hacer las operaciones del servidor web Apache HTTP, al igual que con los servidores Webmail.

```
# useradd –u 502 sympa
```

Primero, se descargarán los ficheros fuente y se descomprimen:

```
# wget https://www.sympa.org/distribution/sympa-6.1.17.tar.gz
# tar zxvf sympa-6.1.17.tar.gz
# cd sympa-6.1.17
```

Ahora, habrá que definir las opciones de compilación. En ellas se determinarán los diferentes directorios para los elementos de Sympa:

```
#   ./configure   --prefix=/home/sympa   --with-confdir=/home/sympa/etc   --with-
mandir=/home/sympa/man          --with-initdir=/home/sympa/init          --with-
piddir=/home/sympa/pid          --with-lockdir=/home/sympa/lock          --with-
sendmail_aliases=/home/sympa/etc/sympa_aliases
```

Una vez que se ha configurado la instalación, se procederá a la misma:

```
# make
# make install
```

Una vez concluida la instalación, al haberla hecho como usuario *root*, hay que redefinir los permisos para los directorios de Sympa:

```
# chown –R sympa.sympa /home/sympa
```

Ahora simplemente hay que configurar la aplicación. Existen dos tipos de ficheros de configuración para Sympa. Uno de ellos, el principal, es para configurar el comportamiento de la herramienta. El otro es para la configuración de la parte web.

En el primero, *sympa.conf*, se definirán los distintos directorios para los diferentes tipos de mensajes (moderación, subscriptores, distribución…), los listmaster de la aplicación, la URL, etc. Ver anexo SYMPA.

En el fichero de configuración *wwsympa.conf* se van a definir los parámetros web, como la página inicial a mostrar o características de *cookies* entre otros.

Por otra parte, para que se pueda autenticar los usuarios por LDAP, habrá que editar un archivo de configuración, *auth.conf*. En el que se determinarán los parámetros de conexión al LDAP y el tipo de filtro que se va a realizar y los resultados esperados.

```
## Here is the default auth.conf
## It defines the authentication backends used by Sympa

#
# AUTENTICACION CONTRA LDAP
#
ldap
        host                            virt_ldap:636
        use_ssl                         1
        timeout                         20
        suffix                          idnc=usuarios,dc=correo,dc=es
        bind_dn                         cn=mailuser,dc=correo,dc=es
```

```
        bind_password                   p4ssw0rd
        get_dn_by_email_filter
(|(mail=[sender])(mailAlternateAddress=[sender]))
        #get_dn_by_email_filter          (mailAlternateAddress=[sender])
        alternative_email_attribute     mailAlternateAddress
        email_attribute                 mail
        scope                           sub

#
# AUTENTICACION INTERNA
#
user_table
       #regexp                 .*
        negative_regexp         \.correo\.es
```

Una vez que se tiene toda esta configuración lista, habrá que hacer alguna modificación en la configuración del servidor Apache para que se redireccione a las listas y puedan trabajar correctamente con los módulos *cgi* de Sympa. Concretamente, habrá que modificar el archivo *httpd.conf* para incluir lo siguiente:

```
############################################################################
#                              - SYMPA -                                   #
############################################################################

<IfModule mod_fcgid.c>
  IPCCommTimeout 1200
  MaxProcessCount 2
</IfModule>

<Location /wws>
  SetHandler fcgid-script
  Options +ExecCGI
</Location>

# Alias concretos para cada robot
# Aqui se aÃ±adiran los alias correspondientes a los subdominios de las
# listas
#
# Ejemplo: ScriptAlias /subdominio/wws            /home/sympa/bin/wwsympa.fcgi
ScriptAlias /wws                        /home/sympa/bin/wwsympa.fcgi
ScriptAlias /correo/wws                   /home/sympa/bin/wwsympa.fcgi
ScriptAlias /testing/wws                /home/sympa/bin/wwsympa.fcgi

# Alias comunes para todos los robots
Alias /wwsicons /home/sympa/static_content/icons
Alias /static-sympa /home/sympa/static_content

############################################################################
#                        FIN - SYMPA -                                     #
############################################################################
```

De este modo, para cada subdominio (robot) redirigirá correctamente a la página correspondiente. Obsvérvese que el módulo *mod_fcgid* de Apache deberá estar instalado, ya que no viene en las instalaciones por defecto de los servidores.

4.4.5.1 Alta disponibilidad

Ya estarían listos los servidores de listas de distribución para su funcionamiento. Ahora se procederá a la puesta en alta disponibilidad de los dos servidores. Las conexiones a ambos servidores ya están balanceadas, pero no están completamente en alta disponibilidad.

Sympa puede trabajar con dos nodos activos y puede procesar correo recibido por uno u otro nodo gracias a su base de datos. Habrá que compartir los siguientes directorios, en este caso, por NFS:

```
/home/sympa/etc
/home/sympa/static_content
/home/sympa/arc
/home/sympa/list_data
/home/sympa/bounce
/home/sympa/spool/digest
/home/sympa/spool/moderation
```

El directorio */home/sympa/spool* será local, excepto los indicados arriba.

Si el Sympa de un nodo se cae, se seguirán recibiendo correo, aunque se quedarán encolados en el MTA (Exim) hasta que Sympa vuelva a funcionar correctamente.

Una vez que se tienen los dos servidores con las carpetas mencionadas compartidas por NFS, se dispondrá de una alta disponibilidad completa para las listas de distribución.

4.4.5.2 Interfaz web

En este apartado se explicará a grandes rasgos la interfaz web de Sympa.
Cuando se entra, aparecerá la pantalla principal con los recuadros de login. Para ver más a fondo esta interfaz, se hará uso del usuario listmaster.

Figura 52 - Sympa: Portada listas

En la portada, se pueden ver los diferentes temas de las listas, las pestañas de las acciones que se pueden realizar. A la izquierda las listas a las que se está suscrito y/o es propietario el usuario.

Al ser listmaster, aparece una pestaña "Admin Sympa". En ella se pueden aceptar listas que estén a la espera de creación, o denegarlas, administrar usuarios, personalizar la interfaz, etc.

Figura 53 - Sympa: Administarción

A la hora de crear una lista, hay numerosas opciones: lista privada, lista pública, moderadas o no, con autorizados… Esta elección será del creador de la lista, dependiendo si quiere que la lista sea vista por todos los usuarios o sólo los suscriptores, si quiere moderar el envío de correo o no…

Figura 54 - Sympa: Crear lista

Para la creación de listas dinámicas, hay que realizar algunos pasos adicionales. Habría que entrar al fichero propio de configuración de la lista en cuestión y añadirle que la fuente de datos sea una Oracle o LDAP, realizando la consulta correspondiente.

Una vez que se tiene una lista creada, el propietario de la misma puede administrar la configuración de la misma para editar cómo se envía y recibe, los suscriptores, visualización de errores relativos a la lista, visualización de logs (sin tener que acceder al propio servidor)…

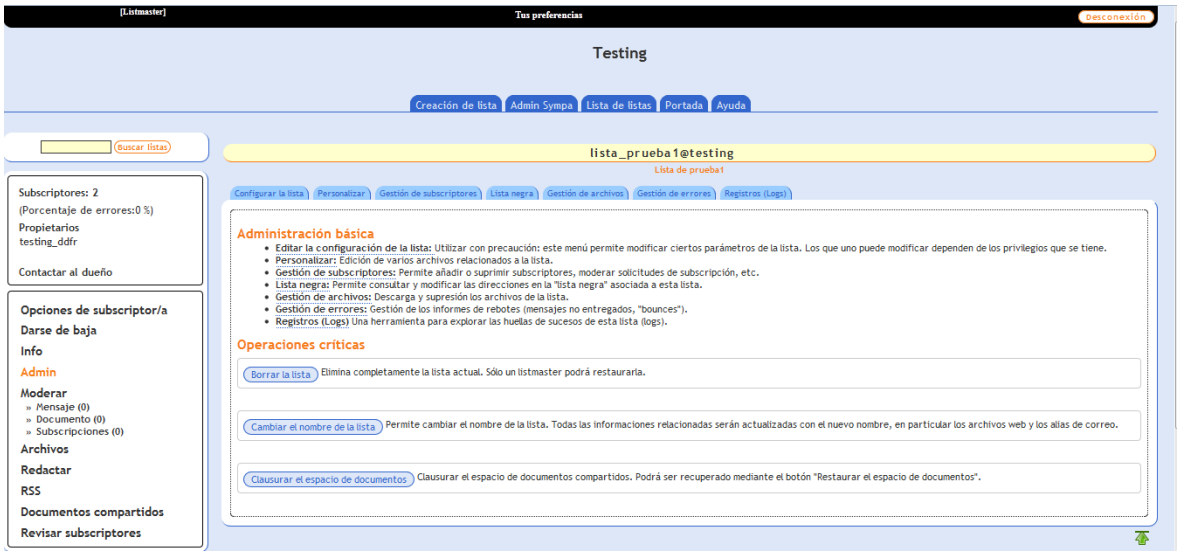

Figura 55 - Sympa: Opciones de lista

Existen guías bastante extensas del funcionamiento completo de esta herramienta, así pues, un uso completo de Sympa no se detallará en el presente PFC. Se han presentado las principales características, así como las capturas correspondientes.

4.4.6 POSTFIX

El MTA para las estafetas de correo saliente será Postfix. La instalación puede ser llevada a cabo mediante el gestor de paquetes de la distribución de Linux en la que se instale, o descargando los fichero fuente y compilarlos e instalarlos.

En el presente proyecto, se descargarán los fuentes, se configurará la instalación para que Postfix haga uso de ciertas librerías y opciones, y se compilará e instalará.

En primer lugar, se decargaran y se descomprimen los archivos fuente:

```
# wget http://de.postfix.org/ftpmirror/official/postfix-2.8.1.tar.gz
# tar zxvf postfix-2.8.1.tar.gz
# cd postfix-2.8.1
```

A continuación, simplemente será configurar la instalación con las opciones que se van a emplear de Postfix (http://www.postfix.org/INSTALL.html). En este caso, se van a necesitar librerías de SSL y TLS para envíos cifrados, y librerías de LDAP para las consultas de usuarios válidos:

```
# make makefiles CCARGS="-DUSE_SASL_AUTH -DUSE_TLS -DHAS_LDAP -I/usr/include -
I/usr/include/sasl" AUXLIBS="-L/usr/lib64 -lsasl2 -lssl -lcrypto -lldap -llber"
```

Por último, simplemente hay que compilar e instalar:

```
# make
# make install
```

El directorio por defecto en el que se instalará esta herramienta es */etc/postfix*. En este directorio se encuentran todos los ficheros de configuración de los que hará uso Postfix. Como este MTA tiene muchas configuraciones posibles, se comentarán las más importantes y, en el ANEXO F, se encontrará la configuración al completo.

Postfix cuenta con dos archivos de configuración principales, *main.cf* y *master.cf*. En el primero se encuentran las opciones de envío de la aplicación, así como las distintas retricciones. En el segundo se definen cómo se enviarán los correos y los puertos adicionales de los que vaya a hacer uso.

Primero, se definirán los parámetros del propio servidor, como el nombre, configuraciones de usuarios válidos (sólo mandarán usuarios internos a la plataforma), la estafeta a la que enviar en último caso (por defecto) y los dominios considerados locales:

```
myorigin = estafeta.correo.es

recipient_canonical_maps = hash:/etc/postfix/recipient_canonical
sender_canonical_maps = hash:/etc/postfix/sender_canonical

myhostname = estafeta.correo.es

mydomain = estafeta.correo.es

mydestination = /etc/postfix/dominiosLocales

local_recipient_maps = ldap:/etc/postfix/validUser.cf $alias_maps

local_transport = smtp:[192.168.100.203]:25

unknown_local_recipient_reject_code = 550

mynetworks_style = subnet

mynetworks = 127.0.0.0/8

relayhost=[ironport.correo.es]
```

Los ficheros de *recipient_canonical* y *sender_canonical* continen mapeos de alias, para los campos TO y FROM respectivamente. Por ejemplo:

```
root@estafeta.correo.es                    postmaster@correo.es
```

Ahora se habilitará el envío autenticado SASL:

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
broken_sasl_auth_clients = yes
```

Además, se configurará para el uso de comunicaciones cifradas (puerto 465 - SMTPS):

```
smtpd_use_tls = yes
smtp_tls_security_level = may
smtp_tls_loglevel = 1
smtpd_tls_key_file = /certificados/estafetas_nopass.pem
smtpd_tls_cert_file = /certificados/estafetas.crt
smtpd_tls_CAfile = /certificados/TERENASSLCA.crt
tls_random_source = dev:/dev/urandom
smtpd_timeout = 300s
```

```
smtpd_recipient_limit = 100
smtpd_recipient_overshoot_limit = 100
data_directory = /var/lib/postfix
inet_protocols = ipv4
```

A continuación, se va a definir los diferentes *transport* a mandar según encuentre al usuario en el LDAP, o un cierto campo:

```
transport_maps            =            ldap:/etc/postfix/ldapListasTransport.cf,
ldap:/etc/postfix/ldapUsuariosLocalesTransport.cf, hash:/etc/postfix/transport
```

Primero mira a ver si se trata de una lista de distribución, luego comprueba que es un usuario y por último, si no ha cumplido ninguna de estas dos condiciones, buscará un *transport* en concreto definido en este fichero. En caso de no cumplir ninguna de estas reglas, si se trata de un usuario externo, lo mandará al *relay* por defecto para salida (los Ironport), pero si se trata de un usuario local, lo enviará al *relay* definido en el campo *local_transport*.

Ahora se van a definir una serie de parámetros para evitar una posible suplantación de identidad a la hora de enviar. De esta manera, el envío deberá ser siempre autenticado para que el sistema pueda verificar la autenticidad del usuario:

```
smtpd_sender_login_maps = ldap:matchlogin

matchlogin_server_host = ldaps://virt_ldap
matchlogin_version = 3
matchlogin_server_port = 636
matchlogin_timeout = 10
matchlogin_bind = yes
matchlogin_search_base = idnc=usuarios,dc=correo,dc=es
matchlogin_bind_dn = cn=mailuser,dc=correo,dc=es
matchlogin_bind_pw = p4ssw0rd

matchlogin_scope = sub
# %s es el mail de origen (mail from)
matchlogin_query_filter = (|(mail=%s)(mailAlternateAddress=%s))
# compara la uid al que pertenece el mail from con el login sasl
matchlogin_result_attribute = uid
```

Por último, se van a declarar las diferentes restricciones en el envío del correo electrónico, cada una se comprobará en las diferentes fases del envío (conexión, comprobación del FROM, comprobación del TO, envío)

```
smtpd_client_restrictions   =   check_client_access   hash:/etc/postfix/emisores-
prohibidos

smtpd_sender_restrictions   =   check_sender_access   hash:/etc/postfix/emisores-
prohibidos

smtpd_recipient_restrictions = reject_unauth_pipelining,
                               reject_non_fqdn_sender,
                               reject_non_fqdn_recipient,
                               reject_unknown_sender_domain,
                               reject_unknown_recipient_domain,
                               permit_mynetworks,
                               reject_sender_login_mismatch,
                               permit_sasl_authenticated,
                               reject_unauth_destination
```

El fichero de *emisores-prohibidos* es como una lista negra (o blanca, depende de cómo se configure), en la que se definen ciertas direcciones de correo electrónico, dominios o direcciones IP para que directamente se rechacen (o acepten, dependerá del parámetro que le siga, ACCEPT o REJECT).

Ahora se pasará a la configuración del fichero *master.cf*, aunque prácticamente funciona correctamente con la configuración predeterminada.

Principalmente, se van a habilitar los dos tipos de envío seguros: TLS y SUBMISSION.

```
submission inet n       -       n       -       -       smtpd
        -o smtpd_tls_security_level=encrypt
        -o smtpd_sasl_auth_enable=yes

smtps     inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
```

En el caso de que se haga uso de un sistema anti-SPAM o anti-virus dentro de la estafeta, es en este fichero donde se definirá cómo funcionará y por qué puertos.

De este modo, se tendría instalada y configurada una estafeta de correo, en la que sólo los usuarios autenticados y con alias válido pueden enviar correo electrónico.

Los ficheros de configuración se encuentran en el anexo POSTFIX.

4.4.7 MySQL

La instalación de la MySQL, aplicativo que almacenará y gestionará las bases de datos de la plataforma, se realizará mediante el gestor de paquetes de la distribución de Linux, en este caso, Scientific Linux.

```
# yum install mysql mysql-server
```

Una vez que se tenga instalada, hay que configurar la contraseña para el usuario de *root*, ya que está en blanco y es un fallo de seguridad que el usuario administrador de las bases de datos no tenga contraseña:

```
# mysqladmin -u root password NEWPASSWORD
```

Ahora, para entrar en las bases de datos, hay que introducir lo siguiente:

```
# mysql -uroot -p
```

El campo de contraseña es recomendable dejarlo en blanco para introducirlo cuando se solicite. Si se introdujese en el comando, se quedaría grabado en el historial de comandos del sevidor.

El fichero de configuración se puede consultar en el anexo MySQL.

Por último, hay que tener en cuenta que habrá que crear todas las bases de datos y los usuarios con privilegios para ellas para cada una de las aplicaciones que hagan uso de la MySQL.

Esto se puede realizar de la siguiente manera:

```
mysql> create database base_datos;
mysql> create user usuario1 identified by ‘CONTRASEÑA_USUARIO1’;
mysql>   grant   all   on   base_datos.*   to   'usuario1'@'%'   identified   by
'CONTRASEÑA_USUARIO1';
```

4.4.7.1 Replicación de MySQL

Antes de empezar, hay que crear el usuario que se encargará de la replicación:

```
mysql> create user replica identified by ‘p4ssw0rd1’;
mysql> grant replication slave on *.* to 'replica'@'%' identified by 'p4ssw0rd1';
mysql> flush privileges;
```

A continuación, una vez que se tengan los dos servidores de MySQL instalados, y teniendo el balanceo hecho en los switches, simplemente habrá que configurar ambos en Maestro / Esclavo. Lo que se llevará a cabo es una configuración Maestro / Maestro, es decir, cada uno será Maestro y Esclavo del otro. De esta forma, si se cayese el servidor que está sirviendo como Maestro, no habrá que retomar la replicación manualmente.

Para ello, lo primero será configurar lo siguiente en cada nodo, en el archivo de configuración *my.cnf*:

```
#skip-slave-start

master-host=bbddX
master-user=replica
master-password=p4ssw0rd1
master-port=3306
```

Es importante definir que no inicie como esclavo, ya que ambos serán maestros. El parámetro *bbddX*, definirá el Maestro/Esclavo del que se hará réplica. No se especificará ninguna base de datos en concreto para que replique todas.

Una vez que ambos nodos están configurados para ser réplica del otro, de procederá a hacer que sean Maestro / Maestro.

Primero, se configurará un nodo esclavo del otro. Para ello se iniciará la aplicación de MySQL y se reiniciará el proceso esclavo de la misma:

```
mysql> stop slave;
mysql> reset slave;
mysql> start slave;
```

En estos momentos se tendría una configuración Maestro / Esclavo. A continuación, se configurará el otro nodo para que sea al mismo tiempo Esclavo del primero.

Los pasos a realizar son similares, salvo que al tener ya un servidor como primario, hay que establecer que va a ser maestro del primero. Ahora se necesitarán dos datos: el fichero de *bin* que se replicará y la posición:

```
mysql> show master status;
+------------------+----------+--------------+------------------+
```

```
| File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+------------------+----------+--------------+------------------+
| mysql-bin.000064 |  1087432 |              |                  |
+------------------+----------+--------------+------------------+
```

Ahora se procederá:

```
mysql> stop slave;
mysql> reset slave;
mysql>    change    master    to    master_host='bbdd2',    master_user='replica',
master_password='p4ssw0rd1',master_log_file='mysql-bin.000064',
master_log_pos=1087432;
mysql> start slave;
```

Ya se tendrían los servidores balanceados en los switches y con configuración Maestro / Maestro. En el apartado 5.7 se observarán los resultados y pruebas de que la replicación está correcta.

4.4.8 OpenLDAP

Los servidores de Bases de Datos (*bbddX*) también tienen instalados unos servidores LDAP, que serán réplicas de un maestro. El presente proyecto se va a centrar en estas réplicas, y no en el servidor maestro.

En primer lugar, hay que instalar el servidor OpenLDAP, con las bibliotecas de desarrollo para poder hacer uso de comandos mediante CLI.

```
# yum install openldap openldap-devel openldap-servers openldap-clients
```

Ahora se va a configurar para que tenga las opciones correctas. Se definirá el tipo de base de datos, el sufijo principal y el usuario administrador del servidor LDAP:

```
database        bdb
suffix          "dc=correo,dc=es"
rootdn          "cn=Replication,dc=correo,dc=es"
rootpw          p4ssw0rd2
```

Otro aspecto básico es que, al ser réplicas, hay que definir de dónde se actualizarán los datos:

```
updatedn "cn=Replication,dc=correo,dc=es"
updateref ldaps://ldap_maestro:636
idletimeout 660
```

El fichero de configuración más detallado se encuenta en el anexo OpenLDAP.

Al tratarse de consultas mediante conexión segura (LDAPS), se necesitarán certificados. Una vez que se obtenga uno desde el maestro, habrá que configurar el fichero */etc/openldap/ldap.con* para que sepa que cómo hay que conectar:

```
TLS_CACERT /etc/openldap/ssl/cacert.pem
```

A continuación, se facilitará desde el servidor maestro los esquemas del LDAP para poder cargar toda la información antes de empezar a replicar. Para ello, se obtendrán mediante

copia directa todos los archivos .schema que tendrán definidos todos los campos posibles y los tipos de campos. Estos archivos se copiarán en */etc/openldap/schema*.

Ahora, para obtener la información del servidor LDAP maestro, se ejecuta el siguiente comando desde la consola (es posible que este proceso tarde un poco, dependiendo de la cantidad de datos alojados):

```
# /var/sbin/slapcat -b "dc=correo,dc=es" -l /tmp/ldap_backup-`date +%d-%b-%Y`.ldif
```

Esto creará un fichero .ldif con toda la información del LDAP. Ahora, simplemente habrá que cargarlo en los servidores. Antes de nada hay que parar el servicio:

```
# /etc/init.d/ldap stop
```

Ahora, si se quisiera hacer una instalación limpia de todos los datos, habría que eliminar muchos ficheros de la carpeta */var/lib/ldap*:

```
# rm *.* /var/lib/ldap/
```

Por último, simplemente habría que cargar el fichero .ldif creado anteriormente:

```
# slapadd -l /tmp/ldap_backup-XX-xxx-201X.ldif
```

Simplemente se inicia el servicio, y, una vez realizado esto en los dos servidores, se tendrían las dos réplicas de LDAP funcionando correctamente y balanceadas en carga por los switches.

5 Integración y pruebas

5.1 DOVECOT

5.1.1 Envío y recepción de correo

La entrega se realiza correctamente. Se entrega el correo a dovecot que aplica el plugin de cuota, aviso de superación de límite de cuota y los filtros si los tiene, en este caso no. Finalmente se entrega el correo en la bandeja de entrada.

```
Apr  6 14:05:27 buzon dovecot: lda: Debug: Loading modules from directory:
/usr/local/dovecot/lib/dovecot
Apr  6 14:05:27 buzon dovecot: lda: Debug: Module loaded:
/usr/local/dovecot/lib/dovecot/lib10_quota_plugin.so
Apr  6 14:05:27 buzon dovecot: lda: Debug: Module loaded:
/usr/local/dovecot/lib/dovecot/lib90_sieve_plugin.so
Apr  6 14:05:27 buzon dovecot: lda: Debug: auth input: pruebas@correo.es
quota_rule=*:bytes=3145728000 home=/buzones/buzon5/601995
Apr  6 14:05:27 buzon dovecot: lda: Debug: Added userdb setting:
plugin/quota_rule=*:bytes=3145728000
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Effective uid=501,
gid=501, home=/buzones/buzon5/601995
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Quota root: name=
backend=maildir args=
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Quota rule: root=
mailbox=* bytes=3145728000 messages=0
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Quota warning:
bytes=2359296000 (75%) messages=0 reverse=no
command=/usr/local/dovecot/bin/quota-warning.sh 75
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Quota warning:
bytes=2831155200 (90%) messages=0 reverse=no
command=/usr/local/dovecot/bin/quota-warning.sh 90
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Namespace :
type=private, prefix=INBOX., sep=., inbox=yes, hidden=no, list=yes,
subscriptions=yes location=maildir:/buzones/buzon5/601995/Maildir
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: maildir++:
root=/buzones/buzon5/601995/Maildir, index=, control=,
inbox=/buzones/buzon5/601995/Maildir
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Quota root: name=
backend=maildir args=
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Quota warning:
bytes=0 (75%) messages=0 reverse=no command=/usr/local/dovecot/bin/quota-
warning.sh 75
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: Quota warning:
bytes=0 (90%) messages=0 reverse=no command=/usr/local/dovecot/bin/quota-
warning.sh 90
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: none: root=,
index=, control=, inbox=
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: using sieve
path for user's script: /buzones/ buzon5/601995/.dovecot.sieve
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: opening
script /buzones/buzon5/601995/.dovecot.sieve
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: script
binary /buzones/buzon5/601995/.dovecot.svbin successfully loaded
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: binary save:
not saving binary /buzones/buzon5/601995/.dovecot.svbin, because it is already
stored
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: executing
script from /buzones/buzon5/601995/.dovecot.svbin
Apr  6 14:05:27 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<7686.0003.0000@estafeta.correo.es>: stored mail into mailbox 'INBOX'
```

A partir de ahora se mostrarán los logs genéricos, sin la opción de depuración activada, es decir, *mail_debug = no*. Esto se hará para no sobrecargar el documento. Si en algunas otras trazas se observa la opción *Debug* es porque con el modo normal de depuración no aparece lo que se quiere mostrar.

5.1.2 Comprobación de avisos de cuota

Se comprueba que se envía un correo al usuario cuando se rebasan los límites de 75% y 90% de la cuota. Cabe destacar que estos mensajes sólo se envían en el momento que el usuario rebase la cuota. Estos mensajes de aviso no son enviados a Exim, sino que Dovecot los entrega directamente al buzón de usuario.

De 75%:

```
Apr  7 17:36:24 buzon dovecot: lda(pruebas@correo.es): Debug: quota: Executing
warning: quota-warning 75 pruebas@correo.es
Apr  7 17:36:24 buzon dovecot: lda(pruebas@correo.es): sieve: msgid=unspecified:
stored mail into mailbox 'INBOX'
```

De 90%:

```
Apr  7 17:52:49 buzon dovecot: lda(pruebas@correo.es): Debug: quota: Executing
warning: quota-warning 90 pruebas@correo.es
Apr  7 17:52:49 buzon dovecot: lda(pruebas@correo.es): sieve: msgid=unspecified:
stored mail into mailbox 'INBOX'
```

Cuando el buzón está lleno, o el mensaje que llega no cabe en el mismo, se rechaza y se envía un correo al usuario:

```
Apr  7 17:16:10 buzon dovecot: lda(pruebas@correo.es): Error: sieve:
msgid=<22ce.0003.0000@estafeta.correo.es>: failed to store into mailbox 'INBOX':
Quota exceeded (mailbox for user is full)
Apr  7 17:16:10 buzon dovecot: lda(pruebas@correo.es): Error: sieve: script
/buzones/buzon5/601995/.dovecot.sieve failed with unsuccessful implicit keep
(user logfile /buzones/buzon5/601995/.dovecot.sieve.log may reveal additional
details)
Apr  7 17:16:10 buzon dovecot: lda(pruebas@correo.es):
msgid=<22ce.0003.0000@estafeta.correo.es>: rejected: Quota exceeded (mailbox for
user is full)
Apr  7 17:16:10 buzon dovecot: lda(pruebas@correo.es): sieve: msgid=<dovecot-
1302189370-283913-0@correo.es>: stored mail into mailbox 'INBOX'
```

En los logs de Exim se registra lo siguiente:

- La llegada del correo.
- El mensaje generado automáticamente por dovecot.
- Intento de envío de un mensaje al propio usuario con la cuota excedida.

```
2013-04-07 17:16:10 1Q7qwL-0000Ot-NK <= pruebas@correo.es H=(estafeta)
[161.111.83.31] P=esmtp S=7872430 id=22ce.0003.0000@estafeta.correo.es
2013-04-07 17:16:10 1Q7qwM-0000PF-Cn <= <> U=vmail P=local S=1849 id=dovecot-
1302189370-283913-0@correo.es
2013-04-07 17:16:10 1Q7qwL-0000Ot-NK => pruebas <pruebas@correo.es> R=ldapuser
T=ldap_delivery_dovecot
```

```
2013-04-07 17:16:10 1Q7qwL-0000Ot-NK Completed
2013-04-07 17:16:10 1Q7qwM-0000PF-Cn => pruebas <pruebas@correo.es> R=ldapuser
T=ldap_delivery_dovecot
2013-04-07 17:16:10 1Q7qwM-0000PF-Cn Completed
```

Los logs y los correos muestran que las cuotas funcionan correctamente.

5.1.3 Pruebas de entrega con filtros

Si el usuario tiene activado algún filtro, el plugin de dovecot *sieve* se encargará de realizar las acciones oportunas que dicho usuario haya definido.

5.1.3.1 Filtro Vacation

Filtro usado:

```
require ["vacation", "regex", "fileinto"];

# Ausencia
if allof ( not exists ["list-help", "list-unsubscribe", "list-subscribe", "list-
owner", "list-post", "list-archive", "list-id", "Mailing-List"], not header
:comparator "i;ascii-casemap" :is "Precedence" ["list", "bulk", "junk"], not
header :comparator "i;ascii-casemap" :matches "To" "Multiple recipients of*" ) {
    vacation :days 7 :addresses "pruebas@correo.es" :subject "Prueba vacaciones"
"Hola, estoy de vacaciones.";
}
```

Ahora se evaluarán distintos casos que se pueden dar.

5.1.3.1.1 Respuesta de vacaciones a un usuario

El correo de vacaciones se manda al usuario que intenta enviar un correo a la vez que se almacena el enviado a usuario ausente.

```
Apr  7 18:24:26 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2983.0003.0000@estafeta.correo.es>: sent vacation response to
<usympa2@correo.es>
Apr  7 18:24:26 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2983.0003.0000@estafeta.correo.es>: stored mail into mailbox 'INBOX'
Apr  7 18:24:26 buzon dovecot: lda(usympa2@correo.es): msgid=<dovecot-sieve-
1302193466-519812-0@correo.es>: saved mail to INBOX
```

5.1.3.1.2 Usuario que ya había mandado un correo

Este caso se da cuando un usuario ya ha recibido un correo de aviso de que otro usuario está de vacaciones, y, por tanto, no se envía de nuevo este aviso.

```
Apr  7 18:30:19 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2a37.0003.0000@estafeta.correo.es>: discarded duplicate vacation response
to <usympa2@correo.es>
Apr  7 18:30:19 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2a37.0003.0000@estafeta.correo.es>: stored mail into mailbox 'INBOX'
```

5.1.3.1.3 Es el propio usuario el que se ha mandado el correo

En este caso, es el propio usuario el que se ha mandado el correo, por tanto, no se le envía el aviso de vacaciones.

```
Apr  7 18:31:33 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2a4d.0003.0000@estafeta.correo.es>: discarded vacation reply to own
address
Apr  7 18:31:33 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2a4d.0003.0000@estafeta.correo.es>: stored mail into mailbox 'INBOX'
```

5.1.3.1.4 Usuario de sistema

Si es un usuario del sistema, no se le envía el correo de aviso de ausencia:

```
Apr  7 18:34:22 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2a86.0003.0000@estafeta.correo.es>: not sending vacation response to
system address <sympa6-request@listas.correo.es>
Apr  7 18:34:22 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2a86.0003.0000@estafeta.correo.es>: stored mail into mailbox 'INBOX'
```

5.1.3.2 Otros Filtros

Se ha definido un filtro de la siguiente manera:

```
require "fileinto";

# Nueva regla
if header :comparator "i;ascii-casemap" :contains "Subject" "prueba"  {
    fileinto "INBOX.carpeta2";
    stop;
}
```

En las siguientes trazas se observa el funcionamiento correcto del filtro:

```
Apr  7 18:41:38 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: using sieve
path for user's script: /buzones/j/601995/.dovecot.sieve
Apr  7 18:41:38 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: opening
script /buzones/j/601995/.dovecot.sieve
Apr  7 18:41:38 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: script
binary /buzones/j/601995/.dovecot.svbin successfully loaded
Apr  7 18:41:38 buzon dovecot: lda(pruebas@correo.es): Debug: sieve: executing
script from /buzones/j/601995/.dovecot.svbin
Apr  7 18:41:39 buzon dovecot: lda(pruebas@correo.es): sieve:
msgid=<2b4a.0003.0000@estafeta.correo.es>: stored mail into mailbox
'INBOX.carpeta2'
```

5.2 EXIM

5.2.1 Envío normal de un correo

Exim trata rápidamente los correos, sin llegar a encolarse. En caso de que hubiese correos encolados, seguramente es que ha ocurrido algún problema en la plataforma o en la entrega. El comando para ver los correos encolados en Exim es: `# exim -bp`

Aquí la entrega normal de un correo local y otro externo:

```
2013-04-10       14:04:04       1VJMfs-0003IG-Ml       <=       usuario1@correo.es
H=(ironport6.correo.es)          [161.111.10.134]          P=esmtp          S=1595
id=1569344449.522F0ABE@smtpin.correo.es
2013-04-10 14:04:04 1VJMfs-0003IG-Ml => usuario2 <usuario2@correo.es> R=ldapuser
T=ldap_delivery_dovecot
2013-04-10 14:04:04 1VJMfs-0003IG-Ml Completed

…
```

```
2013-04-10 14:10:55 1VJMmV-0003xO-P5 <= usuario1@correo.es U=vmail P=local S=1050
id=dovecot-sieve-1378815055-685909-0@buzon.correo.es
2013-04-10     14:10:55     1VJMmV-0003xO-P5     =>     usuario_ext@dominio.ext.es
R=send_to_gateway T=remote_smtp H=virt_smtpin [192.168.100.202]
2013-04-10 14:10:55 1VJMmV-0003xO-P5 Completed
```

Se observa que para los usuarios locales hace uso del *transport* local y lo entrega al MDA. Y para el usuario externo existente en la lista, lo envía hacia las estafetas para su entrega al exterior.

5.2.2 Envío a una lista de distribución

Cuando se produce el envío a una lista de distribución, Exim entregará el correo electrónico a los servidores de listas:

```
2013-04-10     21:49:30     1VJTwI-0006LN-LV     <=     usuario.pruebas@correo.es
H=(ironport.correo.es)          [161.111.10.143]          P=esmtp          S=10950
id=F1B425E78E9F3E45957A42DB5AC329554C32E4@evscr04.correo.es
2013-04-10      21:49:30      1VJTwI-0006LN-LV      =>      lista_prueba@correo.es
R=ldap_list_buzones T=remote_smtp H=virt_listas_smtp [192.168.100.206]
2013-04-10 21:49:30 1VJTwI-0006LN-LV Completed
```

Entonces, este correo lo recibirá el aplicativo de listas de distribución, y, según su política, se entregará a los diferentes usuarios (locales como externos). En el caso de que se entregue, los logs en Exim aparecerán de la siguiente manera:

```
2013-04-10  21:49:30  1VJSBF-0008TM-OY  <=  lista_prueba-owner@correo.es  U=sympa
P=local S=31844 id=522F5D59.8030306@correo.es
2013-04-10 21:49:30 1VJSBF-0008TM-OY => usuario1 <usuario1@correo.es> R=ldapuser
T=ldap_delivery_dovecot
2013-04-10 21:49:30 1VJSBF-0008TM-OY => usuario2 <usuario2@correo.es> R=ldapuser
T=ldap_delivery_dovecot
2013-04-10 21:49:32 1VJSBF-0008TM-OY => usuario3 <usuario3@correo.es> R=ldapuser
T=ldap_delivery_dovecot
2013-04-10 21:49:32 1VJSBF-0008TM-OY => usuario_ext <usuario_ext@dominio.ext.es>
R=send_to_gateway T=remote_smtp H=virt_smtpin [192.168.100.202]
2013-04-10 21:49:32 1VJSBF-0008TM-OY Completed
```

Se observa que para los usuarios locales hace uso del *transport* local y lo entrega al MDA. Y para el usuario externo existente en la lista, lo envía hacia las estafetas para su entrega al exterior.

Si por algún casual, el siguiente MTA devuelve un error a Exim, aparecería algo como esto:

```
2013-04-10    14:42:44    1VIxWM-00022U-Om    ==    usuario@dominio.noexistente.es
R=send_to_gateway T=remote_smtp defer (-44): SMTP error from remote mail server
after    RCPT    TO:<    usuario@dominio.noexistente.es>:    host    virt_smtpin
[192.168.100.202]: 450 4.1.2 < usuario@dominio.noexistente.es>: Recipient address
rejected: Domain not found
```

Este error se lo devuelve, en este caso, Postfix.

5.3 WEBMAIL – OPEN XCHANGE

Una vez que se tiene el sistema instalado, en este paso ya por completo, se puede probar por completo la solución.

Como el presente proyecto no pretende ser una guía de usuario, se presentarán las principales características de la solución.

Introduciendo la url del servidor en un navegador saltaría la pantalla de login:

Figura 56 - Open-Xchange: Login

Una vez introducidas las credenciales del usuario, en primer lugar se mostrará una pantalla en la que se invita al usuario a rellenar toda la información y/o añadir fuentes de información (este paso se puede omitir y rellenar todos estos parámetros en las opciones de Webmail):

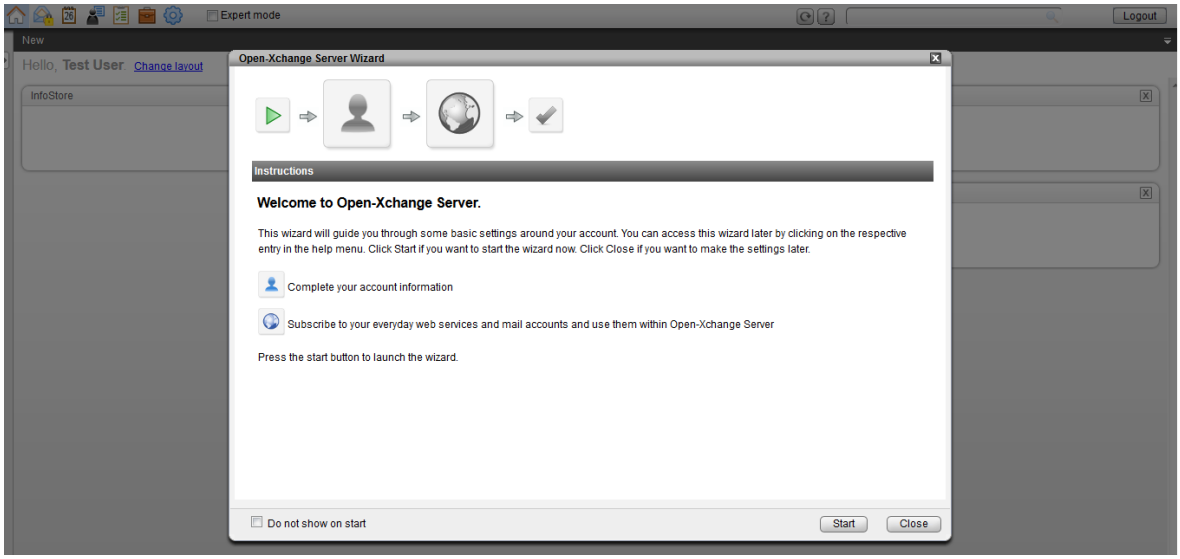

Figura 57 - Open-Xchange: Wizard

A continuación se mostrará una pantalla de resumen de las actividades del usuario en la plataforma, con los últimos correos, eventos del calendario, tareas, ficheros…

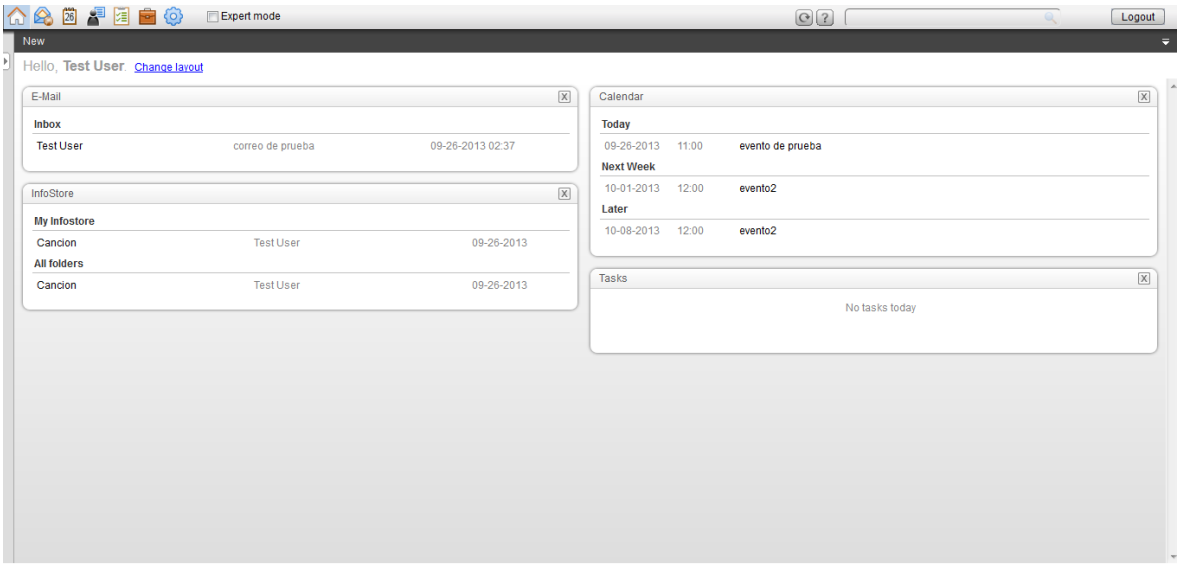

Figura 58 - Open-Xchange: Portal

Para ver los correos, simplemente habrá que seleccionar el icono de un sobre y el usuario irá directamente a las bandejas, donde podrá administrar fácilmente los correos (drag&drop, crear, mover…):

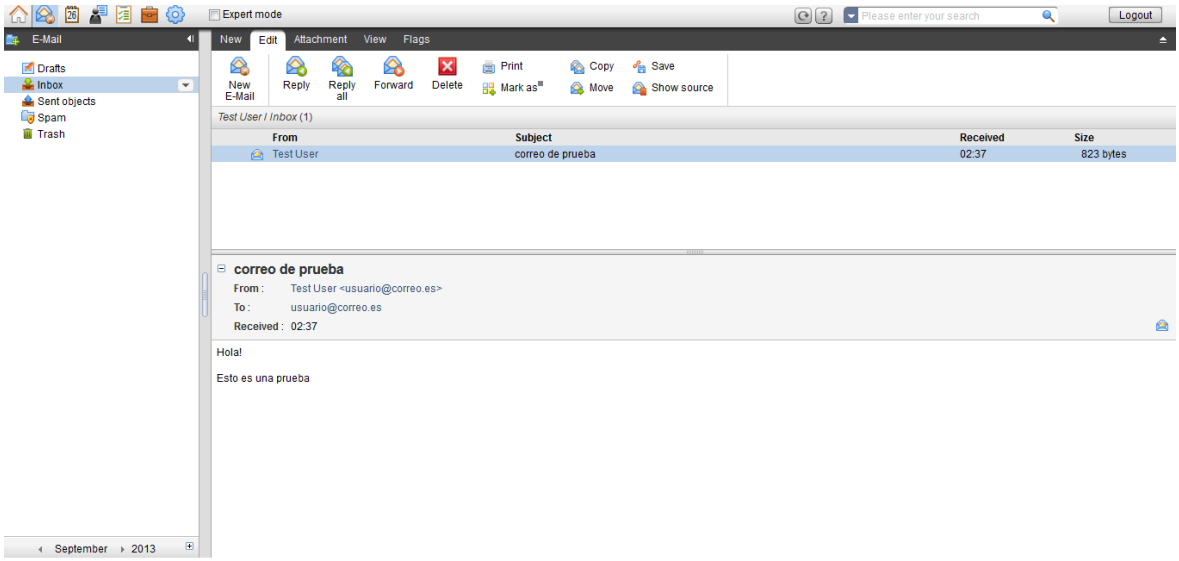

Figura 59 - Open-Xchange: Bandeja Entrada

Para crear un correo, simplemente seleccionar “New E-Mail”:

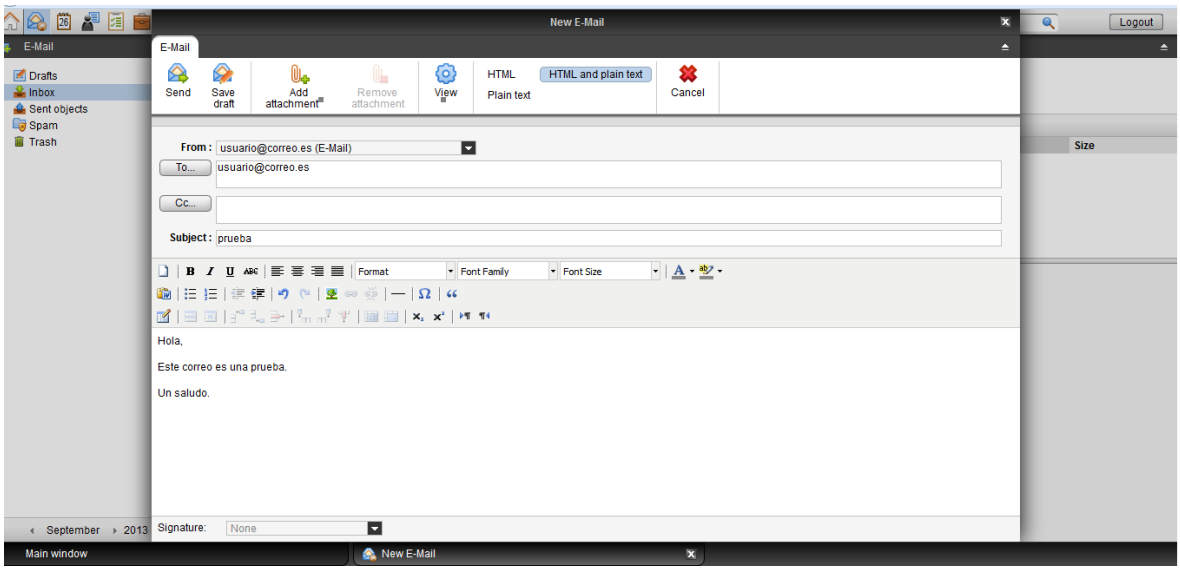

Figura 60 - Open-Xchange: Nuevo correo

La vista del calendario es muy sencilla e intuitiva, fácil para los usuarios:

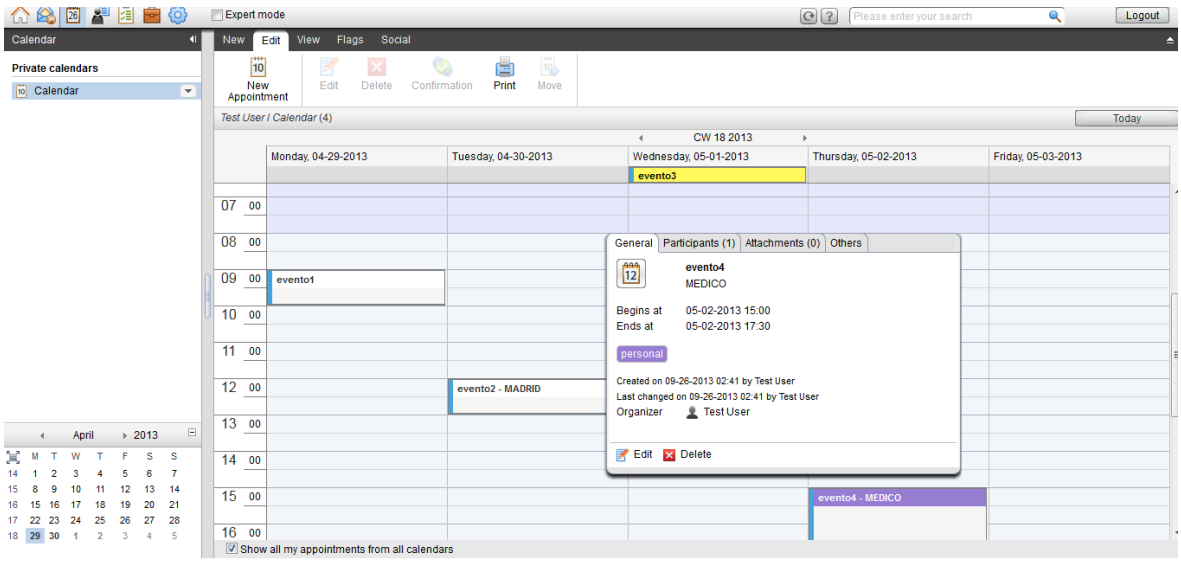

Figura 61 - Open-Xchange: Calendario

Se pueden crear fácilmente eventos en el calendario, seleccionando una hora en concreto de un día, o directamente en Nueva Cita y por defecto la creará en el día actual. En los eventos se puede configurar el lugar, los participantes (ya sean internos buscando en todo el sistema y libretas personales, o externos), recursividad o categorías, entre otros.

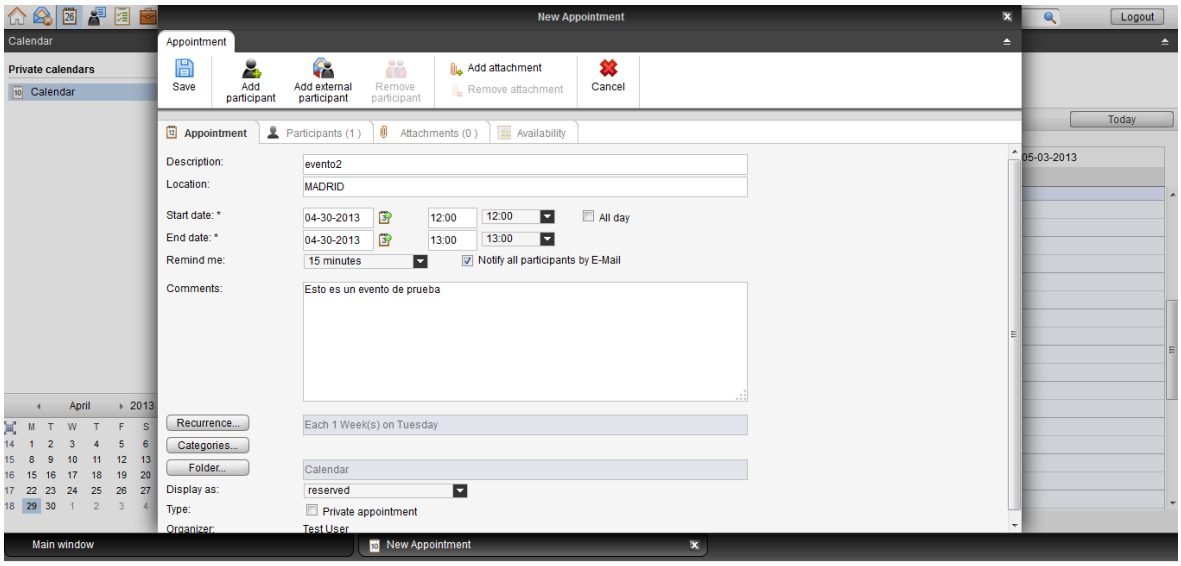

Figura 62 - Open-Xchange: Nuevo evento

La gestión de las tareas es similar al de los eventos del calendario:

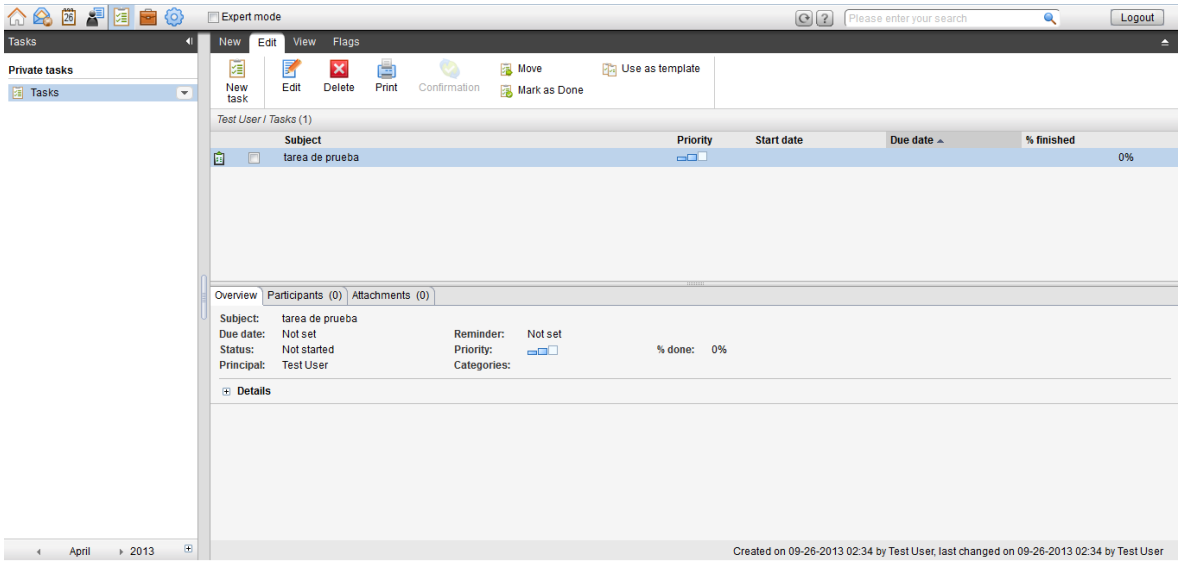

Figura 63 - Open-Xchange: Tareas

Se dispone de un módulo de gestión de ficheros, con el que se pueden subir archivos y compartir con diferentes usuarios, o simplemente como repositorio privado:

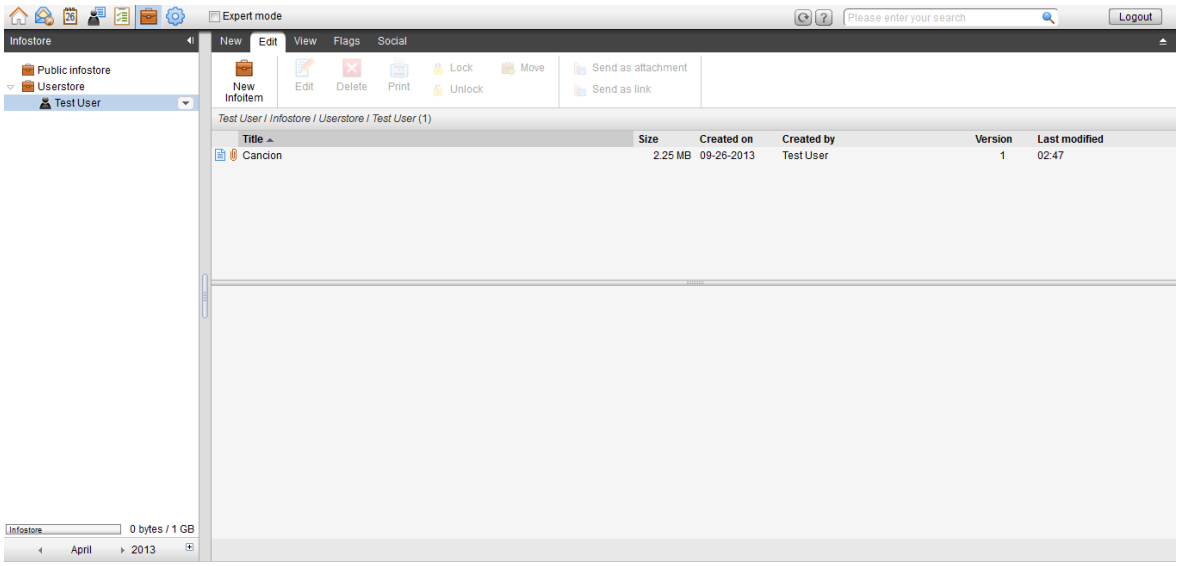

Figura 64 - Open-Xchange: Infostore

En la pantalla de opciones se pueden realizas muchas acciones respecto a todos los módulos de la plataforma. Desde aquí, se puede editar la configuración personal, importar tareas, eventos o contactos, gestionar las categorías, la disposición de la pantalla de inicio, editar las preferencias del calendario, correo, tareas, añadir cuentas de redes sociales… Además, se disponen de plugins de Open-Xchange, los cuales se pueden cargar desde la configuración.

Como se dispone del módulo de filtrado de mensajes mediante Sieve, se ha configurado con Open-Xchange y se pueden gestionar los distintos filtros que se almacenarán en la ruta del usuario en el servidor:

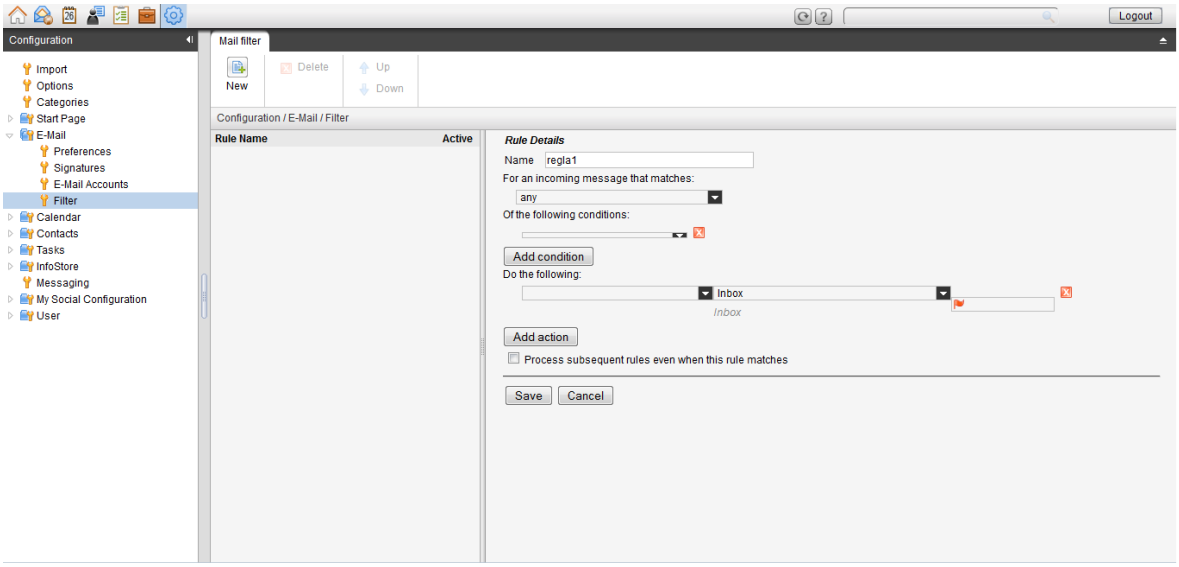

Figura 65 - Open-Xchange: Opciones

5.4 FUNAMBOL

5.4.1 Comprobación de la integración del conector.

En primer lugar, se va a comprobar que la integración de Funambol con el servidor Open-Xchange ha sido la correcta. Para ello, se necesitará la herramienta Funambol Admin Tool, que se podrá instalar en el propio servidor o en un ordenador con acceso a dicho servidor.

Una vez instalada y ejecutada, pedirá los datos para la conexión del servidor:

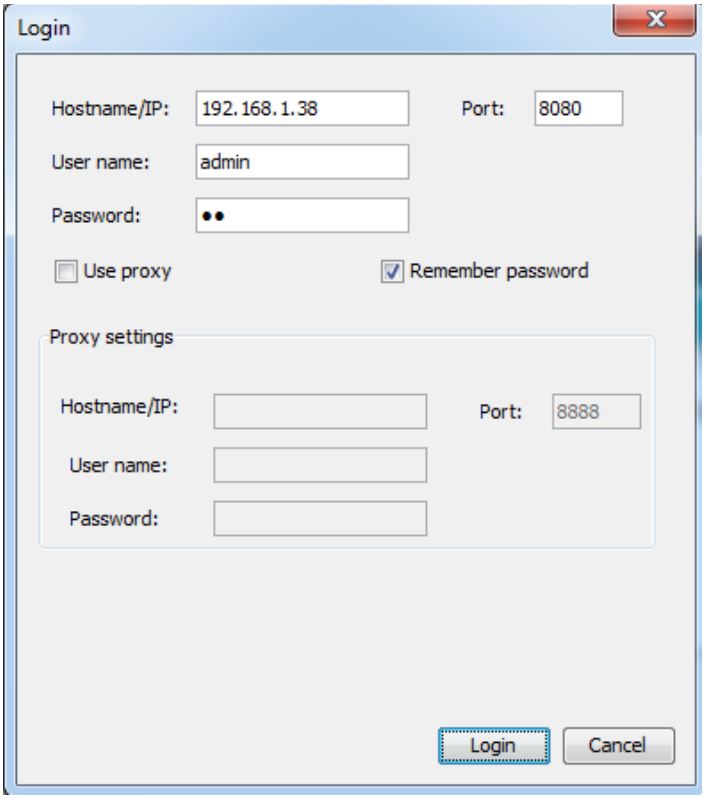

Figura 66 - Funambol: Conexión

Una vez dentro, hay que buscar que exista el módulo *ox*.

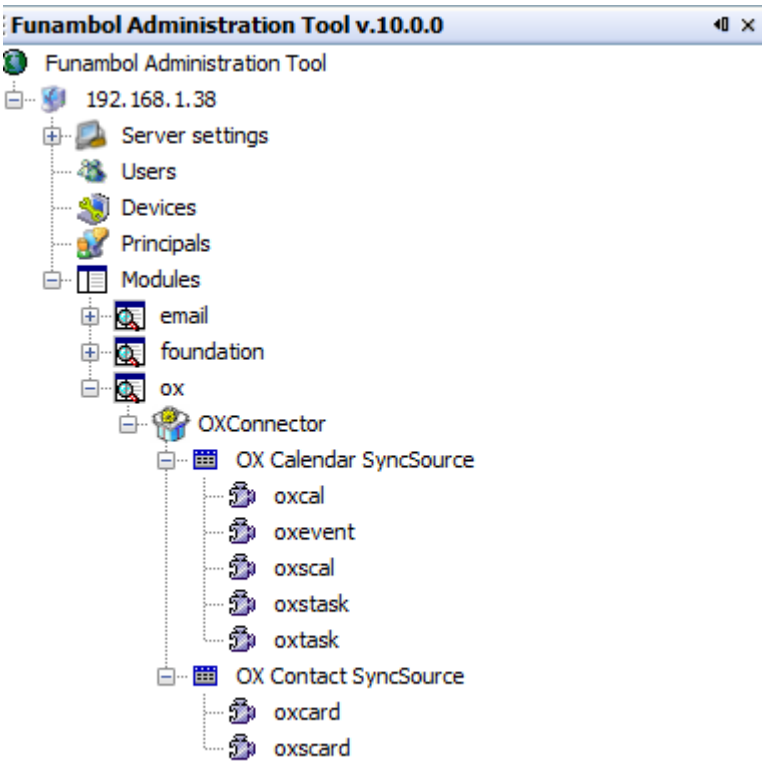

Figura 67 - Funambol: Administración módulos

Por úlitmo, se comprobará que la URL está correctamente definida:

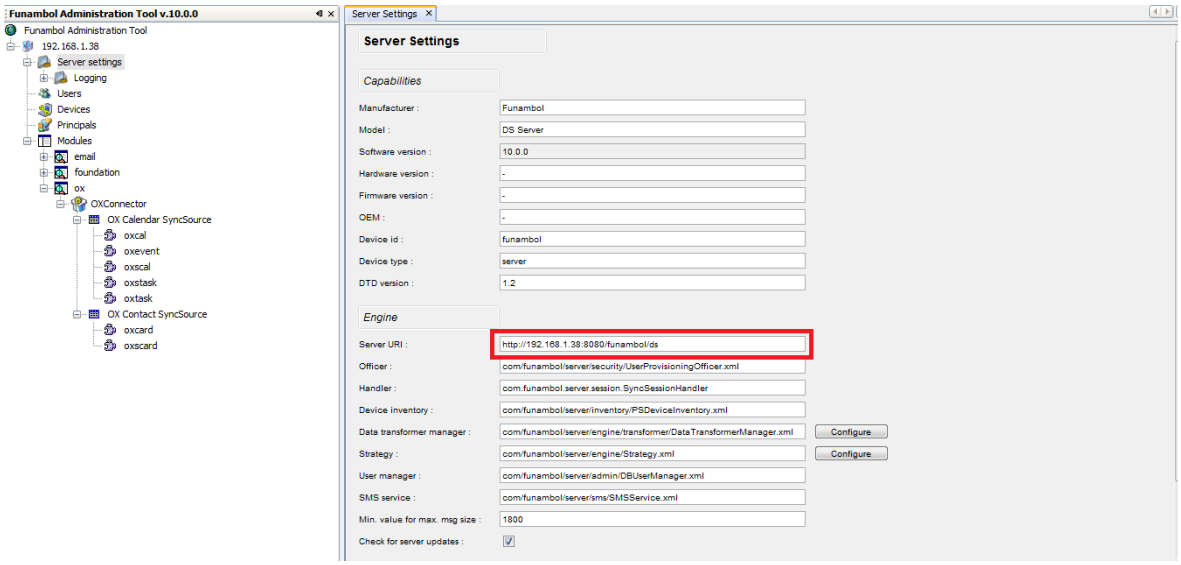

Figura 68 - Funambol: Configuración servidor

5.4.2 Pruebas con sincronización.

Para la sincronización contra un servidor Funambol existen numerosos plugins disponibles para muchos tipos de dispositivos móviles y sistemas operativos http://forge.ow2.org/project/showfiles.php?group_id=96 .

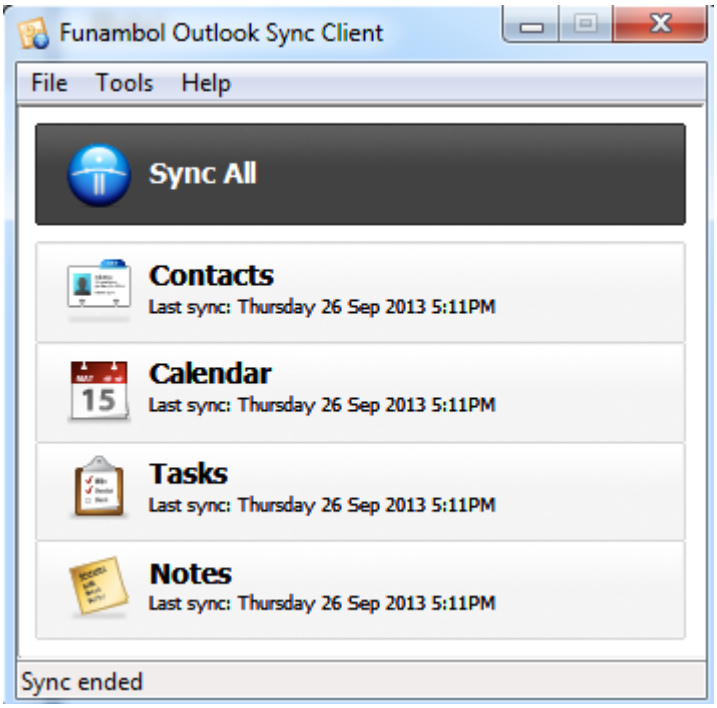

Figura 69 - Funambol: Conector sincronización

Una vez que se haya instalado el plugin, al abrirlo por pimera vez habrá que configurarlo para que tenga los parámetros del servidor.

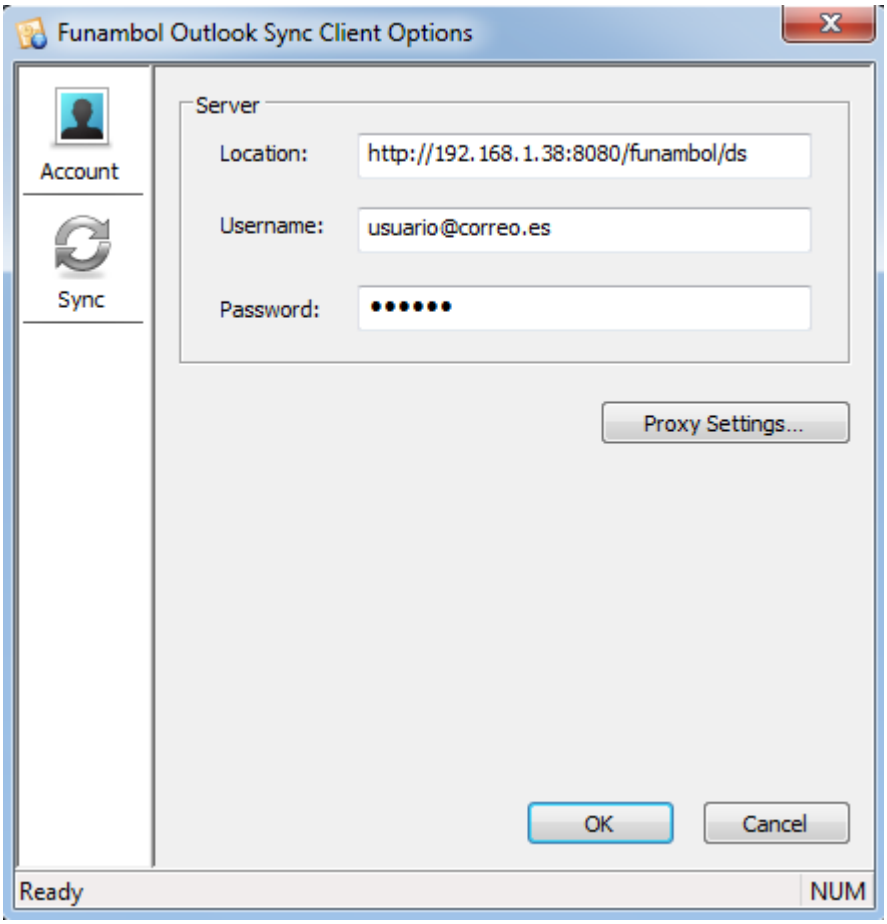

Figura 70 - Funambol: Cuenta conexión

Además, el usuario podrá seleccionar qué datos sincronizar y cómo:

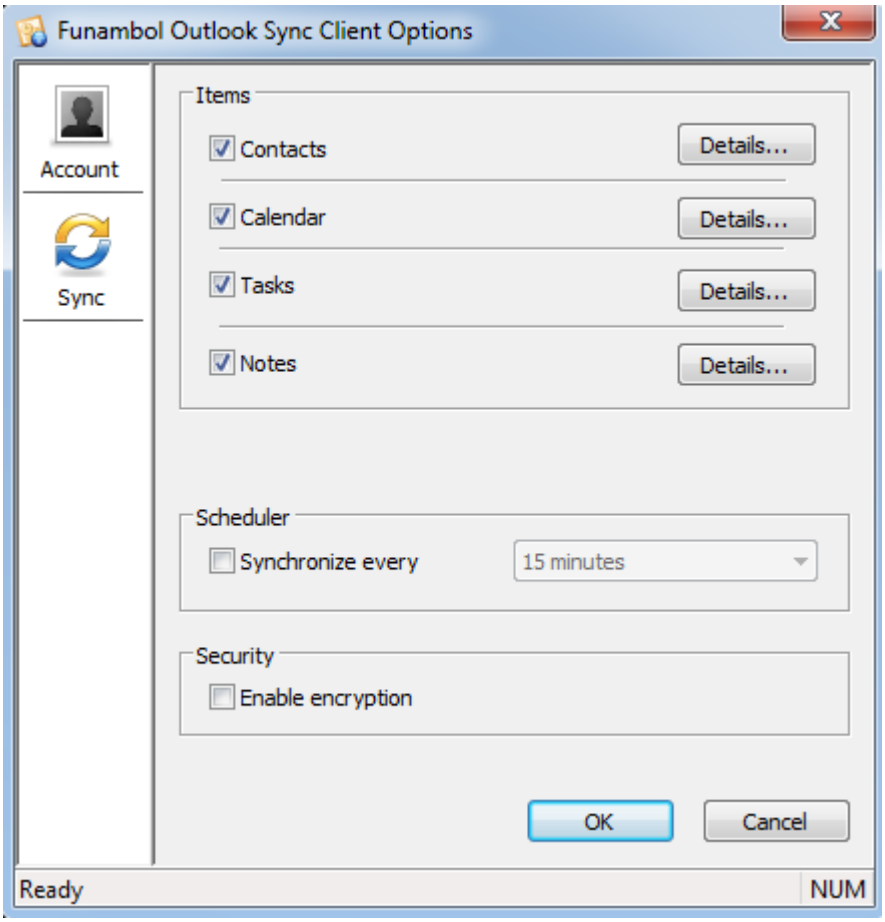

Figura 71 - Funambol: Datos a sincronizar

Después de que se hayan configurado todos los parámetros de conexión y sincronización, el usuario podrá llevar a cabo una sincronización desde la ventana principal del plugin.

Se puede comprobar que la sincronización ha sido correcta, además de porque el usuario vea los datos sincronizados, mediante los ficheros de log del plugin. Por ejemplo:

```
============================================================
================   SYNCHRONIZATION REPORT   ================
============================================================

SYNCHRONIZATION COMPLETED SUCCESSFULLY!
---------------------------------------

Contacts:
---------
    Sync completed successfully!
    Sync type: two-way

             | on Client | on Server
    ---------|-----------|----------
    New      |    1/   1 |    0/   0
    Updated  |    0/   0 |    2/   2
    Deleted  |    1/   1 |    0/   0


Calendar:
---------
```

```
    Sync completed successfully!
    Sync type: two-way

             | on Client | on Server
    ---------|-----------|----------
    New      |   27/  27 |    0/   0
    Updated  |    0/   0 |   12/  12
    Deleted  |    0/   0 |    0/   0


Tasks:
------
    Sync completed successfully!
    Sync type: two-way

             | on Client | on Server
    ---------|-----------|----------
    New      |    1/   1 |    0/   0
    Updated  |    0/   0 |    0/   0
    Deleted  |    0/   0 |    2/   2


Notes:
------
    Sync completed successfully!
    Sync type: two-way

             | on Client | on Server
    ---------|-----------|----------
    New      |    0/   0 |    0/   0
    Updated  |    0/   0 |    0/   0
    Deleted  |    0/   0 |    0/   0
```

Además, desde la herramienta Funambol Admin Tool, se puede observar que los usuarios que van usando esta sincronización van apareciendo en la base de datos:

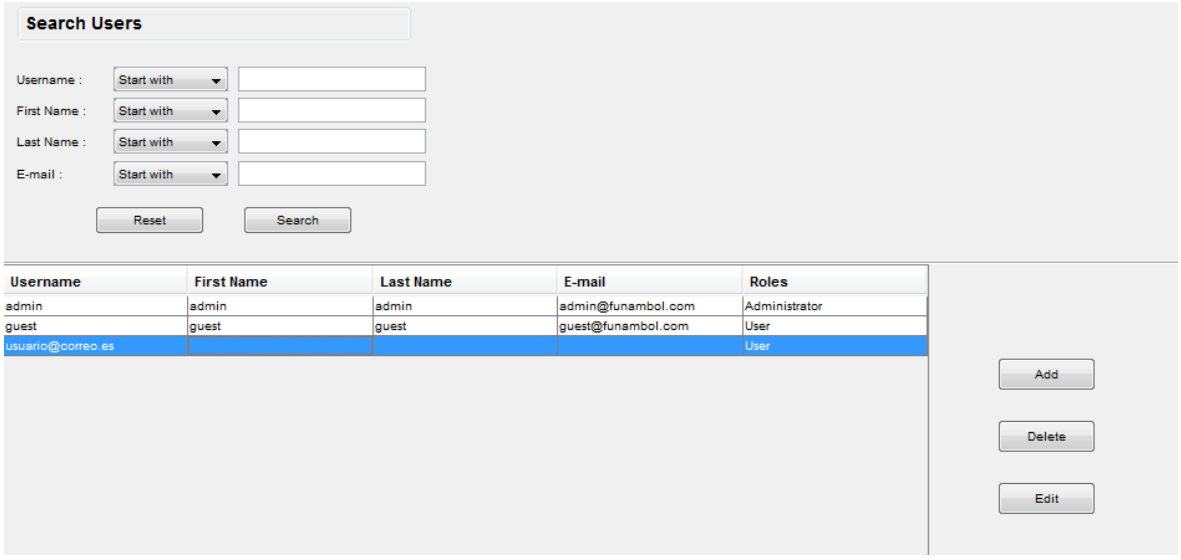

Figura 72 - Funambol: Usuario sincronizado

5.5 SYMPA

Se contemplarán los principales casos de envíos a listas, ya que existen numerosos tipos de listas, así como la posible personalización de esta configuración para una lista en concreto.

5.5.1 Envío a una lista permitida

Caso de envío a una lista de un usuario que está permitido el envío. El mensaje de correo electrónico se distribuirá directamente sin ningún tipo de moderación siempre y cuando el usuario esté autorizado a enviar a esa lista. Esto se puede dar si la lista es abierta a todo el mundo, o si sólo los subscriptores están autorizados y el remitente es uno de ellos.

```
Apr 24 22:55:36 listas sympa[7919]: notice main::DoFile() Processing
/home/sympa/spool/msg/lista_prueba@listas.correo.es.1380056134.23739 ; sender:
=?iso-8859-1?Q?H=E9ctor_Moreno_Blanco?= <hmoreno@gmv.com> ; message-id:
<ADE5C314E6738E4F85E896FF7A8F217119E4C11D@ptmexchange3.gmv.es>
Apr 24 22:55:36 listas sympa[7919]: info main::DoMessage() Processing message for
lista_prueba with priority 5,
<ADE5C314E6738E4F85E896FF7A8F217119E4C11D@ptmexchange3.gmv.es>
Apr 24 22:55:36 listas sympa[7919]: info main::DoMessage() Message for
lista_prueba from hmoreno@gmv.com accepted (0 seconds, 1 sessions, 2
subscribers), message-
id=<ADE5C314E6738E4F85E896FF7A8F217119E4C11D@ptmexchange3.gmv.es> , size=30359
Apr 24 22:55:37 listas bulk[24543]: notice Done sending message
<ADE5C314E6738E4F85E896FF7A8F217119E4C11D@ptmexchange3.gmv.es> to list
lista_prueba@correo.es (priority 5) in 1 seconds since scheduled expedition date.
```

5.5.2 Envío no permitido a una lista

En este caso se enviará a una lista en la que el remitente no tenga permitido el envío. Además de no permitir dicho envío, se notificará a la dirección de correo que ha enviado el correo electrónico con un aviso de autorización denegada:

```
Apr 24 23:02:22 listas sympa[24538]: notice main::DoFile() Processing
/home/sympa/spool/msg/lista_prueba@listas.correo.es.1380056541.23350 ; sender:
=?iso-8859-1?Q?H=E9ctor_Moreno_Blanco?= <hmoreno@gmv.com> ; message-id:
<ADE5C314E6738E4F85E896FF7A8F217119E4C147@ptmexchange3.gmv.es>
Apr 24 23:02:22 listas sympa[24538]: info main::DoMessage() Processing message
for lista_prueba with priority 5,
<ADE5C314E6738E4F85E896FF7A8F217119E4C147@ptmexchange3.gmv.es>
Apr 24 23:02:22 listas sympa[24538]: notice main::DoMessage() Message for l-
prueba-guia from hmoreno@gmv.com rejected() because sender not allowed
Apr 24 23:02:22 listas sympa[24538]: notice Moving bad file
lista_prueba@listas.correo.es.1380056541.23350 to bad/
```

5.5.3 Envío a una lista moderada

A continuación se exponen los dos posibles casos de envío a listas moderadas: que se acepta y se distribuya el correo, o que se rechace. En ambos casos, cuando se mande el correo, se informará al usuario de que su correo será moderado por el moderador o propietario de la lista (no siempre es el mismo).

En primer lugar, el mensaje llegará a los moderadores:

```
Apr 24 23:12:55 listas sympa[24538]: notice main::DoFile() Processing
/home/sympa/spool/msg/lista_prueba@listas.correo.es.1380057174.24783 ; sender:
=?iso-8859-1?Q?H=E9ctor_Moreno_Blanco?= <hmoreno@gmv.com> ; message-id:
<ADE5C314E6738E4F85E896FF7A8F217119E4C16A@ptmexchange3.gmv.es>
Apr 24 23:12:55 listas sympa[24538]: info main::DoMessage() Processing message
for lista_prueba with priority 5,
<ADE5C314E6738E4F85E896FF7A8F217119E4C16A@ptmexchange3.gmv.es>
Apr 24 23:12:55 listas sympa[24538]: notice List::get_editors_email() Warning :
no editor found for list lista_prueba, getting owners
```

```
Apr 24 23:12:55 listas sympa[24538]: info Auth::create_one_time_ticket()
Auth::create_one_time_ticket(moderador@correo.es,listas.correo.es,modindex/lista_
prueba,mail) value = 1383869217777
Apr 24 23:12:55 listas sympa[24538]: notice List::send_to_editor() ticket :
1383869217777
Apr 24 23:12:55 listas sympa[24538]: info main::DoMessage() Key
3bddb3cdfabe24848af0f2c1ee944c13 for list lista_prueba from hmoreno@gmv.com sent
to editors, /home/sympa/spool/msg/lista_prueba@listas.correo.es.1380057174.24783
```

5.5.3.1 Mensaje aceptado

Se enviará un mensaje a la lista moderada que se aceptará y se procederá a su distribución:

```
Sep 24 23:14:50 listas sympa[7919]: notice main::DoFile() Processing
/home/sympa/spool/msg/sympa6@listas.correo.es.1380057288.7221 ; sender:
moderador@correo.es ; message-id: <sympa.1380057288.1508.435@listas.correo.es>
Sep 24 23:14:50 listas sympa[7919]: info main::DoSendMessage() Processing web
message for sympa6@listas.correo.es
Sep 24 23:14:51 listas sympa[7919]: info main::DoSendMessage() Message for
sympa6@listas.correo.es sent
Sep 24 23:14:56 listas sympa[7919]: notice main::DoFile() Processing
/home/sympa/spool/msg/sympa6@listas.correo.es.1380057291.25530 ; sender:
moderador@correo.es ; message-id: <sympa.1380057288.1508.435@listas.correo.es>
Sep 24 23:14:56 listas sympa[7919]: notice Commands::parse() Parsing:
Sep 24 23:14:56 listas sympa[7919]: notice Commands::parse() Parsing: QUIET
DISTRIBUTE lista_prueba 3bddb3cdfabe24848af0f2c1ee944c13
Sep 24 23:14:56 listas sympa[7919]: info Commands::distribute() Message for
lista_prueba from moderador@correo.es accepted (0 seconds, 1 sessions, 3
subscribers), message-
id=<ADE5C314E6738E4F85E896FF7A8F217119E4C16A@ptmexchange3.gmv.es> , size=0
Sep 24 23:14:56 listas sympa[7919]: info Commands::distribute() DISTRIBUTE
lista_prueba 3bddb3cdfabe24848af0f2c1ee944c13 from moderador@correo.es accepted
(0 seconds)
Sep 24 23:14:56 listas bulk[2558]: notice Done sending message
<ADE5C314E6738E4F85E896FF7A8F217119E4C16A@ptmexchange3.gmv.es> to list
lista_prueba@listas.correo.es (priority 5) in 0 seconds since scheduled
expedition date.
```

5.5.3.2 Mensaje rechazado

Se enviará un mensaje a la lista moderada que se rechazará. A la hora de rechazar, se puede elegir si avisar al remitente o no (y con qué mensaje, también personalizable), y si agregar dicho remitente a una lista negra.

```
Apr 24 23:29:16 listas wwsympa[1508]: info [robot listas.correo.es] [session
74856431973973] [client 213.13.172.36] [user moderador@correo.es] [list
lista_prueba] main::do_reject() do_reject(424bbf1516a4c351c835ddbab292b08e)
```

5.6 POSTFIX

5.6.1 Envío correcto de un correo electrónico

Un correo de un usuario interno y válido envía un correo satisfactoriamente a un usuario externo de la plataforma. De la misma manera funcionaría si el usuario fuera interno, ya que se encargarían de volver a introducirlo a los buzones.

```
Apr 24 20:41:56 estafeta postfix/cleanup[24443]: 69CF6101768: message-
id=<20130924184148.69CF6101768@estafeta.correo.es>
Apr 24 20:41:56 estafeta postfix/qmgr[9432]: 69CF6101768:
from=<usuario1@correo.es>, size=363, nrcpt=1 (queue active)
Apr 24 20:41:56 estafeta postfix/smtp[24444]: 69CF6101768:
to=<usuario_ext@hotmail.com>, relay=ironport.correo.es[192.168.100.212]:25,
```

```
delay=16, delays=16/0.02/0/0, dsn=2.0.0, status=sent (250 ok:  Message 2825565
accepted)
Apr 24 20:41:56 estafeta postfix/qmgr[9432]: 69CF6101768: removed
```

5.6.2 Envío de un usuario no válido

Un correo enviado desde un usuario de la arquitectura que no existe. Se rechazará, enviando un correo avisando de ello al usuario que envió dicho correo:

```
Apr 24 18:11:58 estafeta postfix/smtpd[2449]: 3C7E84B97B:
client=buzon1[192.168.13.1]
Apr 24 18:11:58 estafeta postfix/cleanup[2744]: 3C7E84B97B: message-
id=<CAPpGcp6ZfDbGgkqX+d2u27MaeDLVNZ_5g1Q2oididyvLR0O43g@estafeta.correo.es>
Apr 24 18:11:58 estafeta postfix/qmgr[12349]: 3C7E84B97B:
from=<usuario_noexistente@correo.es>, size=486747, nrcpt=1 (queue active)
Apr 24 18:12:34 estafeta postfix/smtp[2455]: 3C7E84B97B: to=<usuario@correo.es>,
relay=ironport.correo.es[192.168.100.212]:25, delay=36, delays=0.03/0.01/0.03/36,
dsn=5.0.0, status=bounced (host ironport.correo.es[192.168.100.212] said: 550
unknown user (in reply to RCPT TO command))
Apr 24 18:12:34 estafeta postfix/bounce[2891]: 3C7E84B97B: sender non-delivery
notification: 17FE04BA92
Apr 24 18:12:34 estafeta postfix/qmgr[12349]: 3C7E84B97B: removed
```

5.6.3 Suplantación de identidad

A continuación, se presentarán los casos de suplantación de identidad. El primero es cuando se hace uso de un alias no válido (o una posible suplantación de correo de otro usuario), es decir, el

```
Apr 15 17:59:16 estafeta postfix/smtpd[18439]: maps_find:
smtpd_sender_login_maps: ldap:matchlogin(0,lock|fold_fix):
alias_noexistente@correo.es = usuario
Apr 15 17:59:16 estafeta postfix/smtpd[18439]: mail_addr_find:
alias_noexistente@correo.es -> usuario
Apr 15 17:59:16 estafeta postfix/smtpd[18439]: NOQUEUE: reject: RCPT from
hmoreno-local[192.168.1.30]: 553 5.7.1 <alias_noexistente@correo.es>: Sender
address rejected: not owned by user usuario; from=<alias_noexistente@correo.es>
to=<usuario@correo.es> proto=ESMTP helo=<[192.168.1.30]>
Apr 15 17:59:16 estafeta postfix/smtpd[18439]: generic_checks:
name=reject_authenticated_sender_login_mismatch status=2
Apr 15 17:59:16 estafeta postfix/smtpd[18439]: generic_checks:
name=reject_sender_login_mismatch status=2
Apr 15 17:59:16 estafeta postfix/smtpd[18439]: > hmoreno-local[192.168.1.30]: 553
5.7.1 <alias_noexistente@correo.es>: Sender address rejected: not owned by user
usuario
```

A continuación, se utilizará un alias existente del usuario:

```
Apr 15 18:00:27 estafeta postfix/smtpd[18439]: dict_ldap_lookup: Using existing
connection for LDAP source matchlogin
Apr 15 18:00:27 estafeta postfix/smtpd[18439]: dict_ldap_lookup: matchlogin:
Searching with filter
(|(mail=alias_usuario@correo.es)(mailAlternateAddress=alias_usuario@correo.es))
Apr 15 18:00:27 estafeta postfix/smtpd[18439]: dict_ldap_get_values[1]: Search
found 1 match(es)
Apr 15 18:00:27 estafeta postfix/smtpd[18439]: dict_ldap_get_values[1]: search
returned 1 value(s) for requested result attribute uid
Apr 15 18:00:27 estafeta postfix/smtpd[18439]: dict_ldap_get_values[1]: Leaving
dict_ldap_get_values
Apr 15 18:00:27 estafeta postfix/smtpd[18439]: dict_ldap_lookup: Search returned
usuario
```

```
Apr      15      18:00:27      estafeta      postfix/smtpd[18439]:      maps_find:
smtpd_sender_login_maps:                         ldap:matchlogin(0,lock|fold_fix):
alias_usuario@correo.es = usuario
Apr      15      18:00:27      estafeta      postfix/smtpd[18439]:      mail_addr_find:
alias_usuario@correo.es -> usuario
Apr      15      18:00:27      estafeta      postfix/smtpd[18439]:      generic_checks:
name=reject_authenticated_sender_login_mismatch status=0
Apr      15      18:00:27      estafeta      postfix/smtpd[18439]:      generic_checks:
name=reject_unauthenticated_sender_login_mismatch
Apr      15      18:00:27      estafeta      postfix/smtpd[18439]:      generic_checks:
name=reject_unauthenticated_sender_login_mismatch status=0
```

5.7 MySQL

5.7.1 Consultas

Una vez que se conecta a la base de datos:

```
# mysql -uroot -p
```

Se pueden visualizar las diferentes bases de datos, como las tablas de cada una, o una simple consulta de una tabla. Además se puede ver una breve descripción de cada tabla (de sus campos).

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| open-xchange       |
| sympa61            |
| test               |
+--------------------+
5 rows in set (0.01 sec)

mysql> use mysql;
Database changed
mysql> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| proc                      |
| procs_priv                |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
| user_info                 |
+---------------------------+
18 rows in set (0.02 sec)
```

```
mysql> describe user_info;
+---------------------+-------------+------+-----+---------+-------+
| Field               | Type        | Null | Key | Default | Extra |
+---------------------+-------------+------+-----+---------+-------+
| User                | varchar(16) | NO   | PRI | NULL    |       |
| Full_name           | varchar(60) | YES  | MUL | NULL    |       |
| Description         | varchar(255)| YES  |     | NULL    |       |
| Email               | varchar(80) | YES  |     | NULL    |       |
| Contact_information | text        | YES  |     | NULL    |       |
| Icon                | blob        | YES  |     | NULL    |       |
+---------------------+-------------+------+-----+---------+-------+
6 rows in set (0.00 sec)
```

5.7.2 Replicación

Para comprobar que las bases de datos se están replicando correctamente en ambos sentidos, primero se observará la replicación en uno y luego en otro.

En el nodo *bbdd1* se tomará nota de la siguiente información:

```
mysql> show master status;
+------------------+----------+--------------+------------------+
| File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+------------------+----------+--------------+------------------+
| mysql-bin.000064 |  1087432 |              |                  |
+------------------+----------+--------------+------------------+
```

Y se comprobará que están correctos en *bbdd2*:

```
mysql> show slave status\G
*************************** 1. row ***************************
             Slave_IO_State: Waiting for master to send event
                Master_Host: bbdd1
                Master_User: replica
                Master_Port: 3306
              Connect_Retry: 60
            Master_Log_File: mysql-bin.000064
        Read_Master_Log_Pos: 1087432
             Relay_Log_File: mysqld-relay-bin.001116
              Relay_Log_Pos: 235
      Relay_Master_Log_File: mysql-bin.000064
           Slave_IO_Running: Yes
          Slave_SQL_Running: Yes
            Replicate_Do_DB:
        Replicate_Ignore_DB:
         Replicate_Do_Table:
     Replicate_Ignore_Table:
    Replicate_Wild_Do_Table:
Replicate_Wild_Ignore_Table:
                 Last_Errno: 0
                 Last_Error:
               Skip_Counter: 0
        Exec_Master_Log_Pos: 1087432
            Relay_Log_Space: 235
            Until_Condition: None
             Until_Log_File:
              Until_Log_Pos: 0
         Master_SSL_Allowed: No
         Master_SSL_CA_File:
         Master_SSL_CA_Path:
            Master_SSL_Cert:
          Master_SSL_Cipher:
             Master_SSL_Key:
      Seconds_Behind_Master: 0
1 row in set (0.00 sec)
```

Además de comprobar que los campos *Exec_Master_Log_Pos* y *Relay_Master_Log_File* concuerdan con la salida del maestro, también que no existe ningún error (*Last_Errno*) y que el campo *Seconds_Behind_Master* está a 0.

A continuación se hace en el otro sentido para comprobar que todo está correcto.

5.8 OpenLDAP

A continuación se realizarán unas pruebas de consulta, modificación, eliminación de datos del LDAP.

5.8.1 Consulta de un usuario

Con el comando *ldapsearch* se pueden buscar usuarios mediante filtros de búsqueda. Es importante, al igual que ocurría con la MySQL, que la contraseña no se introduzca directamente en la consola, sino esperar a que se solicite.

```
# ldapsearch -x -LLL -H ldaps://virt_ldap:636 -D 'cn=Replication,dc=correo,dc=es'
-W -b 'idnc=usuarios,dc=correo,dc=es' uid=usuario_prueba

dn: cn=PRUEBA.CUENTA DE PRUEBAS.605962,idnc=usuarios,dc=correo,dc=es
idInterviniente: 605962
estado: 1
codCorreo: 4
visibleEnPaginasBlancas: 0
sexo: -
givenName: PRUEBA
pkCode: urn:mace:rediris.es:correo.es:usuario:v1:605962
uid: usuario_prueba
objectClass: top
objectClass: qmailUser
objectClass: VirtualMailAccount
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: correoPerson
objectClass: accountState
mailDelete: FALSE
privacidad: no
mailAlternateAddress: usuario@correo.es
firstAccess: TRUE
failedAccessCounter: 0
accountActive: TRUE
mailMessageStore: /buzon/buzon2/605962
mail: usuario@correo.es
sn: CUENTA DE PRUEBAS
cn: PRUEBA.CUENTA DE PRUEBAS.605962
pwdChangedTime: 201302150932Z
pwdHistory: 201205090936Z#{sha}Wd4PJdScWAzZjoNTYWcBwZ15sAQ=#201302121134Z#{sha
 }IPEi8NliZovf+zJ0RTbhBgtjdNk=#201302150932Z#{sha}PYFqQgCgHtgIGC+8VeLtYuJQbak=
userPassword:: e3NoYX1QWUZxUWdDZ0h0Z0lHQys4VmVMdFl1SlFiYWs9
mailQuotaSize: 10485760000
```

5.8.2 Adición de un usuario

Para la adición de un usuario, hay que atacar directamente al LDAP maestro. Para ello, se necesitará un fichero .ldif con todos los campos mínimos para ese usuario (se puede hacer manualmente en la consola, pero es más tedioso y con más probabilidades de error), y después se ejecutará el siguiente comando:

```
# ldapadd -x -LLL -H ldaps://ldap_maestro:636 -D 'cn=mailuser,dc=correo,dc=es' -W
-f info_usuario.ldif
```

5.8.3 Eliminación de un usuario

Para la eliminación de un usuario, hay que proceder de manera similar, simplemente hay que ejecutar el comando y especificar el CN completo del usuario a eliminar:

```
# ldapdelete -x -H ldaps://localhost:636 -D "cn=Replication,dc=correo,dc=es" -W
"cn=PRUEBA.CUENTA DE PRUEBAS.605962,idnc=usuarios,dc=correo,dc=es"
```

5.8.4 Modificación de un campo

Para modificar cualquier atributo de un usuario en el LDAP, existe el comando *ldapmodify*. Con este comando, se puede modificar un atributo, añadir o eliminar. Al igual que con la adición de usuarios, requiere un fichero .ldif (también se puede hacer manualmente).

El fichero, sería algo así:

```
dn: cn=PRUEBA.CUENTA DE PRUEBAS.605962,idnc=usuarios,dc=correo,dc=es
changetype: modify
replace: uid
uid: usuario2
-
add: uid2
uid2: usuario3
-
delete: uid2
```

Y la ejecución del commando, similar al de la adición:

```
# ldapmodify -x -LLL -H ldaps://ldap_maestro:636 -D 'cn=mailuser,dc=correo,dc=es'
-W -f modify_usuario.ldif
```

6 Conclusiones y trabajo futuro

6.1 Conclusiones

En base al estudio presentado en este PFC pordemos concluir que existen numerosas opciones o alternativas para la implantación de una plataforma de correo electrónico. La elección, de una u otra, se basará en criterios usabilidad, coste y fucionalidad, así como en las tecnologías que soporten en cada momento la plataforma elegida.

Adicionalmente, se ha demostrado que no se precisa pago alguno de licencias para disponer una plataforma funcional y eficaz, con todos los elementos.

Por otra parte, cuando se trata de la sincronización, no es tan sencillo encontrar gran variedad de productos de software libre. Aunque esto siempre dependerá de la solución Webmail que se instale.

Como aspectos clave de este proyecto, se resaltan los siguientes:

- La "fortaleza" del sistema propuesto, basado en sistemas ampliamente tratados y la diversidad de infraestruturas sobre la que se puede implantar.
- Numerosos profesionales capaces de proporcionar soporte y dar continuidad a los sistemas.
- Reducido coste de licencias y supresión de dependencias de "sistemas y plataformas propietarias".
- Facilidad de implementación.
- Facilidades para su externalización, siguiendo las tendencias del mercado hacia entornos CLOUD (PaaS, IaaS, SaaS).
- Evolución técnica de la plataforma, basado en la comunidad Open Source en continua aportación técnica.

Por último, se considera importante para la mejora y evolución de la plataforma, la evolución tecnológica y expansión del software libre, ya que es una de las bases de la misma, así como la aceptación y expansión de la externaliación de las soluciones TIC, hacia entornos físicos especializados donde el coste, la seguridad y la continuidad son factores clave de las decisiones de las organizaciones.

6.2 Trabajo futuro

A continuación, se van a proponer algunas eventuales mejoras de diseño y funcionamiento de la plataforma de correo electrónico presentada en el presente PFC (virtualiación, balanceos de software, monitorización, redes provadas "abiertas", *wikipedia*, cortafuegos…).

6.2.1 Virtualización

Una primera y lógica actualización de mejora de la plataforma se basaría en la virtualización de la misma. Esto mejoraría su administración y facilitaría la incorporación de más servidores en caso de tener problemas de carga.

Por otro lado, una vez que la plataforma estuviera virtualizada, el siguiente paso consistiría en trasladar todos los servicios a la *nube*. Tendencia que día a día es más seguida por numerosas empresas, organizaciones y particulares para facilitar la gestión de las diferentes plataformas existentes y favorecer la movilidad de los usuarios.

Al tratarse de una plataforma de correo electrónico elaborada prácticamente en su totalidad con software libre, los servidores de virtualización que se podrían implantar serían Xen Hypervisor. Éstos estarían alojados en máquinas de gran poptencia de proceso y almacenamiento y con suficientes recursos para poder albergar un gran número de servidores.

La administración de estas máquinas se lleva principalmente de forma manual por mediación de línea de comandos (en Xen es el comando 'xm'). Y la monitorización mediante herramientas gráficas (Convirt Appliance).

6.2.2 Balanceadores software

Una vez que se hubiera virtualizado la plataforma, se podrían añadir dos máquinas de balanceo para eliminar los switches. Estas máquinas tendrían un balanceador LVS, presente en el kernel de Linux, y con una posible interfaz web, Piranha.

El balanceo software es mucho más barato frente al hardware, ya que es un servidor Linux normal y corriente. Aunque puede presentar algo menos de potencia o estabilidad, estos problemas suelen ser mínimos.

6.2.3 Monitorización

Con el fin de tener monitorizada toda la plataforma de correo, se puede implantar un sistema de monitorización que permite tener vigilado en todo momento todas las máquinas y sus servicios.

Estos chequeos comprenden desde la disponibilidad de la máquina (memoria, CPU…) hasta los servicios propios de la plataforma. Cabe resaltar que no todos los servicios estaban a disposición para chequeos y por tanto se tendrían que desarrollar los scripts que realizan estos chequeos a ciertos servicios/puertos.

Esta monitorización se puede llevar a cabo mediante la instalación de un servidor de Nagios, que es de software libre. Este tipo de servidor de monitorización son muy potentes ya que permiten la elaboración propia de scripts de chequeo, y poseen una interfaz bastante sencilla pero también personalizable para que tenga un mejor *look&feel*. Además, se pueden mandar alarmas tanto a dispositivos móviles como a correo electrónico.

6.2.4 OpenVPN

Con el objetivo de poder conectar con la plataforma de manera segura desde cualquier lugar del mundo, se puede plantear la creación de un servidor de VPN con la tecnología OpenVPN. De este modo, a los usuarios que se quieran conectar a la plataforma, se les asignará un certificado personalizado con el cual podrán acceder a las máquinas de manera rápida y sencilla.

6.2.5 Wikipedia

Para una comprensión de la plataforma entera se instalaría una Wikipedia de consulta en la que se encontrarán detallados todas las características, tanto hardware como software, de la infraestructura al completo.

Asimismo, en esta Wikipedia también dispondrá de procedimientos realizados para distintas actividades que se hayan realizado o para problemas que puedan surgir en la plataforma. También podrá haber procedimientos para diferentes tareas a realizar periódicamente.

El software empleado para la implementación de esta Wikipedia es de software libre y se denomina Redmine. Su instalación puede ser bastante complicada, pero gracias a BitNami, se disponen de binarios que instala todos los paquetes y dependencias necesarios para el funcionamiento de este aplicativo.

6.2.6 Firewall Builder

La administración de las reglas de un cortafuegos IPTABLES de manera manual puede ser muy complicada según vayan aumentando estas reglas. Existe una herramienta, también de software libre que permite una gestión gráfica de IPTABLES, que permite también la gestión en clúster. Se denomina Firewall Builder.

Permite todo tipo de gestión posible con IPTABLES, desde la simple creación de reglas, como nateos de direcciones, etc.

Se puede instalar tanto en las propias máquinas de cortafuegos como en un servidor separado de éstos.

Referencias

[1] Aníbal R. Figueras. "Una Panorámica de las Telecomunicaciones". Prentice Hall. 2002
[2] Brian B. "A Brief History of Telecommunications". http://www.cellphones.ca/features/brief-history-telecommunications/
[3] IBM Radiotype. http://www-03.ibm.com/ibm/history/exhibits/specialprod1/specialprod1_3.html
[4] Teleprinter. https://en.wikipedia.org/wiki/Teleprinter
[5] Inventors of the Modern Computer – ARPANET. http://inventors.about.com/library/weekly/aa091598.htm
[6] Historia del correo electrónico. http://www.telecable.es/personales/carlosmg1/historia_correo.htm
[7] Correo electrónico. http://es.wikipedia.org/wiki/Correo_electr%C3%B3nico
[8] Simple Mail Transfer Protocol. http://tools.ietf.org/html/rfc5321
[9] Post-Office Protocol – Version 3. http://tools.ietf.org/html/rfc1939
[10] Internet Message Access Protocol – Version 4rev1. http://tools.ietf.org/html/rfc3501
[11] File Transfer Protocol. http://tools.ietf.org/html/rfc959
[12] An HTTP Extension Framework. http://tools.ietf.org/html/rfc2774
[13] Hypertext Markup Language – 2.0. http://tools.ietf.org/html/rfc1866
[14] Multipurpose Internet Mail Extensions – MIME. http://tools.ietf.org/html/rfc2045 http://tools.ietf.org/html/rfc2046 http://tools.ietf.org/html/rfc2047 http://tools.ietf.org/html/rfc4288 http://tools.ietf.org/html/rfc4289 http://tools.ietf.org/html/rfc2077
[15] Sieve: An Email Filtering Language. http://tools.ietf.org/html/rfc5228
[16] The Secure Sockets Layer (SSL) Protocol – Version 3.0. http://tools.ietf.org/html/rfc6101
[17] The Transport Layer Security (TLS) Protocol – Version 1.2. http://tools.ietf.org/html/rfc5246 http://tools.ietf.org/html/rfc6176
[18] Lightweight Directory Access Protocol - http://tools.ietf.org/html/rfc4510
[19] SyncML. http://en.wikipedia.org/wiki/SyncML
[20] TCP/IP. http://www.ietf.org/rfc/rfc793.txt
[21] Communication Layers. http://tools.ietf.org/html/rfc1122
[22] OSI for routing in TCP/IP. http://tools.ietf.org/html/rfc1195
[23] Domain Names. http://tools.ietf.org/html/rfc1034 http://tools.ietf.org/html/rfc1035
[24] Network Address Translator. http://tools.ietf.org/html/rfc3022
[25] DSPAM. http://dspam.nuclearelephant.com/index.shtml
[26] SPAMASSASSIN. http://wiki.apache.org/spamassassin/
[27] DomainKeys Identified Mail. http://tools.ietf.org/html/rfc4686 https://www.ietf.org/rfc/rfc4871.txt http://tools.ietf.org/html/rfc5617 http://tools.ietf.org/html/rfc5585 http://tools.ietf.org/html/rfc5672 http://tools.ietf.org/html/rfc5863 http://tools.ietf.org/html/rfc6376 http://tools.ietf.org/html/rfc6377
[28] Sender Policy Framework. http://tools.ietf.org/html/rfc4408
[29] Sendmail. http://www.sendmail.com/sm/open_source/
[30] B. Costales. "Sendmail – 3ªed.". O'Reilly. 2003
[31] Postfix. http://www.postfix.org/
[32] K.D. Dent. "Postfix: The Definitive Guide". O'Reilly. 2003
[33] Exim. http://www.exim.org/

[34] P. Hazel. “The Exim SMTP mail server. Official Guide for Release 4”. UIT Cambridge. 2003.
[35] Qmail. http://cr.yp.to/qmail.html
[36] John Levine. “qmail”. O’Reilly. 2004
[37] Cisco – Ironport. Overview. http://www.cisco.com/web/about/ac49/ac0/ac1/ac259/ironport.html
[38] Cisco – Ironport. Customer Q&A. http://www.cisco.com/en/US/services/ps10436/ps11169/ironport-customer-eo-qa.pdf
[39] Ironport Systems. “Ironport AsyncOS – User Guide”. 2012
[40] Ironport Systems. “Ironport AsyncOS – Advanced User Guide”. 2012
[41] Procmail. http://www.procmail.org/
[42] Courier Maildrop. http://www.courier-mta.org/maildrop/
[43] Cyrus. http://cyrusimap.web.cmu.edu/
[44] Dovecot. http://www.dovecot.org/
[45] Dovecot - Secure IMAP Server. http://www.dovecot.org/security.html
[46] Open-Source mailers and Groupware. http://cruisytaiwan.wordpress.com/2009/09/21/open-source-mailers-and-groupware-part-2/
[47] Zarafa. http://www.zarafa.es/
[48] Horde Groupware. http://www.horde.org/
[49] Roundcube. http://roundcube.net/
[50] Roundcube – Plugin Repository. http://trac.roundcube.net/wiki/Plugin_Repository
[51] Open-Xchange. http://www.open-xchange.com/home.html
[52] Open-Xchange: Oxpedia. http://oxpedia.org/index.php?title=Main_Page_CE
[53] Egroupware. http://www.egroupware.org/
[54] Zimbra. http://www.zimbra.com/
[55] Egroupware – Community Edition. http://www.egroupware.org/community_edition
[56] José Antonio Merlo Vega. “Las Listas de Distribución como Herramienta Profesional”. http://exlibris.usal.es/merlo/escritos/pdf/mei.pdf
[57] UPV .“¿Qué son las listas de distribución?”. https://www.upv.es/entidades/ASIC/catalogo/431879normalc.html
[58] Lista de correo electrónico. http://es.wikipedia.org/wiki/Lista_de_correo_electr%C3%B3nico
[59] Espacio Linux. “Instalando y configurando majordomo”. http://www.espaciolinux.com/2003/07/instalando-y-configurando-majordomo-1945-mailing-list-manager/
[60] Majordomo (software). http://en.wikipedia.org/wiki/Majordomo_%28software%29
[61] Majordomo. http://www.greatcircle.com/majordomo/
[62] Sympa Mailing List Server. https://www.sympa.org/
[63] Sympa – Detailed list of features. http://www.sympa.org/overview/features
[64] Listserv. http://www.lsoft.com/products/listserv.asp
[65] Sympa – Prerequisites. https://www.sympa.org/manual_6.1/installing-sympa#prerequisites
[66] Funambol Sync Server: http://www.funambol.com/
[67] Open-Xchange – Instalación. http://oxpedia.org/wiki/index.php?title=Open-Xchange_Installation_Guide_for_RHEL5
[68] Sympa: Prerrequisitos. https://www.sympa.org/manual_6.1/installing-sympa#prerequisites
[69] Funambol: archivos del proyecto. http://forge.ow2.org/project/showfiles.php?group_id=96

Anexos

A IPTABLES

/etc/sysconfig/iptables:

```
# Generated by iptables-save v1.3.5 on Thu Oct 18 12:24:58 2012
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [658:191236]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -s 127.0.0.1 -j ACCEPT
-A RH-Firewall-1-INPUT -p igmp -j DROP
-A RH-Firewall-1-INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
-A      RH-Firewall-1-INPUT      -p      tcp      -m      multiport      --dports
25,80,110,143,443,465,587,993,995 -j ACCEPT
-A      RH-Firewall-1-INPUT      -p      tcp      -m      multiport      --dports
21,22,25,80,110,143,443,465,587,993,995 -s 161.111.80.253 -j ACCEPT
-A      RH-Firewall-1-INPUT      -p      tcp      -m      multiport      --dports
21,22,25,80,110,143,443,465,587,993,995 -s 161.111.80.48 -j ACCEPT
#####################################################################
-A      RH-Firewall-1-INPUT      -p      tcp      -m      multiport      --dports
22,25,80,110,143,443,465,587,993,995 -s 192.168.55.251 -j ACCEPT
-A      RH-Firewall-1-INPUT      -p      tcp      -m      multiport      --dports
22,25,80,110,143,443,587,993,995 -s 212.0.110.2 -j ACCEPT
-A      RH-Firewall-1-INPUT      -p      tcp      -m      multiport      --dports
22,25,80,110,143,443,587,993,995 -s 213.27.133.3 -j ACCEPT
-A      RH-Firewall-1-INPUT      -p      tcp      -m      multiport      --dports
22,25,80,110,143,443,587,993,995 -s 195.219.143.2 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 22,21,25 -s 161.111.10.144 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 22,21,25 -s 161.111.10.143 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 22,21,25 -s 161.111.10.139 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 22,21 -s 161.111.10.117 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 389,636 -s 161.111.100.93 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 389,636 -s 161.111.100.92 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 389,636 -s 161.111.100.131 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 389,636 -s 161.111.100.132 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 1525 -s 161.111.100.89 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 1525 -s 161.111.83.59 -j
ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m multiport --dports 389,636 -s 161.111.98.27 -j
ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.100.0/24 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A RH-Firewall-1-INPUT -j LOG --log-level 5
-A RH-Firewall-1-INPUT -p tcp -j DROP
-A RH-Firewall-1-INPUT -p udp -j DROP
COMMIT
# Completed on Thu Oct 18 12:24:58 2012
# Generated by iptables-save v1.3.5 on Thu Oct 18 12:24:58 2012
```

```
*nat
:PREROUTING ACCEPT [2267:142839]
:POSTROUTING ACCEPT [28:1944]
:OUTPUT ACCEPT [28:1944]
-A PREROUTING -i eth1 -d 161.111.10.239 -j DNAT --to-destination 192.168.100.202
-A PREROUTING -i eth1 -d 161.111.10.248 -j DNAT --to-destination 192.168.100.202
-A PREROUTING -i eth1 -d 161.111.10.223 -j DNAT --to-destination 192.168.100.205
-A PREROUTING -i eth1 -d 161.111.10.39 -j DNAT --to-destination 192.168.100.213
-A PREROUTING -i eth1 -d 161.111.10.250 -j DNAT --to-destination 192.168.13.30
-A PREROUTING -i eth1 -d 161.111.10.169 -j DNAT --to-destination 192.168.100.208
-A PREROUTING -i eth1 -d 161.111.10.242 -j DNAT --to-destination 192.168.100.204
-A PREROUTING -i eth1 -d 161.111.10.104 -j DNAT --to-destination 192.168.100.203
-A PREROUTING -i eth1 -d 161.111.10.26 -j DNAT --to-destination 192.168.100.210
-A PREROUTING -i eth1 -d 161.111.10.67 -j DNAT --to-destination 192.168.100.203
-A PREROUTING -i eth1 -d 161.111.10.249 -j DNAT --to-destination 192.168.100.209
-A PREROUTING -i eth1 -d 161.111.10.241 -j DNAT --to-destination 192.168.100.201
-A PREROUTING -i eth1 -d 161.111.10.240 -j DNAT --to-destination 192.168.100.206
-A POSTROUTING -s 192.168.100.0/24 -o eth1 -j MASQUERADE
COMMIT
# Completed on Thu Oct 18 12:24:58 2012
```

B SWITCHES

/cfg/dump:

```
script start "Nortel Networks Layer2-7 GbE Switch Module" 4  /**** DO NOT EDIT
THIS LINE!
/* Configuration dump taken 10:21:50 Fri Oct  5, 2012
/* Version 21.0.5,  Base MAC address 00:0f:06:ed:c6:00
/c/sys
        idle 20
/c/sys/access/user
        admpw "3a70dd0f0850880af232b6e6cbe02bf812d64701b13c2c4147c0dec739c721f6"
/c/port INT1
        pvid 303
/c/port INT4
        pvid 303
/c/port INT8
        pvid 303
/c/port INT11
        pvid 303
/c/port EXT1
        pvid 306
/c/port EXT2
        pvid 301
/c/port EXT3
        tag ena
        pvid 305
/c/port EXT4
        pvid 301
/c/l2/vlan 1
        def INT2 INT3 INT5 INT6 INT7 INT9 INT10 INT12 INT13 INT14 EXT3
/c/l2/vlan 300
        ena
        name "Balanceo"
        def INT3 INT10 EXT3
/c/l2/vlan 301
        ena
        name "Nas"
        def INT2 INT5 INT6 INT7 INT9 INT12 INT13 INT14 EXT2 EXT3 EXT4
/c/l2/vlan 303
        ena
        name "Correo"
        def INT1 INT2 INT4 INT5 INT6 INT7 INT8 INT9 INT11 INT12 INT13 INT14 EXT3
/c/l2/vlan 305
        ena
        name "VLAN de HB"
        def INT3 INT10 EXT3
/c/l2/vlan 306
        ena
        name "VLAN PRIVADA"
        def INT3 INT10 EXT1
/c/l2/stg 1/clear
/c/l2/stg 1/add 1 300 301 303 305 306
/c/sys/access/sshd/on
/c/l3/if 1
        ena
        addr 192.168.100.101
        vlan 300
/c/l3/if 2
        ena
        addr 192.168.13.101
        vlan 303
/c/l3/gw 1
        ena
        addr 192.168.100.10
/c/l3/vrrp/on
```

```
/c/l3/vrrp/vr 1
        ena
        vrid 21
        if 1
        prio 110
        addr 192.168.100.100
        track
                ports e
/c/l3/vrrp/vr 2
        ena
        vrid 22
        if 2
        prio 110
        addr 192.168.13.100
        track
                ports e
/c/l3/vrrp/vr 3
        ena
        vrid 201
        if 2
        prio 110
        addr 192.168.13.201
        track
                ports e
/c/l3/vrrp/vr 4
        ena
        vrid 202
        if 2
        prio 110
        addr 192.168.13.202
        track
                ports e
/c/l3/vrrp/vr 5
        ena
        vrid 203
        if 2
        prio 110
        addr 192.168.13.203
        track
                ports e
/c/l3/vrrp/vr 6
        ena
        vrid 204
        if 2
        prio 110
        addr 192.168.13.204
        track
                ports e
/c/l3/vrrp/vr 7
        ena
        vrid 205
        if 2
        prio 110
        addr 192.168.13.205
        track
                ports e
/c/l3/vrrp/vr 8
        ena
        vrid 206
        if 2
        prio 110
        addr 192.168.13.206
        track
                ports e
/c/l3/vrrp/vr 9
        ena
        vrid 207
```

```
        if 2
        prio 110
        addr 192.168.13.207
        track
                ports e
/c/l3/vrrp/group
        ena
        vrid 2
        if 2
        prio 110
        track
                ports ena
/c/sys/ntp
        on
        prisrv 161.111.80.11
        tzone +2:00
/c/slb/adv
        direct ena
        grace ena
/c/slb/sync
        prios d
        reals e
        state e
/c/slb/sync/peer 1
        ena
        addr 192.168.100.102
/c/slb/sync/peer 2
        ena
        addr 192.168.100.101
/c/slb/real 1
        ena
        rip 192.168.13.1
        weight 10
        tmout 30
        inter 30
        name "buzon1"
/c/slb/real 2
        ena
        rip 192.168.13.2
        weight 10
        tmout 30
        inter 30
        name "buzon2"
/c/slb/real 3
        ena
        rip 192.168.13.3
        weight 10
        tmout 30
        inter 30
        name "buzon3"
/c/slb/real 4
        ena
        rip 192.168.13.4
        weight 20
        tmout 30
        inter 30
        name "buzon4"
/c/slb/real 5
        ena
        rip 192.168.13.5
        weight 20
        tmout 30
        inter 30
        name "buzon5"
/c/slb/real 6
        ena
        rip 192.168.13.6
```

```
        weight 20
        tmout 30
        inter 30
        name "buzon6"
/c/slb/real 7
        ena
        rip 192.168.13.7
        tmout 30
        name "buzon7"
/c/slb/real 8
        ena
        rip 192.168.13.8
        weight 10
        tmout 30
        inter 30
        name "buzon8"
/c/slb/real 9
        ena
        rip 192.168.13.9
        weight 10
        tmout 30
        inter 30
        name "listas1"
/c/slb/real 10
        ena
        rip 192.168.13.10
        weight 10
        tmout 30
        inter 30
        name "listas2"
/c/slb/real 11
        ena
        rip 192.168.13.11
        weight 20
        inter 30
        name "estafeta1"
/c/slb/real 12
        ena
        rip 192.168.13.12
        weight 20
        inter 30
        name "estafeta2"
/c/slb/real 21
        ena
        rip 192.168.13.21
        weight 10
        inter 30
        name "bbdd1"
/c/slb/real 22
        ena
        rip 192.168.13.22
        weight 10
        inter 30
        name "bbdd2"
/c/slb/group 1
        metric roundrobin
        add 1
        add 2
        add 3
        add 4
        add 5
        add 6
        add 7
        add 8
        name "buzones_webmail"
/c/slb/group 2
        metric roundrobin
```

```
        add 11
        add 12
        name "estafetas"
/c/slb/group 3
        metric roundrobin
        add 1
        add 2
        add 3
        add 4
        add 5
        add 6
        add 7
        add 8
        name "buzones_smtp"
/c/slb/group 4
        metric roundrobin
        add 1
        add 2
        add 3
        add 4
        add 5
        add 6
        add 7
        add 8
        name "buzones_imap"
/c/slb/group 5
        metric roundrobin
        add 9
        add 10
        name "listas_http"
/c/slb/group 6
        metric roundrobin
        add 9
        add 10
        name "listas_smtp"
/c/slb/group 7
        metric roundrobin
        add 21
        add 22
        name "ldap"
/c/slb/port INT1
        client ena
        server ena
/c/slb/port INT2
        client ena
        server ena
/c/slb/port INT3
        client ena
        server ena
/c/slb/port INT4
        client ena
        server ena
/c/slb/port INT5
        client ena
        server ena
/c/slb/port INT6
        client ena
        server ena
/c/slb/port INT7
        client ena
        server ena
/c/slb/port INT8
        client ena
        server ena
/c/slb/port INT9
        client ena
        server ena
```

```
/c/slb/port INT10
        client ena
        server ena
/c/slb/port INT11
        client ena
        server ena
/c/slb/port INT12
        client ena
        server ena
/c/slb/port INT13
        client ena
        server ena
/c/slb/port INT14
        client ena
        server ena
/c/slb/port EXT1
        client ena
        server ena
/c/slb/port EXT2
        client ena
        server ena
/c/slb/port EXT3
        client ena
        server ena
/c/slb/port EXT4
        client ena
        server ena
/c/slb/virt 1
        ena
        vip 192.168.13.201
/c/slb/virt 1/service https
        group 1
        pbind clientip
/c/slb/virt 1/service http
        group 1
        pbind clientip
/c/slb/virt 2
        ena
        vip 192.168.13.202
/c/slb/virt 2/service smtp
        group 2
/c/slb/virt 2/service 587
        group 2
        rport 25
/c/slb/virt 3
        ena
        vip 192.168.13.203
/c/slb/virt 3/service smtp
        group 3
/c/slb/virt 4
        ena
        vip 192.168.13.204
/c/slb/virt 4/service pop3
        group 4
/c/slb/virt 4/service imap
        group 4
/c/slb/virt 4/service 993
        group 4
/c/slb/virt 4/service 995
        group 4
/c/slb/virt 5
        ena
        vip 192.168.13.205
/c/slb/virt 5/service http
        group 5
        pbind clientip
/c/slb/virt 5/service https
```

```
        group 5
        pbind clientip
/c/slb/virt 6
        ena
        vip 192.168.13.206
/c/slb/virt 6/service smtp
        group 6
/c/slb/virt 7
        ena
        vip 192.168.13.207
/c/slb/virt 7/service ldap
        group 7
/
script end  /**** DO NOT EDIT THIS LINE!
```

C DOVECOT

/etc/dovecot/dovecot.conf:

```
# 2.1.6: /usr/local/dovecot/etc/dovecot/dovecot.conf
auth_cache_size = 500 k
auth_cache_ttl = 1000 secs
disable_plaintext_auth = no
first_valid_uid = 501
lock_method = dotlock
mail_fsync = always
mail_gid = vmail
mail_location = maildir:%h/Maildir
mail_nfs_index = yes
mail_nfs_storage = yes
mail_plugins = quota autocreate mail_log notify
mail_uid = vmail
managesieve_notify_capability = mailto
managesieve_sieve_capability = fileinto reject envelope encoded-character
vacation subaddress comparator-i;ascii-numeric relational regex imap4flags copy
include variables body enotify environment mailbox date ihave imapflags notify
mmap_disable = yes
namespace {
  inbox = yes
  location =
  prefix =
  separator = .
  type = private
}
namespace {
  hidden = yes
  inbox = no
  list = no
  location =
  prefix = INBOX.
  separator = .
  type = private
}
passdb {
  args = /etc/dovecot/dovecot-ldap.conf
  driver = ldap
}
plugin {
  autocreate = Spam
  autosubscribe = Spam
  mail_log_events = delete expunge copy mailbox_delete mailbox_rename
  quota_warning = storage=75%% quota-warning 75 %u
  quota_warning2 = storage=90%% quota-warning 90 %u
  sieve = %h/.dovecot.sieve
  sieve_dir = %h/sieve
  sieve_extensions = +imapflags +notify
}
protocols = imap pop3 sieve
service anvil {
  client_limit = 5000
}
service auth {
  client_limit = 9000
  unix_listener auth-master {
    group = vmail
    mode = 0700
    user = vmail
  }
  user = root
  vsz_limit = 1 G
}
```

```
service imap-login {
  executable = /usr/local/dovecot/libexec/dovecot/imap-login
  inet_listener imap {
    address = *
    port = 143
  }
  inet_listener imaps {
    address = *
    port = 993
  }
  process_limit = 2048
  process_min_avail = 20
  service_count = 0
  user = vmail
}
service imap {
  executable = /usr/local/dovecot/libexec/dovecot/imap
  process_limit = 2048
}
service managesieve-login {
  executable = /usr/local/dovecot/libexec/dovecot/managesieve-login
  inet_listener sieve {
    address = *
    port = 4190
  }
  inet_listener sieve_deprecated {
    address = *
    port = 12000
  }
  user = vmail
}
service managesieve {
  executable = /usr/local/dovecot/libexec/dovecot/managesieve
}
service pop3-login {
  executable = /usr/local/dovecot/libexec/dovecot/pop3-login
  inet_listener pop3 {
    address = *
    port = 110
  }
  inet_listener pop3s {
    address = *
    port = 995
  }
  process_limit = 2048
  process_min_avail = 20
  service_count = 0
  user = vmail
}
service pop3 {
  executable = /usr/local/dovecot/libexec/dovecot/pop3
  process_limit = 2048
}
service quota-warning {
  executable = script /usr/local/dovecot/bin/quota-warning.sh
  unix_listener quota-warning {
    group = vmail
    mode = 0700
    user = vmail
  }
}
ssl_ca = </etc/ssl/correo.ca-bundle
ssl_cert = </etc/ssl/correo.crt
ssl_key = </etc/ssl/correo.pem
ssl_verify_client_cert = yes
syslog_facility = local3
userdb {
```

```
  args = /etc/dovecot/dovecot-ldap.conf
  driver = ldap
}
valid_chroot_dirs = /buzones/
protocol imap {
  imap_client_workarounds =
  mail_plugin_dir = /usr/local/dovecot/lib/dovecot
  mail_plugins = quota autocreate mail_log notify imap_quota
}
protocol pop3 {
  mail_plugin_dir = /usr/local/dovecot/lib/dovecot
  mail_plugins = quota autocreate mail_log notify
  pop3_uidl_format = %08Xu%08Xv
}
protocol lda {
  auth_socket_path = /usr/local/dovecot/var/run/dovecot/auth-master
  hostname = buzonX.correo.es
  mail_plugin_dir = /usr/local/dovecot/lib/dovecot
  mail_plugins = quota autocreate mail_log notify sieve
  postmaster_address = postmaster@correo.es
  quota_full_tempfail = no
  rejection_reason = Su mensaje para <%t> fue rechazado automaticamente por
nuestro sistema :%n%r
  rejection_subject = Rechazado: %s
  sendmail_path = /usr/sbin/exim
}
protocol sieve {
  managesieve_implementation_string = dovecot Pigeonhole
  managesieve_logout_format = bytes ( in=%i : out=%o )
  managesieve_max_line_length = 65536
}
```

/etc/dovecot/dovecot-ldap.conf:

```
# INFORMACIÓN DE CONEXIÓN AL LDAP
uris = ldaps://virt_ldap
auth_bind = yes
ldap_version = 3
dnpass = p4ssw0rd
dn = cn=mailuser,dc=correo,dc=es
#debug_level =  -1
base = idnc=usuarios,dc=correo,dc=es
deref = never
scope = subtree

## CONSULTA AL LDAP PARA AUTENTICACION
pass_filter = (&(objectClass=qmailUser)(uid=%u)(accountActive=TRUE))
pass_attrs = uid=user,userPassword=password, mailQuotaSize=quota_rule=*:bytes=%$

## CONSULTA AL LDAP COMO BBDD
# Se extrae la ruta al buzon del usuario y la cuota del usuario
user_attrs = mailMessageStore=home, mailQuotaSize=quota_rule=*:bytes=%$
user_filter                                                              =
(&(objectClass=qmailUser)(|(mailAlternateAddress=%u)(mail=%u)(uid=%u))(accountAct
ive=TRUE))
```

/etc/init.d/dovecot:

```
#! /bin/sh
#
# dovecot    This shell script takes care of starting and stopping dovecot
#
# chkconfig: 2345 70 40
# description:  Dovecot is an open source IMAP and POP3 email server /
#               for Linux/UNIX-like systems
```

```
#
# processname: dovecot
# config: /etc/dovecot/dovecot.conf

DAEMON=/usr/local/dovecot/sbin/dovecot

ulimit -n 9000

test -x $DAEMON || exit 1
set -e

base_dir=`$DAEMON -a|grep '^base_dir = '|sed 's/^base_dir = //'`
pidfile=$base_dir/master.pid

if test -f $pidfile; then
  running=yes
else
  running=no
fi

case "$1" in
  start)
    echo -n "Starting Dovecot"
    $DAEMON
    echo "."
    ;;
  stop)
    if test $running = yes; then
      echo "Stopping Dovecot"
      kill `cat $pidfile`
      echo "."
    else
      echo "Dovecot is already stopped."
    fi
    ;;
  reload)
    if test $running = yes; then
      echo -n "Reloading Dovecot configuration"
      kill -HUP `cat $base_dir/master.pid`
      echo "."
    else
      echo "Dovecot isn't running."
    fi
    ;;
  restart|force-reload)
    echo -n "Restarting Dovecot"
    if test $running = yes; then
      kill `cat $base_dir/master.pid`
      sleep 1
    fi
    $DAEMON
    echo "."
    ;;
  *)
    echo  "Usage:  /etc/init.d/dovecot  {start|stop|reload|restart|force-reload}"
>&2
    exit 1
    ;;
esac

exit 0
```

D EXIM

/etc/exim/exim.conf

```
##########################################################################
#                    Runtime configuration file for Exim                 #
##########################################################################


# This is a default configuration file which will operate correctly in
# uncomplicated installations. Please see the manual for a complete list
# of all the runtime configuration options that can be included in a
# configuration file. There are many more than are mentioned here. The
# manual is in the file doc/spec.txt in the Exim distribution as a plain
# ASCII file. Other formats (PostScript, Texinfo, HTML, PDF) are available
# from the Exim ftp sites. The manual is also online at the Exim web sites.


# This file is divided into several parts, all but the first of which are
# headed by a line starting with the word "begin". Only those parts that
# are required need to be present. Blank lines, and lines starting with #
# are ignored.


############ IMPORTANT ########## IMPORTANT ############ IMPORTANT ############
#                                                                            #
# Whenever you change Exim's configuration file, you *must* remember to     #
# HUP the Exim daemon, because it will not pick up the new configuration    #
# until you do. However, any other Exim processes that are started, for     #
# example, a process started by an MUA in order to send a message, will     #
# see the new configuration as soon as it is in place.                      #
#                                                                            #
# You do not need to HUP the daemon for changes in auxiliary files that     #
# are referenced from this file. They are read every time they are used.    #
#                                                                            #
# It is usually a good idea to test a new configuration for syntactic       #
# correctness before installing it (for example, by running the command     #
# "exim -C /config/file.new -bV").                                          #
#                                                                            #
############ IMPORTANT ########## IMPORTANT ############ IMPORTANT ############
trusted_users = sympa
log_file_path = syslog : /var/log/exim/%s.log

##########################################################################
#                      MAIN CONFIGURATION SETTINGS                       #
##########################################################################

# Specify your host's canonical name here. This should normally be the fully
# qualified "official" name of your host. If this option is not set, the
# uname() function is called to obtain the name. In many cases this does
# the right thing and you need not set anything explicitly.

primary_hostname = correo.es
smtp_enforce_sync = false

# The next three settings create two lists of domains and one list of hosts.
# These lists are referred to later in this configuration using the syntax
# +local_domains, +relay_to_domains, and +relay_from_hosts, respectively. They
# are all colon-separated lists:

domainlist        local_domains        =        ${tr        {${lookup        ldapm{
user="cn=mailuser,dc=correo,dc=es"                                  pass="p4ssw0rd"
ldaps://virt_ldap/ou=dominios,idnc=correo,idnc=sistemas,idnc=servicios,dc=correo,
dc=es?vd?one?(&(accountActive=TRUE)(mailDelete=FALSE))}}} {\n}{:}}

#domainlist local_domains = correo.es
```

```
domainlist relay_to_domains =
hostlist   relay_from_hosts = 127.0.0.1


# Most straightforward access control requirements can be obtained by
# appropriate settings of the above options. In more complicated situations, you
# may need to modify the Access Control List (ACL) which appears later in this
# file.

# The first setting specifies your local domains, for example:
#
#   domainlist local_domains = my.first.domain : my.second.domain
#
# You can use "@" to mean "the name of the local host", as in the default
# setting above. This is the name that is specified by primary_hostname,
# as specified above (or defaulted). If you do not want to do any local
# deliveries, remove the "@" from the setting above. If you want to accept mail
# addressed to your host's literal IP address, for example, mail addressed to
# "user@[192.168.23.44]", you can add "@[]" as an item in the local domains
# list. You also need to uncomment "allow_domain_literals" below. This is not
# recommended for today's Internet.

# The second setting specifies domains for which your host is an incoming relay.
# If you are not doing any relaying, you should leave the list empty. However,
# if your host is an MX backup or gateway of some kind for some domains, you
# must set relay_to_domains to match those domains. For example:
#
# domainlist relay_to_domains = *.myco.com : my.friend.org
#
# This will allow any host to relay through your host to those domains.
# See the section of the manual entitled "Control of relaying" for more
# information.

# The third setting specifies hosts that can use your host as an outgoing relay
# to any other host on the Internet. Such a setting commonly refers to a
# complete local network as well as the localhost. For example:
#
# hostlist relay_from_hosts = 127.0.0.1 : 192.168.0.0/16
#
# The "/16" is a bit mask (CIDR notation), not a number of hosts. Note that you
# have to include 127.0.0.1 if you want to allow processes on your host to send
# SMTP mail by using the loopback address. A number of MUAs use this method of
# sending mail.


# All three of these lists may contain many different kinds of item, including
# wildcarded names, regular expressions, and file lookups. See the reference
# manual for details. The lists above are used in the access control list for
# incoming messages. The name of this ACL is defined here:

acl_smtp_rcpt = acl_check_rcpt

# You should not change that setting until you understand how ACLs work.

# The following ACL entries are used if you want to do content scanning with
# the exiscan-acl patch. When you uncomment one of these lines, you must also
# review the respective entries in the ACL section further below.

# acl_smtp_mime = acl_check_mime
# acl_smtp_data = acl_check_content

# This configuration variable defines the virus scanner that is used with
# the 'malware' ACL condition of the exiscan acl-patch. If you do not use
# virus scanning, leave it commented. Please read doc/exiscan-acl-readme.txt
# for a list of supported scanners.

# av_scanner = sophie:/var/run/sophie
```

```
# The following setting is only needed if you use the 'spam' ACL condition
# of the exiscan-acl patch. It specifies on which host and port the SpamAssassin
# "spamd" daemon is listening. If you do not use this condition, or you use
# the default of "127.0.0.1 783", you can omit this option.

# spamd_address = 127.0.0.1 783

# Specify the domain you want to be added to all unqualified addresses
# here. An unqualified address is one that does not contain an "@" character
# followed by a domain. For example, "caesar@rome.example" is a fully qualified
# address, but the string "caesar" (i.e. just a login name) is an unqualified
# email address. Unqualified addresses are accepted only from local callers by
# default. See the recipient_unqualified_hosts option if you want to permit
# unqualified addresses from remote sources. If this option is not set, the
# primary_hostname value is used for qualification.

#qualify_domain = estafeta.correo.es
qualify_domain = listas.correo.es

# If you want unqualified recipient addresses to be qualified with a different
# domain to unqualified sender addresses, specify the recipient domain here.
# If this option is not set, the qualify_domain value is used.

# qualify_recipient =


# The following line must be uncommented if you want Exim to recognize
# addresses of the form "user@[10.11.12.13]" that is, with a "domain literal"
# (an IP address) instead of a named domain. The RFCs still require this form,
# but it makes little sense to permit mail to be sent to specific hosts by
# their IP address in the modern Internet. This ancient format has been used
# by those seeking to abuse hosts by using them for unwanted relaying. If you
# really do want to support domain literals, uncomment the following line, and
# see also the "domain_literal" router below.

# allow_domain_literals


# No deliveries will ever be run under the uids of these users (a colon-
# separated list). An attempt to do so causes a panic error to be logged, and
# the delivery to be deferred. This is a paranoic safety catch. There is an
# even stronger safety catch in the form of the FIXED_NEVER_USERS setting
# in the configuration for building Exim. The list of users that it specifies
# is built into the binary, and cannot be changed. The option below just adds
# additional users to the list. The default for FIXED_NEVER_USERS is "root",
# but just to be absolutely sure, the default here is also "root".

# Note that the default setting means you cannot deliver mail addressed to root
# as if it were a normal user. This isn't usually a problem, as most sites have
# an alias for root that redirects such mail to a human administrator.

never_users = root


# The setting below causes Exim to do a reverse DNS lookup on all incoming
# IP calls, in order to get the true host name. If you feel this is too
# expensive, you can specify the networks for which a lookup is done, or
# remove the setting entirely.

#host_lookup = !192.168.0.0/16:*
#host_lookup = !*


# The settings below, which are actually the same as the defaults in the
# code, cause Exim to make RFC 1413 (ident) callbacks for all incoming SMTP
# calls. You can limit the hosts to which these calls are made, and/or change
```

```
# the timeout that is used. If you set the timeout to zero, all RFC 1413 calls
# are disabled. RFC 1413 calls are cheap and can provide useful information
# for tracing problem messages, but some hosts and firewalls have problems
# with them. This can result in a timeout instead of an immediate refused
# connection, leading to delays on starting up an SMTP session.

rfc1413_hosts = *
rfc1413_query_timeout = 0s


# By default, Exim expects all envelope addresses to be fully qualified, that
# is, they must contain both a local part and a domain. If you want to accept
# unqualified addresses (just a local part) from certain hosts, you can specify
# these hosts by setting one or both of
#
# sender_unqualified_hosts =
# recipient_unqualified_hosts =
#
# to control sender and recipient addresses, respectively. When this is done,
# unqualified addresses are qualified using the settings of qualify_domain
# and/or qualify_recipient (see above).


# If you want Exim to support the "percent hack" for certain domains,
# uncomment the following line and provide a list of domains. The "percent
# hack" is the feature by which mail addressed to x%y@z (where z is one of
# the domains listed) is locally rerouted to x@y and sent on. If z is not one
# of the "percent hack" domains, x%y is treated as an ordinary local part. This
# hack is rarely needed nowadays; you should not enable it unless you are sure
# that you really need it.
#
# percent_hack_domains =
#
# As well as setting this option you will also need to remove the test
# for local parts containing % in the ACL definition below.


# When Exim can neither deliver a message nor return it to sender, it "freezes"
# the delivery error message (aka "bounce message"). There are also other
# circumstances in which messages get frozen. They will stay on the queue for
# ever unless one of the following options is set.

# This option unfreezes frozen bounce messages after two days, tries
# once more to deliver them, and ignores any delivery failures.

ignore_bounce_errors_after = 2d

# This option cancels (removes) frozen messages that are older than a week.

timeout_frozen_after = 7d
smtp_accept_max = 200

# Para vacation
print_topbitchars = true

# El tamano por defecto de correos en exim es de 50MB
# message_size_limit = 50

#####################################################################
#                       ACL CONFIGURATION                           #
#         Specifies access control lists for incoming SMTP mail     #
#####################################################################

begin acl

# This access control list is used for every RCPT command in an incoming
# SMTP message. The tests are run in order until the address is either
```

```
# accepted or denied.

acl_check_rcpt:

  # Accept if the source is local SMTP (i.e. not over TCP/IP). We do this by
  # testing for an empty sending host field.

  accept  hosts = :

  ###############################################################################
  # The following section of the ACL is concerned with local parts that contain
  # @ or % or ! or / or | or dots in unusual places.
  #
  # The characters other than dots are rarely found in genuine local parts, but
  # are often tried by people looking to circumvent relaying restrictions.
  # Therefore, although they are valid in local parts, these rules lock them
  # out, as a precaution.
  #
  # Empty components (two dots in a row) are not valid in RFC 2822, but Exim
  # allows them because they have been encountered. (Consider local parts
  # constructed as "firstinitial.secondinitial.familyname" when applied to
  # someone like me, who has no second initial.) However, a local part starting
  # with a dot or containing /../ can cause trouble if it is used as part of a
  # file name (e.g. for a mailing list). This is also true for local parts that
  # contain slashes. A pipe symbol can also be troublesome if the local part is
  # incorporated unthinkingly into a shell command line.
  #
  # Two different rules are used. The first one is stricter, and is applied to
  # messages that are addressed to one of the local domains handled by this
  # host. It blocks local parts that begin with a dot or contain @ % ! / or |.
  # If you have local accounts that include these characters, you will have to
  # modify this rule.

  deny    message       = Restricted characters in address
          domains       = +local_domains
          local_parts   = ^[.] : ^.*[@%!/|]

  # The second rule applies to all other domains, and is less strict. This
  # allows your own users to send outgoing messages to sites that use slashes
  # and vertical bars in their local parts. It blocks local parts that begin
  # with a dot, slash, or vertical bar, but allows these characters within the
  # local part. However, the sequence /../ is barred. The use of @ % and ! is
  # blocked, as before. The motivation here is to prevent your users (or
  # your users' viruses) from mounting certain kinds of attack on remote sites.

  deny    message       = Restricted characters in address
          domains       = !+local_domains
          local_parts   = ^[./|] : ^.*[@%!] : ^.*/\\.\\./
  ###############################################################################

  # Accept mail to postmaster in any local domain, regardless of the source,
  # and without verifying the sender.

  accept  local_parts   = postmaster
          domains       = +local_domains

  # Deny unless the sender address can be verified.

  #require verify        = sender

  ###############################################################################
  # There are no checks on DNS "black" lists because the domains that contain
  # these lists are changing all the time. However, here are two examples of
  # how you could get Exim to perform a DNS black list lookup at this point.
  # The first one denies, while the second just warns.
  #
```

```
  # deny    message        = rejected because $sender_host_address is in a black
list at $dnslist_domain\n$dnslist_text
  #         dnslists      = black.list.example
  #
  # warn    message       = X-Warning: $sender_host_address is in a black list at
$dnslist_domain
  #         log_message   = found in $dnslist_domain
  #         dnslists      = black.list.example
  ##############################################################################

  # Accept if the address is in a local domain, but only if the recipient can
  # be verified. Otherwise deny. The "endpass" line is the border between
  # passing on to the next ACL statement (if tests above it fail) or denying
  # access (if tests below it fail).

  accept  domains       = +local_domains
          endpass
          verify        = recipient

  # Accept if the address is in a domain for which we are relaying, but again,
  # only if the recipient can be verified.

  accept  domains       = +relay_to_domains
          endpass
          verify        = recipient

  # If control reaches this point, the domain is neither in +local_domains
  # nor in +relay_to_domains.

  # Accept if the message comes from one of the hosts for which we are an
  # outgoing relay. Recipient verification is omitted here, because in many
  # cases the clients are dumb MUAs that don't cope well with SMTP error
  # responses. If you are actually relaying out from MTAs, you should probably
  # add recipient verification here.

  accept  hosts         = +relay_from_hosts

  # Accept if the message arrived over an authenticated connection, from
  # any host. Again, these messages are usually from MUAs, so recipient
  # verification is omitted.

  accept  authenticated = *

  # Reaching the end of the ACL causes a "deny", but we might as well give
  # an explicit message.

  deny    message       = relay not permitted


# These access control lists are used for content scanning with the exiscan-acl
# patch. You must also uncomment the entries for acl_smtp_data and acl_smtp_mime
#  (scroll up), otherwise the ACLs will not be used. IMPORTANT: the default
entries here
# should be treated as EXAMPLES. You MUST read the file doc/exiscan-acl-spec.txt
# to fully understand what you are doing ...

acl_check_mime:

  # Decode MIME parts to disk. This will support virus scanners later.
  #warn decode = default

  # File extension filtering.
  deny message = Blacklisted file extension detected
       condition = ${if match \
                           {${lc:$mime_filename}} \
                           {\N(\.exe|\.pif|\.bat|\.scr|\.lnk|\.com)$\N} \
                     {1}{0}}
```

```
  # Reject messages that carry chinese character sets.
  # WARNING: This is an EXAMPLE.
  deny message = Sorry, noone speaks chinese here
       condition = ${if eq{$mime_charset}{gb2312}{1}{0}}

  accept

acl_check_content:

  # Reject virus infested messages.
  deny  message = This message contains malware ($malware_name)
        #malware = *

  #  Always  add  X-Spam-Score  and  X-Spam-Report  headers,  using  SA  system-wide
settings
  # (user "nobody"), no matter if over threshold or not.
  warn  message = X-Spam-Score: $spam_score ($spam_bar)
        #spam = nobody:true
  warn  message = X-Spam-Report: $spam_report
        #spam = nobody:true

  # Add X-Spam-Flag if spam is over system-wide threshold
  warn message = X-Spam-Flag: YES
       #spam = nobody

  # Reject spam messages with score over 10, using an extra condition.
  deny  message = This message scored $spam_score points. Congratulations!
        #spam = nobody:true
        condition = ${if >{$spam_score_int}{100}{1}{0}}

  # finally accept all the rest
  accept


#############################################################################
#                       ROUTERS CONFIGURATION                               #
#                Specifies how addresses are handled                        #
#############################################################################
#     THE ORDER IN WHICH THE ROUTERS ARE DEFINED IS IMPORTANT!               #
# An address is passed to each router in turn until it is accepted.         #
#############################################################################

begin routers

# This router routes to remote hosts over SMTP by explicit IP address,
# when an email address is given in "domain literal" form, for example,
# <user@[192.168.35.64]>. The RFCs require this facility. However, it is
# little-known these days, and has been exploited by evil people seeking
# to abuse SMTP relays. Consequently it is commented out in the default
# configuration. If you uncomment this router, you also need to uncomment
# allow_domain_literals above, so that Exim can recognize the syntax of
# domain literal addresses.

# domain_literal:
#   driver = ipliteral
#   domains = ! +local_domains
#   transport = remote_smtp


# This router routes addresses that are not in local domains by doing a DNS
# lookup on the domain name. Any domain that resolves to 0.0.0.0 or to a
# loopback interface address (127.0.0.0/8) is treated as if it had no DNS
# entry. Note that 0.0.0.0 is the same as 0.0.0.0/32, which is commonly treated
# as the local host inside the network stack. It is not 0.0.0.0/0, the default
# route. If the DNS lookup fails, no further routers are tried because of
# the no_more setting, and consequently the address is unrouteable.
```

```
# Para reenviar a las estafetas los no locales

   send_to_gateway:
     driver = manualroute
     domains = !+local_domains
     transport = remote_smtp
     route_list = * virt_smtpin


# The remaining routers handle addresses in the local domain(s).


# This router handles aliasing using a linearly searched alias file with the
# name SYSTEM_ALIASES_FILE. When this configuration is installed automatically,
# the name gets inserted into this file from whatever is set in Exim's
# build-time configuration. The default path is the traditional /etc/aliases.
# If you install this configuration by hand, you need to specify the correct
# path in the "data" setting below.
#
##### NB  You must ensure that the alias file exists. It used to be the case
##### NB  that every Unix had that file, because it was the Sendmail default.
##### NB  These days, there are systems that don't have it. Your aliases
##### NB  file should at least contain an alias for "postmaster".
#
# If any of your aliases expand to pipes or files, you will need to set
# up a user and a group for these deliveries to run under. You can do
# this by uncommenting the "user" option below (changing the user name
# as appropriate) and adding a "group" option if necessary. Alternatively, you
# can specify "user" on the transports that are used. Note that the transports
# listed below are the same as are used for .forward files; you might want
# to set up different ones for pipe and file deliveries from aliases.

system_aliases:
  driver = redirect
  allow_fail
  allow_defer
  data = ${lookup{$local_part}lsearch{/etc/aliases}}
# user = exim
  file_transport = address_file
  pipe_transport = address_pipe
  user = vmail
  group = vmail


#localuser:
#  driver = accept
#  check_local_user
## local_part_suffix = +* : -*
## local_part_suffix_optional
#  transport = local_delivery
#  cannot_route_message = Unknown user


##########################################
#       ROUTERs PARA LISTAS:             #
##########################################

# Router para listas
#            Condicion: que exista entrada en el LDAP, AccountActive=TRUE y
mailMessageStore=/buzon/listas
# IMPORTANTE: las entradas en ldap de listas tienen, ademÃ¡s, "codCorreo: 2"
#
ldap_list_buzones:
  driver = manualroute
  condition = ${if eq {}{${lookup ldap { user="cn=mailuser,dc=correo,dc=es"
pass="p4ssw0rd"
```

```
ldaps://virt_ldap/idnc=usuarios,dc=correo,dc=es?mailMessageStore?sub?(&(mail=${lo
cal_part}@${domain})(AccountActive=TRUE)(mailMessageStore=/buzon/listas))}}}{no}{
yes}}
  retry_use_local_part
  transport = remote_smtp
  route_list = * virt_listas_smtp


########################################
#       ROUTERs PARA USUARIOS          #
########################################
ldapuser:
  driver = accept
  condition = ${if eq {}{${lookup ldap { user="cn=mailuser,dc=correo,dc=es"
pass="p4ssw0rd"
ldaps://virt_ldap/idnc=usuarios,dc=correo,dc=es?mailMessageStore?sub?(&(|(mail=${
local_part}@${domain})(mailAlternateAddress=${local_part}@${domain}))(objectclass
=person)(AccountActive=TRUE))}}}{no}{yes}}
# local_part_suffix = +* : -*
# local_part_suffix_optional
  transport = ldap_delivery_dovecot


################################################################################
####################
# IMPORTANTE: Debido a la necesidad de enviar a estafetas todo el correo de
salida, no se realiza
# ninguna comprobacion DNS de los dominios. Se deja a las estafetas que hagan la
comprobacion de DNS.
# Esta configuracion no permite generar correo BOUNCE en los buzones.
################################################################################
####################
   send_to_gateway_si_todo_falla:
     driver = manualroute
     domains = +local_domains
     transport = remote_smtp
     route_list = * virt_smtpin


#########################################################################
#                      TRANSPORTS CONFIGURATION                         #
#########################################################################
#                       ORDER DOES NOT MATTER                           #
#     Only one appropriate transport is called for each delivery.       #
#########################################################################

# A transport is used only when referenced from a router that successfully
# handles an address.

begin transports


# This transport is used for delivering messages over SMTP connections.

remote_smtp:
  driver = smtp

#
# transport para Entrega de correo
#

ldap_delivery_dovecot:
  driver = pipe
  command = /usr/local/dovecot/libexec/dovecot/deliver -d $local_part@$domain -f
$sender_address
  message_prefix =
  message_suffix =
  delivery_date_add
```

```
  envelope_to_add
  return_path_add
  log_output
  user = vmail
  group = vmail
  temp_errors = 64 : 69 : 70: 71 : 72 : 73 : 74 : 75 : 78

address_pipe:
  driver = pipe
  return_output


# This transport is used for handling deliveries directly to files that are
# generated by aliasing or forwarding.

address_file:
  driver = appendfile
  delivery_date_add
  envelope_to_add
  return_path_add


# This transport is used for handling autoreplies generated by the filtering
# option of the userforward router.

address_reply:
  driver = autoreply


# This transport is used to deliver local mail to cyrus IMAP server via UNIX
# socket.
#
#local_delivery:
#  driver = lmtp
#  command = "/usr/lib/cyrus-imapd/deliver -l"
#  batch_max = 20
#  user = cyrus


########################################################################
#                      RETRY CONFIGURATION                             #
########################################################################

begin retry

# This single retry rule applies to all domains and all errors. It specifies
# retries every 15 minutes for 2 hours, then increasing retry intervals,
# starting at 1 hour and increasing each time by a factor of 1.5, up to 16
# hours, then retries every 6 hours until 4 days have passed since the first
# failed delivery.
# PPIM -> Durante dos horas se reintenta cada 5 minutos, despues, empezando
# en 30 minutos incrementando con factor 1.5 (30m x 1.5 x i) hasta 16 horas
# y despues cada dos horas durante 4 dias.

# Address or Domain    Error       Retries
# -----------------    -----       -------
*                      quota
*                      *           F,2h,5m; G,16h,30m,1.5; F,4d,2h



########################################################################
#                      REWRITE CONFIGURATION                           #
########################################################################

# There are no rewriting specifications in this default configuration file.
```

```
begin rewrite



#############################################################################
#                     AUTHENTICATION CONFIGURATION                          #
#############################################################################

# There are no authenticator specifications in this default configuration file.

begin authenticators



#############################################################################
#                     CONFIGURATION FOR local_scan()                        #
#############################################################################

# If you have built Exim to include a local_scan() function that contains
# tables for private options, you can define those options here. Remember to
# uncomment the "begin" line. It is commented by default because it provokes
# an error with Exim binaries that are not built with LOCAL_SCAN_HAS_OPTIONS
# set in the Local/Makefile.

# begin local_scan

# End of Exim configuration file
```

E SYMPA

/etc/sympa.conf

```
###\\\\ Directories and file location ////###

## Directory containing mailing lists subdirectories
home    /home/sympa/list_data

## Directory for configuration files ; it also contains scenari/ and templates/
directories
etc     /home/sympa/etc

## File containing Sympa PID while running.
## Sympa also locks this file to ensure that it is not running more than once.
Caution : user sympa need to write access without special privilegee.
pidfile /home/sympa/sympa.pid

##
pidfile_distribute      /home/sympa/sympa-distribute.pid

##
pidfile_creation        /home/sympa/sympa-creation.pid

##
pidfile_bulk    /home/sympa/bulk.pid

## Umask used for file creation by Sympa
umask   027

## Directory containing available NLS catalogues (Message internationalization)
localedir       /home/sympa/locale

## The main spool containing various specialized spools
## All spool are created at runtime by sympa.pl
spool   /home/sympa/spool

## Incoming spool
queue   /home/sympa/spool/msg

## Bounce incoming spool
queuebounce     /home/sympa/spool/bounce

##
queuedistribute /home/sympa/spool/distribute

## Automatic list creation spool
queueautomatic  /home/sympa/spool/automatic

##
queuedigest     /home/sympa/spool/digest

##
queuemod        /home/sympa/spool/moderation

##
queuetopic      /home/sympa/spool/topic

##
queueauth       /home/sympa/spool/auth

##
queueoutgoing   /home/sympa/spool/outgoing

##
queuetask       /home/sympa/spool/task
```

```
##
queuesubscribe  /home/sympa/spool/subscribe

## URL to a virtual host.
http_host       listas.correo.es/wws

## The directory where Sympa stores static contents (CSS, members pictures,
documentation) directly delivered by Apache
static_content_path     /home/sympa/static_content

## The URL mapped with the static_content_path directory defined above
static_content_url      /static-sympa

###\\\\ Syslog ////###

## The syslog facility for sympa
## Do not forget to edit syslog.conf
syslog  LOCAL1

## Communication mode with syslogd is either unix (via Unix sockets) or inet (use
of UDP)
log_socket_type unix

## Log intensity
## 0 : normal, 2,3,4 for debug
log_level       0

##
log_smtp        off

## Number of months that elapse before a log is expired.
logs_expiration_period  1

###\\\\ General definition ////###

## Main robot hostname
domain  listas.correo.es

## Listmasters email list comma separated
## Sympa will associate listmaster privileges to these email addresses (mail and
web interfaces). Some error reports may also be sent to these addresses.
listmaster      listmaster@correo.es

## Local part of sympa email adresse
## Effective address will be \[EMAIL\]@\[HOST\]
email   sympa6

## Who is able to create lists
## This parameter is a scenario, check sympa documentation about scenarios if you
want to define one
create_list     public_listmaster

##
edit_list       owner

###\\\\ Tuning ////###

## Use of binary version of the list config structure on disk: none | binary_file
## Set this parameter to "binary_file" if you manage a big amount of lists
(1000+) ; it should make the web interface startup faster
cache_list_config       binary_file

## Sympa commands priority
sympa_priority  1

## Default priority for list messages
```

```
default_list_priority   5

## Default timeout between two scheduled synchronizations of list members with
data sources.
default_ttl     3600

## Default timeout between two action-triggered synchronizations of list members
with data sources.
default_distribution_ttl        300

## Default timeout while performing a fetch for an include_sql_query sync
default_sql_fetch_timeout       300

## Default priority for a packet to be sent by bulk.
sympa_packet_priority   5

##
request_priority        0

##
owner_priority  9

## The minimum number of packets in database before the bulk forks to increase
sending rate
bulk_fork_threshold     1

## The max number of bulks that will run on the same server.
bulk_max_count  3

## the number of seconds a slave bulk will remain running without processing a
message before it spontaneously dies.
bulk_lazytime   600

## The number of seconds a master bulk waits between two packets number checks.
## Keep it small if you expect brutal increases in the message sending load.
bulk_wait_to_fork       10

## the number of seconds a bulk sleeps between starting a new loop if it didn't
find a message to send.
## Keep it small if you want your server to be reactive.
bulk_sleep      1

## Secret used by Sympa to make MD5 fingerprint in web cookies secure
## Should not be changed ! May invalid all user password
cookie  1116017060

## If set to "on", enables support of legacy characters
legacy_character_support_feature        off

## The default maximum size (in bytes) for messages (can be re-defined for each
list)
max_size        5242880

## comma separated list of operations for which blacklist filter is applied
## Setting this parameter to "none" will hide the blacklist feature
use_blacklist   send,create_list

## Specify which rfc2369 mailing list headers to add
# was rfc2369_header_fields ARRAY(0x203d5c40)
rfc2369_header_fields   help,subscribe,unsubscribe,post,owner,archive

## Specify header fields to be removed before message distribution
# was remove_headers ARRAY(0x203d5d50)
remove_headers              X-Sympa-To,X-Family-To,Return-Receipt-To,Precedence,X-
Sequence,Disposition-Notification-To

## Reject mail from automates (crontab, etc) sent to a list?
```

```
reject_mail_from_automates_feature      on

##
bounce_warn_rate        30

##
bounce_halt_rate        50

###\\\\ Internationalization ////###

## Default lang (ca | cs | de | el | es | et_EE | en | fr | fi | hu | it | ja_JP
| ko | nl | nb_NO | oc | pl | pt_BR | ru | sv | tr | vi | zh_CN | zh_TW)
## This is the default language used by Sympa
lang    es

## Supported languages
## This is the set of language that will be proposed to your users for the Sympa
GUI. Don't select a language if you don't have the proper locale packages
installed.
supported_lang
ca,cs,de,el,es,et_EE,en_US,fr,fi,hu,it,ja_JP,ko,nl,nb_NO,oc,pl,pt_BR,ru,sv,tr,vi,
zh_CN,zh_TW

###\\\\ Errors management ////###

## Bouncing email rate for warn list owner
bounce_warn_rate        30

## Bouncing email rate for halt the list (not implemented)
## Not yet used in current version, Default is 50
bounce_halt_rate        50

## Task name for expiration of old bounces
expire_bounce_task      daily

## Welcome message return-path
## If set to unique, new subcriber is removed if welcome message bounce
welcome_return_path     owner

## Remind message return-path
## If set to unique, subcriber is removed if remind message bounce, use with care
remind_return_path      owner

###\\\\ MTA related ////###

## Path to the MTA (sendmail, postfix, exim or qmail)
## should point to a sendmail-compatible binary (eg: a binary named "sendmail" is
distributed with Postfix)
sendmail        /usr/sbin/exim

## Maximum number of recipients per call to Sendmail. The nrcpt_by_domain.conf
file allows a different tuning per destination domain.
nrcpt   10

## Max. number of different domains per call to Sendmail
avg     10

## Max. number of Sendmail processes (launched by Sympa) running simultaneously
## Proposed value is quite low, you can rise it up to 100, 200 or even 300 with
powerfull systems.
maxsmtp 10

###\\\\ Plugin ////###

## Path to the antivirus scanner engine
## supported antivirus : McAfee/uvscan, Fsecure/fsav, Sophos, AVP and Trend
Micro/VirusWall
```

```
# antivirus_path        /usr/local/uvscan/uvscan

## Antivirus pluggin command argument
# antivirus_args        --secure --summary --dat /usr/local/uvscan

###\\\\ DKIM ////###

##
dkim_feature    off

##
## Insert a DKIM signature to message from the robot, from the list or both
dkim_add_signature_to   robot,list

###\\\\ S/MIME pluggin ////###

## Path to OpenSSL
## Sympa knowns S/MIME if openssl is installed
# openssl       /usr/bin/ssl

## The directory path use by OpenSSL for trusted CA certificates
# capath        /home/sympa/etc/ssl.crt

##    This  parameter  sets  the  all-in-one  file  where  you  can  assemble  the
Certificates of Certification Authorities (CA)
cafile  /home/sympa/default/ca-bundle.crt

## User CERTs directory
ssl_cert_dir    /home/sympa/list_data/X509-user-certs

##
crl_dir /home/sympa/list_data/crl

## Password used to crypt lists private keys
# key_passwd    your_password

###\\\\ Database ////###

## Database type (mysql | Pg | Oracle | Sybase | SQLite)
## be carefull to the case
db_type mysql

## Name of the database
## with SQLite, the name of the DB corresponds to the DB file
db_name sympa61

## The host hosting your sympa database
db_host serv_mysql

## The database port
db_port 3306

## Database user for connexion
db_user sympa

## Database password (associated to the db_user)
## Whatever you use a password or not, you must protect the SQL server (is it a
not a public internet service ?)
db_passwd       d3ud1s4n

## Database private extention to user table
## You need to extend the database format with these fields
# db_additional_user_fields     age,address

## Database private extention to subscriber table
## You need to extend the database format with these fields
# db_additional_subscriber_fields       billing_delay,subscription_expiration
```

```
###\\\\ Web interface ////###

## Sympa's main page URL
wwsympa_url     https://listas.correo.es/wws

## Messages are supposed to be filtered by an antispam that add one more headers
to messages. This parameter is used to select a special scenario in order to
decide the message spam status : ham, spam or unsure. This parameter replace
antispam_tag_header_name,           antispam_tag_header_spam_regexp           and
antispam_tag_header_ham_regexp.
spam_status     x-spam-status

## If a spam filter (like spamassassin or j-chkmail) add a smtp headers to tag
spams, name of this header (example X-Spam-Status)
antispam_tag_header_name        X-Spam-Status

## The regexp applied on this header to verify message is a spam (example \s*Yes)
antispam_tag_header_spam_regexp ^\s*Yes

## The regexp applied on this header to verify message is NOT a spam (example
\s*No)
antispam_tag_header_ham_regexp  ^\s*No

##
max_wrong_password      19

###\\\\ LDAP ALIAS MANAGER ////###
alias_manager /home/sympa/bin/ldap_alias_manager.pl
```

/etc/wwsympa.conf

```
###\\\\ Directories and file location ////###

## File containing archived PID while running.
archived_pidfile        /home/sympa/archived.pid

## File containing bounced PID while running.
bounced_pidfile /home/sympa/bounced.pid

## File containing task_manager PID while running.
task_manager_pidfile    /home/sympa/task_manager.pid

## Where to store HTML archives
## Better if not in a critical partition
arc_path        /home/sympa/arc

## Where to store bounces
## Better if not in a critical partition
bounce_path     /home/sympa/bounce

###\\\\ Syslog ////###

## The syslog facility for wwsympa, archived and bounced
## default is to use previously defined sympa log facility
log_facility    LOCAL2

###\\\\ General definition ////###

###\\\\ Tuning ////###

## Password case (insensitive | sensitive)
## Should not be changed ! May invalid all user password
password_case   insensitive

## HTTP cookies lifetime
```

```
cookie_expire   0

## HTTP cookies validity domain
cookie_domain   localhost

###\\\\ Internationalization ////###

###\\\\ Errors management ////###

###\\\\ MTA related ////###

###\\\\ Plugin ////###

## Path to MhOnarc mail2html pluggin
## This is required for HTML mail archiving
mhonarc /usr/bin/mhonarc

###\\\\ DKIM ////###

###\\\\ S/MIME pluggin ////###

###\\\\ Database ////###

###\\\\ Web interface ////###

## Is fast_cgi module for Apache (or Roxen) installed (0 | 1)
## This module provide much faster web interface
use_fast_cgi    1

## Title of main web page
title   Listas Generales

## Main page type (lists | home)
default_home    home
```

F POSTFIX

/etc/postfix/main.cf

```
##############################################################################
# Propio de la instalacion de Postfix
##############################################################################

queue_directory = /var/spool/postfix

command_directory = /usr/sbin

daemon_directory = /usr/libexec/postfix

mail_owner = postfix

##############################################################################
# PARAMETROS PRINCIPALES LOCALES
##############################################################################

myorigin = estafeta.correo.es

recipient_canonical_maps = hash:/etc/postfix/recipient_canonical
sender_canonical_maps = hash:/etc/postfix/sender_canonical

myhostname = estafeta.correo.es

mydomain = estafeta.correo.es

mydestination = /etc/postfix/dominiosLocales

local_recipient_maps = ldap:/etc/postfix/validUser.cf $alias_maps

local_transport = smtp:[192.168.100.203]:25

unknown_local_recipient_reject_code = 550

mynetworks_style = subnet

mynetworks = 127.0.0.0/8

relayhost=[ironport.correo.es]

##############################################################################
# OTROS
##############################################################################

smtpd_banner = Bienvenido a SMTP CORREO Mail Server

#debug_peer_level = 2
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5


sendmail_path = /usr/sbin/sendmail.postfix

newaliases_path = /usr/bin/newaliases.postfix

mailq_path = /usr/bin/mailq.postfix

setgid_group = postdrop

html_directory = /usr/share/doc/postfix-2.8.1-documentation/html

manpage_directory = /usr/share/man
```

```
sample_directory = /etc/postfix

readme_directory = /usr/share/doc/postfix-2.8.1-documentation/readme

alias_database = hash:/etc/postfix/aliases
alias_maps = hash:/etc/postfix/aliases

################################################################################
# SUPLANTACION DE IDENTIDAD
################################################################################
# Para evitar la suplantacion de identidad
smtpd_sender_login_maps = ldap:matchlogin

matchlogin_server_host = ldaps://virt_ldap
matchlogin_version = 3
matchlogin_server_port = 636
matchlogin_timeout = 10
matchlogin_bind = yes
matchlogin_search_base = idnc=usuarios,dc=correo,dc=es
matchlogin_bind_dn = cn=mailuser,dc=correo,dc=es
matchlogin_bind_pw = p4ssw0rd

matchlogin_scope = sub
# %s es el mail de origen (mail from)
matchlogin_query_filter = (|(mail=%s)(mailAlternateAddress=%s))
# compara la uid al que pertenece el mail from con el login sasl
matchlogin_result_attribute = uid

################################################################################
# ENVIO AUTENTICADO - SASL
################################################################################

smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
broken_sasl_auth_clients = yes

################################################################################
# USO TLS - Comunicaciones cifradas
################################################################################
smtpd_use_tls = yes
smtp_tls_security_level = may
smtp_tls_loglevel = 1
smtpd_tls_key_file = /certificados/estafeta_nopass.pem
smtpd_tls_cert_file = /certificados/estafeta.crt
smtpd_tls_CAfile = /certificados/TERENASSLCA.crt
tls_random_source = dev:/dev/urandom
smtpd_timeout = 300s
smtpd_recipient_limit = 100
smtpd_recipient_overshoot_limit = 100
data_directory = /var/lib/postfix
inet_protocols = ipv4

################################################################################
# RESTRICCIONES DE ENVIO
################################################################################
mailbox_size_limit = 0

message_size_limit = 30000000

maximal_queue_lifetime = 5d

################################################################################
# TRANSPORTs
################################################################################
transport_maps             =            ldap:/etc/postfix/ldapListasTransport.cf,
ldap:/etc/postfix/ldapUsuariosLocalesTransport.cf, hash:/etc/postfix/transport
```

```
##############################################################################
# RESTRICCIONES - GENERALES
##############################################################################
smtpd_delay_reject = yes
smtpd_helo_required = yes
disable_vrfy_command = yes

##############################################################################
# RESTRICCIONES - CLIENT
#  Se aplican cuando se produce la conexion
##############################################################################
smtpd_client_restrictions   =   check_client_access   hash:/etc/postfix/emisores-
prohibidos

##############################################################################
# RESTRICCIONES - MAIL FROM
#  Se aplican en el paso del protocolo smtp: "mail from"
##############################################################################
smtpd_sender_restrictions   =   check_sender_access   hash:/etc/postfix/emisores-
prohibidos

##############################################################################
# RESTRICCIONES - RCPT TO
#  Se aplican en el paso del protocolo smtp: "rctp to"
##############################################################################
smtpd_recipient_restrictions = reject_unauth_pipelining,
                               reject_non_fqdn_sender,
                               reject_non_fqdn_recipient,
                               reject_unknown_sender_domain,
                               reject_unknown_recipient_domain,
                               permit_mynetworks,
                               reject_sender_login_mismatch,
                               permit_sasl_authenticated,
                               reject_unauth_destination
```

/etc/postfix/master.cf

```
#
# Postfix master process configuration file.  For details on the format
# of the file, see the Postfix master(5) manual page.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -     smtpd
submission inet n      -       n       -       -       smtpd
        -o smtpd_tls_security_level=encrypt
        -o smtpd_sasl_auth_enable=yes
#       -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#       -o milter_macro_daemon_name=ORIGINATING
#
#       -o smtpd_etrn_restrictions=reject
#       -o smtpd_client_restrictions=permit_sasl_authenticated,reject
smtps    inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
#628      inet  n       -       n       -       -       qmqpd
pickup    fifo  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       n       -       0       bounce
```

```
defer     unix  -       -       n       -       0       bounce
trace     unix  -       -       n       -       0       bounce
verify    unix  -       -       n       -       1       verify
flush     unix  n       -       n       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
smtp      unix  -       -       n       -       -       smtp
# When relaying mail as backup MX, disable fallback_relay to avoid MX loops
relay     unix  -       -       n       -       -       smtp
#       -o fallback_relay=
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
discard   unix  -       -       n       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       n       -       1       anvil
scache    unix  -       -       n       -       1       scache
#
# ====================================================================
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent.  See the pipe(8) man page for information about ${recipient}
# and other message envelope options.
# ====================================================================
#
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${recipient}
#
# The Cyrus deliver program has changed incompatibly, multiple times.
#
old-cyrus unix  -       n       n       -       -       pipe
  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
# Cyrus 2.1.5 (Amos Gouaux)
# Also specify in main.cf: cyrus_destination_recipient_limit=1
cyrus     unix  -       n       n       -       -       pipe
  user=cyrus argv=/cyrus/bin/deliver -e -r ${sender} -m ${extension} ${user}
#
# See the Postfix UUCP_README file for configuration details.
#
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu  user=uucp  argv=uux  -r  -n  -z  -a$sender  -  $nexthop!rmail.postfix
($recipient)
#
# Other external delivery methods.
#
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=foo argv=/usr/local/sbin/bsmtp -f $sender $nexthop $recipient

retry     unix  -       -       n       -       -       error
proxywrite unix -       -       n       -       1       proxymap
#smtp      inet  n       -       n       -       1       postscreen
#smtpd     pass  -       -       n       -       -       smtpd
#dnsblog   unix  -       -       n       -       0       dnsblog
#tlsproxy  unix  -       -       n       -       0       tlsproxy
```

/etc/postfix/validUser.cf

```
server_host = ldaps://virt_ldap:636
server_base = idnc=usuarios,dc=correo,dc=es
```

```
search_base = idnc=usuarios,dc=correo,dc=es
ssl = yes
tls = no
bind = yes
version = 3
bind_dn = cn=mailuser,dc=correo,dc=es
bind_pw = p4ssw0rd
query_filter = (&(|(mail=%s)(mailalternateaddress=%s))(accountActive=TRUE))
result_attribute = uid
```

/etc/postfix/ldapListasTransport.cf

```
server_host = ldaps://virt_ldap:636
server_base = idnc=usuarios,dc=correo,dc=es
search_base = idnc=usuarios,dc=correo,dc=es
ssl = yes
tls = no
bind = yes
version = 3
bind_dn = cn=mailuser,dc=correo,dc=es
bind_pw = p4ssw0rd
query_filter = (&(mail=%s)(accountActive=TRUE)(mailMessageStore=/buzon/listas))
result_attribute = uid
result_filter = smtp:[ironport.correo.es]
```

/etc/postfix/ldapUsuariosLocalesTransport.cf

```
server_host = ldaps://virt_ldap:636
server_base = idnc=usuarios,dc=correo,dc=es
search_base = idnc=usuarios,dc=correo,dc=es
ssl = yes
tls = no
bind = yes
version = 3
bind_dn = cn=mailuser,dc=correo,dc=es
bind_pw = p4ssw0rd
query_filter = (&(|(mail=%s)(mailalternateaddress=%s))(accountActive=TRUE))
result_attribute = uid
result_filter = smtp:[ironport.correo.es]
```

G MySQL

/etc/my.cnf

```
# MySQL config file for very large systems.
#
# The following options will be passed to all MySQL clients
[client]
port            = 3306
socket          = /tmp/mysql.sock

# Here follows entries for some specific programs

# The MySQL server
[mysqld]
port            = 3306
socket          = /tmp/mysql.sock
skip-locking
key_buffer = 128M
max_allowed_packet = 16M
table_cache = 512
sort_buffer_size = 2M
read_buffer_size = 512K
read_rnd_buffer_size = 8M
myisam_sort_buffer_size = 64M
thread_cache_size = 8
query_cache_size = 128M
thread_concurrency = 8
query_cache_limit= 2M
max_connections = 1000
max_connect_errors = 1000
expire_logs_days = 60

join_buffer_size = 256K
low_priority_updates = 1
max_heap_table_size = 32M

# Registro logs
log-error
log-warnings
# Log Slow Queries
log-slow-queries=/var/mysql-log-slow-queries

# Replication Master Server (default)
# binary logging is required for replication
log-bin=mysql-bin

# required unique id between 1 and 2^32 - 1
# defaults to 1 if master-host is not set
# but will not function as a master if omitted
server-id       = 2

#skip-slave-start

# Replication Slave

master-host=bbdd1
master-user=replica
master-password=p4ssw0rd1
master-port=3306

auto_increment_increment= 2
auto_increment_offset= 2

[mysqldump]
quick
max_allowed_packet = 16M
```

```
[mysql]
no-auto-rehash

[isamchk]
key_buffer = 256M
sort_buffer_size = 256M
read_buffer = 2M
write_buffer = 2M

[myisamchk]
key_buffer = 256M
sort_buffer_size = 256M
read_buffer = 2M
write_buffer = 2M

[mysqlhotcopy]
interactive-timeout
```

H OpenLDAP

/etc/openldap/slapd.conf

```
# Allow LDAPv2 binds:
allow bind_v2

# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

# Schema and objectClass definitions
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/copa.schema
include         /etc/openldap/schema/iris.schema
include         /etc/openldap/schema/correonbdc.schema
include         /etc/openldap/schema/correopolicy.schema
include         /etc/openldap/schema/correo.schema
include         /etc/openldap/schema/correomail.schema
include         /etc/openldap/schema/catre.schema
include         /etc/openldap/schema/openCA.schema
include         /etc/openldap/schema/krb5-kdc.schema
include         /etc/openldap/schema/postfix.schema
include         /etc/openldap/schema/sendmail.schema
include         /etc/openldap/schema/qmail.schema
include         /etc/openldap/schema/phamm.schema

#include         /etc/openldap/access.confc

#include         /etc/openldap/pre-access.acl

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck     on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd.args

# Read slapd.conf(5) for possible values
loglevel       512

# Password format in LDAP (Default: {SMD5})
password-hash   {CLEARTEXT}

# TLS

TLSVerifyClient never
TLSCACertificateFile  /etc/openldap/ssl/cacert.pem
TLSCertificateFile    /etc/openldap/ssl/bbdd-cert.pem
TLSCertificateKeyFile /etc/openldap/ssl/bbdd-key.pem

# Disable access methods (Default: none)
# disallow bind_simple

# Enable sizelimit
sizelimit 32000

#######################################################################
# ldbm database definitions
#######################################################################

# The backend type
```

```
database        bdb
suffix          "dc=correo,dc=es"
rootdn          "cn=Replication,dc=correo,dc=es"
rootpw          p4ssw0rd2
directory       /var/lib/ldap
checkpoint      512     720

index   objectClass                             eq,pres
index   cn,givenname                            eq,subinitial
index   mail                                    eq,sub
index   vd,mailDelete                               eq,pres
index   accountActive                           eq,pres
index   mailAlternateAddress                    eq
index   mailforwardingaddress                    eq
index   sn                                      pres,eq,sub
index   uid                                     eq
index   mailMessageStore                        eq
#index  modifyTimestamp                         eq

# Save the time that the entry gets modified
lastmod         on

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below

#include /etc/openldap/access.conf

updatedn "cn=Replication,dc=correo,dc=es"
updateref ldaps://ldap_maestro:636
idletimeout 660
```

I Open-Xchange

/etc/httpd/conf.d/proxy_ajp.conf

```
<Location /servlet/axis2/services>
    # restrict access to the soap provisioning API
    Order Deny,Allow
    Deny from all
    Allow from 127.0.0.1 192.168.1
    # you might add more ip addresses / networks here
    # Allow from 192.168 10 172.16
</Location>

LoadModule proxy_ajp_module modules/mod_proxy_ajp.so

<IfModule mod_proxy_ajp.c>
   ProxyRequests Off

   <Proxy balancer://oxcluster>
       Order deny,allow
       Allow from all
       # multiple server setups need to have the hostname inserted instead
localhost
       BalancerMember ajp://localhost:8009 timeout=100 smax=0 ttl=60 retry=60
loadfactor=50 route=OX1
       # Enable and maybe add additional hosts running OX here
       # BalancerMember ajp://oxhost2:8009 timeout=100  smax=0 ttl=60 retry=60
loadfactor=50 route=OX2
      ProxySet stickysession=JSESSIONID|jsessionid scolonpathdelim=On

   </Proxy>

   # OX frontend
   <Proxy /ajax>
       ProxyPass balancer://oxcluster/ajax
   </Proxy>
   <Proxy /servlet>
       ProxyPass balancer://oxcluster/servlet
   </Proxy>
   <Proxy /infostore>
       ProxyPass balancer://oxcluster/infostore
   </Proxy>
   <Proxy /publications>
       ProxyPass balancer://oxcluster/publications
   </Proxy>
   # USM
   <Proxy /usm-json>
       ProxyPass balancer://oxcluster/usm-json
   </Proxy>
   # SOAP
   <Proxy /webservices>
       ProxyPass balancer://oxcluster/webservices
  </Proxy>

   # OXtender
   <Proxy /Microsoft-Server-ActiveSync>
       ProxyPass balancer://oxcluster/Microsoft-Server-ActiveSync
   </Proxy>
</IfModule>
```

/etc/httpd/conf.d/ox.conf

```
<VirtualHost *:80>
       ServerAdmin webmaster@localhost

       DocumentRoot /var/www/html/
       <Directory /var/www/html/>
              AllowOverride None
```

```
             Order allow,deny
             allow from all
             RedirectMatch ^/$ /ox6/
               Options +FollowSymLinks +SymLinksIfOwnerMatch
      </Directory>
       # deflate
     AddOutputFilterByType   DEFLATE   text/html   text/plain   text/javascript
application/javascript text/css text/xml application/xml text/x-js application/x-
javascript

      # pre-compressed files
      AddType text/javascript .jsz
      AddType text/css .cssz
      AddType text/xml .xmlz
       AddType text/plain .po

      AddEncoding gzip .jsz .cssz .xmlz
      SetEnvIf Request_URI "\.(jsz|cssz|xmlz)$" no-gzip

      ExpiresActive On

      <Location /ox6>
              # Expires (via ExpiresByType to override global settings)
              ExpiresByType image/gif "access plus 6 months"
              ExpiresByType image/png "access plus 6 months"
              ExpiresByType image/jpg "access plus 6 months"
              ExpiresByType image/jpeg "access plus 6 months"
              ExpiresByType text/css "access plus 6 months"
              ExpiresByType text/html "access plus 6 months"
              ExpiresByType text/xml "access plus 6 months"
              ExpiresByType text/javascript "access plus 6 months"
              ExpiresByType text/x-js "access plus 6 months"
              ExpiresByType application/x-javascript "access plus 6 months"
              ExpiresDefault "access plus 6 months"
              Header append Cache-Control "private"
              Header unset Last-Modified
              Header unset Vary
              # Strip version
              RewriteEngine On
              RewriteRule v=\w+/(.+) $1 [L]
              # Turn off ETag
              Header unset ETag
              FileETag None
      </Location>

      <Location /ox6/ox.html>
              ExpiresByType text/html "now"
              ExpiresDefault "now"
              Header unset Last-Modified
              Header  set  Cache-Control  "no-store,  no-cache,  must-revalidate,
post-check=0, pre-check=0"
              # Turn off ETag
              Header unset ETag
              FileETag None
      </Location>

      <Location /ox6/index.html>
              ExpiresByType text/html "now"
              ExpiresDefault "now"
              Header unset Last-Modified
              Header  set  Cache-Control  "no-store,  no-cache,  must-revalidate,
post-check=0, pre-check=0"
              # Turn off ETag
              Header unset ETag
              FileETag None
      </Location>
</VirtualHost>
```

PRESUPUESTO

El presente presupuesto contempla el trabajo de investigación de las soluciones de infraestructura, su desglose, suministro y despliegue, así como todas las tareas relativas a la instalación, configuración, pruebas y puesta en marcha con las necesidades de recursos humanos y técncos con suficiente cualificación técnica para su ejecución en el plazo exigido de 90 días.
Las tareas posteriores, relativas a migraciones, soporte, formación y mantenimiento serán ejecutadas por la empresa subcontratista correspondiente.

1) Ejecución Material

- IBM BladeCenter E Chassis..... 3.190 €
- 14 x IBM BladeCenter HS20 (184€ x 14)..... 2.576 €
- 2 x Nortel Networks Layer 2-7 GbE Switch Module (7.472 x 2)..... 14.944 €
- 4 x Bandejas Disco NetApp DS2246 (26.653€ x 4)..... 106.612 €
- 2 x Controladoras NetApp FAS2220A (4.110€ x 2)..... 8.220 €
- 4 x Cisco Ironport C360 Appliance (29.950€ x 4)..... 119.800 €
- Material Auxliar de Conectividad (cables, conectores, etc.)..... 2.500 €
- **Total de ejecución material ..... 257.842 €**

2) Gastos generales

- 5 % sobre Ejecución Material..... 12.892 €

3) Honorarios Proyecto

- Instalación Hardware (80 horas / técnico x 75€ / hora)..... 6.000 €
- Configuración Sistema (40 horas / técnico x 75€ / hora)..... 3.000 €
- Desarrollo e Implementación (160 horas / técnico x 75€ / hora)..... 12.000 €
- Pruebas y Validación (40 horas / técnico x 75€ / hora)..... 3.000 €
- Puesta en marcha (40 horas / ténico x 75€ / hora)..... 3.000 €
- Dirección de proyecto (10 % s/servicios)..... 2.700 €
- **Total Honorarios..... 29.700 €**

4) Subtotal del presupuesto

- Subtotal Presupuesto..... **300.434 €**

5) I.V.A. aplicable

- 21% Subtotal Presupuesto ..... 63.091 €

6) Total presupuesto

- Total Presupuesto..... **363.525 €**

Madrid, Noviembre de 2013
El Ingeniero Jefe de Proyecto

Fdo.: Héctor Moreno Blanco
Ingeniero Superior de Telecomunicación

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Este documento contiene las condiciones técnicas que guiarán la realización, en este proyecto, de una Plataforma de Correo Electrónico con Sincronización de Elementos PIM mediante Servidor Funambol. Se pretende la implantación de un sistema basado en software GNU, adaptado al directorio corporativo (OpenLDAP) y con sincronización de elementos personales (calendario, contactos, tareas, etc.) con diferentes dispositivos.

En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de diseñar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Situación Actual

La entidad dispone actualmente de un servicio de Correo Electrónico Corporativo que lleva operativo desde 2001 y que tiene las siguientes características: es un sistema redundante, en alta disponibilidad, que consta de un servidor Netscape Messaging Server 4.15, sobre sistema operativo Solaris 8, en un clúster de dos máquinas SUN, con unas 1200 cuentas POP3.

En los servidores de correo existe un sistema antivirus basado en Wall de Trend Micro. La administración del sistema se realiza desde una única consola.

Entorno Tecnlógico

El parque informático sobre el que el sistema de correo debe operar es heterogéneo, con una inmensa mayoría de clientes estándar en entornos Windows (con clientes Outlook y Outlook Express), MAC y un pequeño número de clientes basados en entornos Linux/Solaris (con clientes Mozzilla, NetScape, Evolution, etc). Los clientes disponen además de cliente LDAP para la búsqueda de direcciones de correo de la entidad.

Alcance del Proyecto

Como resultado de este Proyecto se pretende obtener:

1. Una plataforma de correo electrónico basado en software GNU (gratuito), sobre sistema operativo Red Hat o distribuciones similares.
2. Servicio de sincronización de elementos personales para los usuarios.

Es decir, el Proyecto comprende el suministro, diseño, instalación, configuración, documentación y puesta en marcha de la nueva plataforma de correo electrónico, así como la formación del personal seleccionado por la entidad.

Condiciones generales

En detalle, se pretende:

- **Renovación de equipamiento**: suministro, instalación y configuración del equipamiento hardware, suficientemente dimensionado, con fuentes de

alimentación redundantes de suministrode energía independiente. El equipamiento deberá ser entregado en un tiempo inferior a 30 días a partir de la firma del contrato. Nuevo almacenamiento eficiente y fiable para las cuentas de usuario.

- **Servicios de instalación y configuración**: Integración, configuración y conexión de los equipos a la red de la entidad en sus instalaciones (la infraestructura de red y conectividad entre las diferentes delegaciones y la sede central, responsabilidad de la entidad, se consideran suficientes para la correcta implantación del servicio). Instalación en el *rack* de todos los equipos. Diseño y pruebas del sistema de cliente de correo Outlook, Eudora, Evolution, Thunderbird, Apple Mail y dispositivos móviles (iPhone, Android, BlackBerry, Windows Mobile). Se valorará especialmente el uso de software libre para todo tipo de herramientas auxiliares que se utilicen en la solución ofertada.

Estas tareas deberán realizarse en un tiempo inferior a 90 días a partir de la firma del contrato.

Documentación y Formación

Formación para el personal de la entidad (para Administración y Operación). Se pide un mínimo de 25 horas de formación grupal.Se valorará la oferta de un mayor número de horas de formación, que se deberá realizar en las fechas propuestas por la entidad, una vez que esté operativo el nuevo sistema.

Gestión de las Garantías

El equipamiento, HW y SW, así como los trabajos realizados para la implantación del sistema deberá disponer de garantía de 3 años. Es requisito obligatorio de obligado cumplimiento.En caso de prorrogarse el contrato, se requiere la gestión de las garantías con los fabricantes durante el tiempo de duración del contrato siendo los costes de la extensión de garantía de su cuenta.

Caracterísitcas del nuevo Sistema de Correo

Las características de la nueva plataforma de correo deberán ser, preferentemente como sigue:

- Se valorará especialmente el uso de software libre para todo tipo de herramientas auxiliares que se utilicenen la solución ofertada.
- Plataforma instalada sobre Linux, usando Open Source. Sistemas operativos preferidos: Red Hat y distribuciónes similares.
- Intercambio de información entre aplicaciones ante el evento de la recepción de un mensaje de correo en una de ellas. Dichas aplicaciones se ejecutan en entornos UNIX/Linux.
- Integración de la base de datos de usuarios con el directorio OpenLDAP de la entidad y otros servicios (DNS, NTP, etc.)
- Entorno de alta disponibilidad.

- Servicio de correo accesible a través de IMAP4, POP3 y Webmail. Estos protocolos deben poder configurarse en modo seguro y que debe haber autenticación en el servidor tanto para consulta/descarga de correo como para su envío.
- Posiblidad de autenticación para el envío por SMTP.
- Cuentas de usuario a gestionar: como mínimo 10000.

Seguridad

El sistema debe estar protegido ante ataques de SPAM, denegación de servicios o de cualquier tipo de intrusión no autorizada (fraude, virus… tanto para correo interno como externo).

Arquitectura

El sistema precisa de dos servidores *relay* que estarán ubicados en la DMZ y cuatro servidores de correo protegidos por un cortafuegos. Todos los sistemas en alta disponibilidad y suficientemente dimensionados.

Equipamiento

- **Servidores**: se requiere que el sistema funcione en alta disponibilidad, suficientemente dimensionado para gestionar mínimo 10000 cuentas de correo. En caso de que en un plazo de seis meses a partir de la puesta en marcha del sistema se constate que las prestaciones de los equipos no son suficientes, el adjudicatario procederá a potenciar éstas o sustituir los equipos necesarios por otros más adecuados.
- **Almacenamiento**: Se deberá ofrecer un sistema de almacenamiento eficaz y fiable para albergar mínimo 10000 cuentas de correo de 6Gb de capacidad. Se valorará que dicho sistema buen rendimiento en operaciones de lectura y escritura, requerido para un sistema de correo electrónico.
- **Sistema antivirus y anti-SPAM:** se requiere que todo el flujo de correo de la plataforma, tanto entrante como saliente, esté protegido de ataques de virus y SPAM. Se valorará una solución de software GNU.
- **Armario (*rack*) y accesorios:** Para instalar adecuadamente los equipos del sistema de correo en el CPD de la entidad, se deberá ofertar un armario con las características adecuadas para tal fin, así como los accesorios suficientes para la correcta instalación de los equipos.

Tareas a realizar

Se realizarán las tareas propias para la correcta integración, configuración y conexión del equipamiento ofertado a la red de la entidad en sus instalaciones. Igualmente, se instalará todo el software ofertado en los equipos propuestos. Las ofertas incluirán detalles sobre la propuesta de instalación de los siguientes elementos:

- Servidores en configuración de alta disponibilidad y con posibilidad de incorporar más máquinas por razones de escalabilidad en caso de ser necesario. Los modelos

de servidor incluirán sus características para cubrir necesidades mínimas y su posible crecimiento.

- Sistema operativo, versión y posibles extras.
- Almacenamiento de los buzones en red.
- Servidor de SMTP. Preferentemente Postfix o similar.
- Servidor IMAP/POP3. Preferiblemente Courier o similar.
- Servidor Webmail. Preferiblemente Horde u OpenXchange o similar.
- Filtrado de correos. Preferiblemente ClamAV y DSPAM.
- Configuración de alta disponibilidad.

Servicios de Valor Añadido

El adjudicatario podrá ofrecer los siguientes servicios, los cuales serán convenientemente valorados, reservándose la entidad el derecho de su implementación:

- Sistema de listas de distribución como complemento para la arquitectura de correo.
- Tecnología de virtualización, cuyos objetivos serían: disponer de copias de seguridad de los servidores, homogeneidad en la instalación en todos los nodos del clúster o preparación para la tendencia actual a la nube.
- Colaboración en grupo: adaptación de herramientas de colaboraciónen grupo (por ejemplo Zimbra) para uso compartido de agendas, calendarios y documentación.
- Sistema de sincronización de elementos personales PIM con diferentes dispositivos y clientes software (por ejemplo Funambol).

Presupuesto

La oferta económica deberá incluir, además del importe total de la oferta, el presupuesto pormenorizado de todos los elementos incluidos (requisito de obligado cumplimiento). En particular:

1. Coste del equipamiento:
    a. Coste detallado de todo el hardware ofertado (servidores).
    b. Coste de las licencias y suscripciones del software ofertado, en su caso.
    c. Coste del armario (*rack*), accesorios, cables y tarjetas, para la instalación de todo el hardware.
2. Coste de los servicios de instalación, configuración y pruebas.
3. Coste de la elaboración de la documentación y formación:
    a. Redacción de Documentación y normativa.
    b. Formación técnica sobre la arquitectura.