TFC – Plataforma GNU/Linux

Plataforma de correo y entorno colaborativo open source

Resurrección Mazo González

E.T.I.S.

Miguel Ángel Senar Rosell

13/06/2011

Aunque pequeño sea el esfuerzo realizado en este trabajo de final de carrera, frente a la larga sombra de sacrificio que el ocaso de esta aventura ha dejado tras de sí, me gustaría cerrar este episodio de mi vida, con la oportunidad de agradecer a todos aquellos, y sobre todo aquellas, que me apoyaron sin condición, para verme aquí. Además, y si cabe por encima de esos agradecimientos, agradecerlo también a todos aquell@s que no creyeron en mi, intentando así eclipsar más que sueño, un requisito profesional. Gracias.

DESCRIPCIÓN DEL PROYECTO

Desplegar una solución fiable, potente y escalable de correo electrónico, en combinación de un entorno colaborativo de aplicaciones, bajo el apadrinamiento de software open source.

OBJETIVO DEL PROYECTO

Antecedentes

Dada la actual situación de austeridad económica existente, las PYMES, en su evolución natural de integración en la denominada Sociedad de la Información, se enfrentan a la problemática de afrontar altos costos de licenciamientos, para la obtención de los beneficios ofrecidos por productos de terceros, basados en software propietario, que hagan posible esta evolución: servicios de correo electrónico, entornos colaborativos de trabajo, etc. En contrapunto a las soluciones de este tipo de productos no libres de costos, existe una gran cantidad de software conocido como "*software libre*" (*free software*) o de "*código abierto*" (*open source*), capaces de ofrecer, mediante una buena implementación, un alto rendimiento y una mayor plasticidad, frente a los primeros, todo ello sujeto a los beneficios de la libre distribución, que por regla general, minimizan los costes de la inversión.

Propósito final

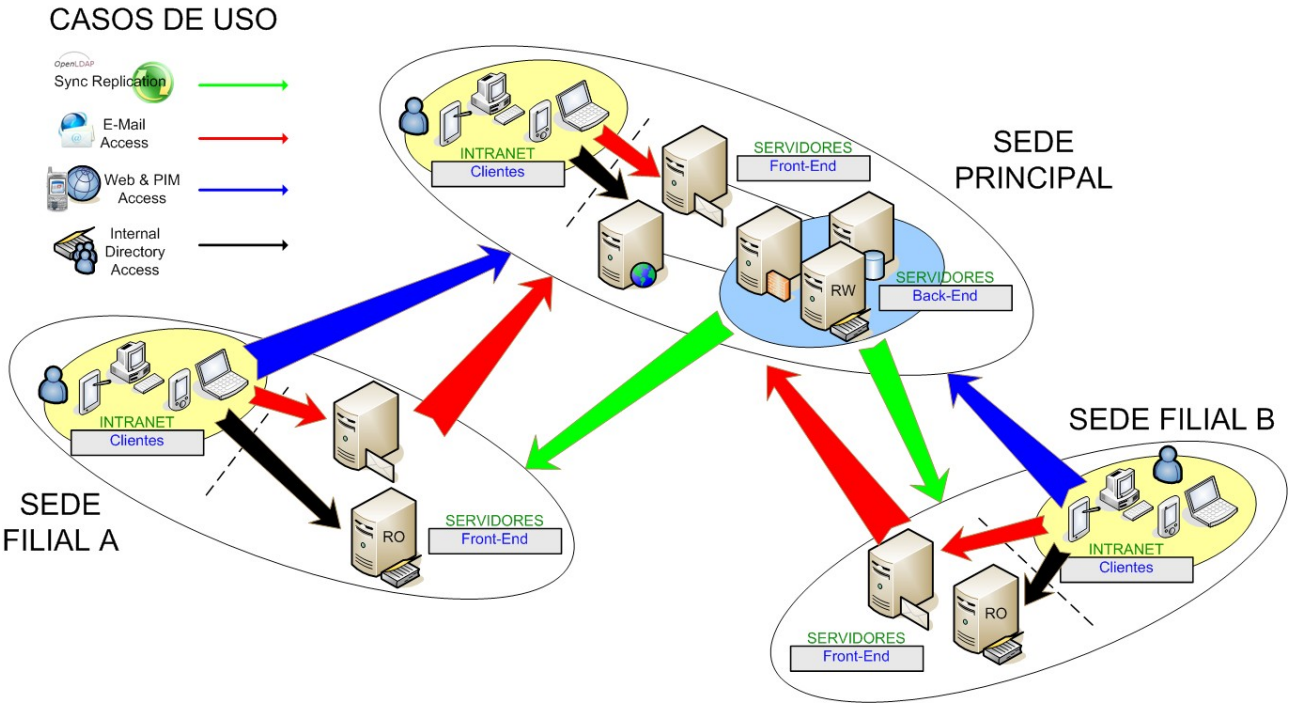
El objetivo de este proyecto de final de carrera tiene por motivación, el elaborar una plataforma de correo electrónico fiable, potente y escalable, acompañada de una *suite* de herramientas y aplicaciones web, que ofrezcan un entorno de software colaborativo robusto y accesible, todo ello basada en software open source. La solución a implementar, ambiciosamente buscará ofrecer una respuesta integrable en cualquier entorno corporativo, y potencialmente dimensionable a cualquier necesidad particular.

Esta propuesta fundamentada en software open source y GNU/Linux, propone implementar una plataforma basada en la interacción de un **sub-sistema de correo electrónico**, un **sub-sistema de directorio de usuarios**, y un **sub-sistema de aplicaciones web colaborativas**, de gestión de datos PIM (*Personal Information Manager*), y de administración, todo ello basado en el uso de los protocolos estándares y los RFCs de Internet: **IMAP4**, **POP3**, **SMTP**, **HTTP**, **LDAPv3**, y todas sus variantes basadas en el cifrado de los canales, mediante **SSLv3**/**TLSv1**.

Índice de contenido

DESCRIPCIÓN DE LA SOLUCIÓN TÉCNICA

La solución de desarrollo, implantación y despliegue propuesta en este proyecto, se basa en el acondicionamiento y preparación de la infraestructura de servidores y elementos de red necesarios, para materializar un sistema de correo electrónico corporativo, y un entorno de software colaborativo, que permitan a los usuarios comunes a ambos sistemas, tratar y compartir información, como puede ser la de datos PIM, la de intercambio de correo electrónico o la de compartición de agendas electrónicas. Además, la solución ofrece acceso universal a los datos, desde cualquier dispositivo móvil o fijo que lo permita, utilizando para ello el acceso a Internet.



Para ello, y dentro de la solución, se incluyen una serie de sub-sistemas, cuya sinergia operativa dará pie al funcionamiento global del sistema. Entre los sub-sistemas integrados contamos con los siguientes:

Sub-sistema de correo electrónico

El sub-sistema de correo electrónico será gestionado con distintos elementos partícipes en el funcionamiento global del mismo, cuyo propósito será el de ofrecer una solución completa de correo electrónico:

- MTAs *front-ends* para la gestión del SMTP (envío de mensajes), y la gestión proxy de conexiones POP3/IMAP4 (acceso a buzones).

- MTAs *filtradores*, que a modo de bridge, analizará todo el tráfico SMTP, tanto de inbound como de otubound, para filtrar cualquier patrón susceptible de ser *virus* o *spam*.
- Servidores de buzón *back-end* del tipo POP3/IMAP4, basados en la solución del tipo *maildir*.

Los diferentes tipos de **MTA** (*Message Transfer Agent*) podrán formar granjas horizontales de servidores balanceados en su clase, lo que permite tener un sistema fácilmente escalable, y ofrecer una mejora rendimiento, en el caso de degradación, por el incremento de los usuarios o de su uso. La solución de servidores de buzón, en base al dimensionamiento que se requiera, y el *hardware* que se tenga, podrá ser *clusterizado* mediante sistemas de ficheros basados en **SAN** (*Storage Area Network*), más robustos y eficientes, o balanceados mediante el uso de sistemas de ficheros de red (**NFS**, **CIFS**, etc.), basados en soluciones **NAS** (*Network Attached Storage*).

Sub-sistema de directorio de usuarios

El sub-sistema de directorio de usuarios se basará en el uso de un directorio LDAP, utilizando el esquema de servidores *maestro*, con acceso de escritura, y servidores *réplica* de sólo lectura, que servirán no sólo de catálogo de usuarios, sino de pasarelas de *autenticación* para cualquier servicio que pueda beneficiarse de su integración, con servicios de directorio LDAP.

Los servidores réplica de sólo lectura podrán formar granjas horizontales de servidores balanceados en su tipo, lo que permite tener un sistema fácilmente escalable, mejorar el rendimiento, y proveer continuidad, ante la pérdida o degradación de los servidores maestro. Los servidores maestro, dependiendo de la tecnología software sobre la que se implementen, podrán contar con *clusterización* en *multi-master*.

Sub-sistema de aplicaciones web

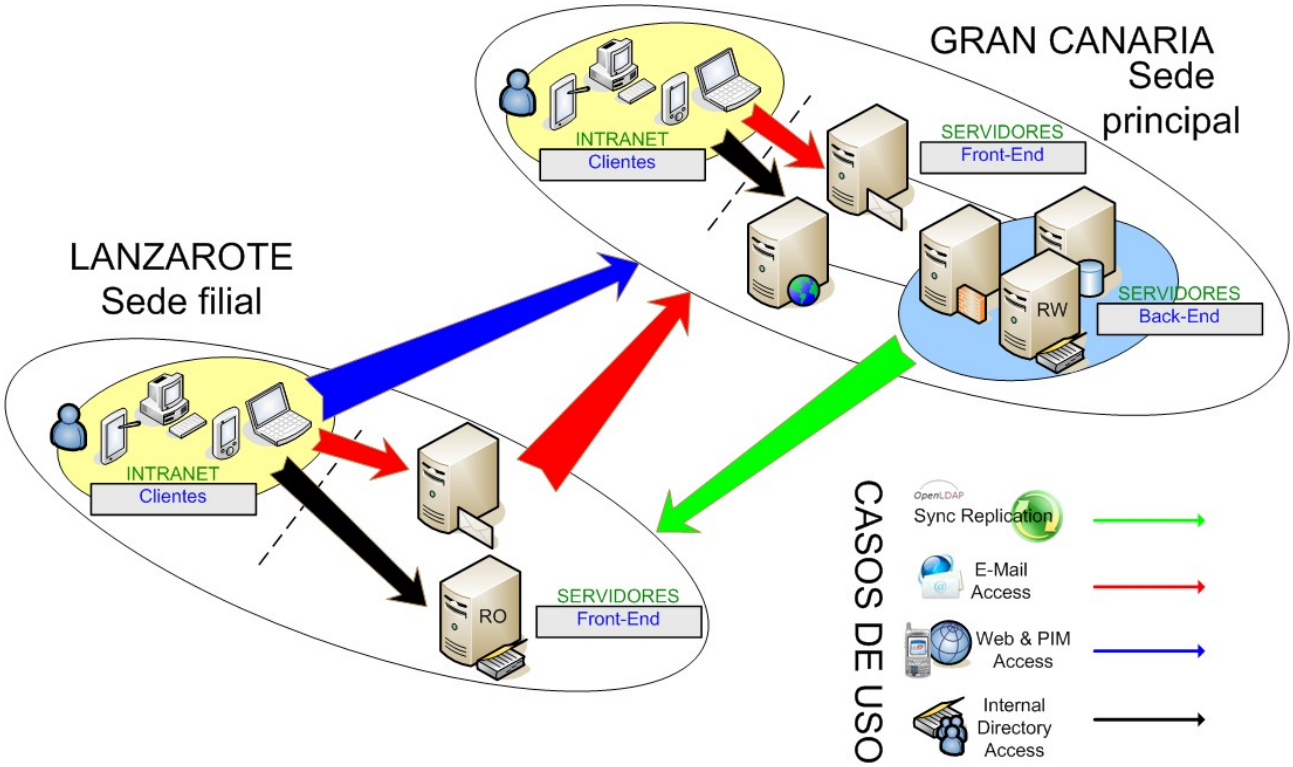
El sub-sistema de aplicaciones web se basará en el uso una granja horizontal de uno o varios servidores web balanceados, que sea fácilmente escalable, compartiendo para ello, los contenidos mediante sistemas de ficheros de red, basados en soluciones NAS, vía NFS. Entre las aplicaciones web se dispondrá de:

- Una herramienta de consola con GUI, de administración y provisión.
- Una herramienta de autoservicio y login.
- Una suite de aplicaciones web para entornos de colaboración (trabajo en grupo), y manipulación de datos PIM.

Como *back-end* de datos para las aplicaciones web, se utilizará una solución de base de datos **MySQL**, que se ha seleccionado por ser un componente open source de probada estabilidad.

Escenario práctico

Se ha diseñado un escenario que simula una corporación joven, con una sede principal ubicada en la isla de Gran Canaria, y con intenciones de expansión hacia el resto de las islas, como la isla de Lanzarote, donde está instaurando una sede filial.



Cómo podemos observar en el escenario, la solución contará contará con una sede filial que proveerá de servicios frontales (front-end) a los usuarios de la misma, mientras que todo el grueso de servicios de bak-end residirán en la sede principal, donde se alojarán los datos de usuarios, tanto de correo, como de aplicaciones de colaboración.

Aunque no es objetivo de este proyecto, la solución planteada brinda la oportunidad de ofrecer también un sistema de directorio corporativo, que permita centralizar la gestión de identidades en un único punto de la organización, y que es capaz de ofrecer este servicio de funcionamiento básico, a expensas de pérdidas de comunicación parciales con el los servidores maestros de directorio.

Tecnologías hardware involucradas

Acorde a las pretensiones de elaborar un sistema de correo electrónico y un sistema de aplicaciones de colaboración de bajo coste para una organización, la solución se ha diseñado para ser compatible e instalable bajo cualquier tipo de infraestructura hardware, que cumpla una serie de condiciones

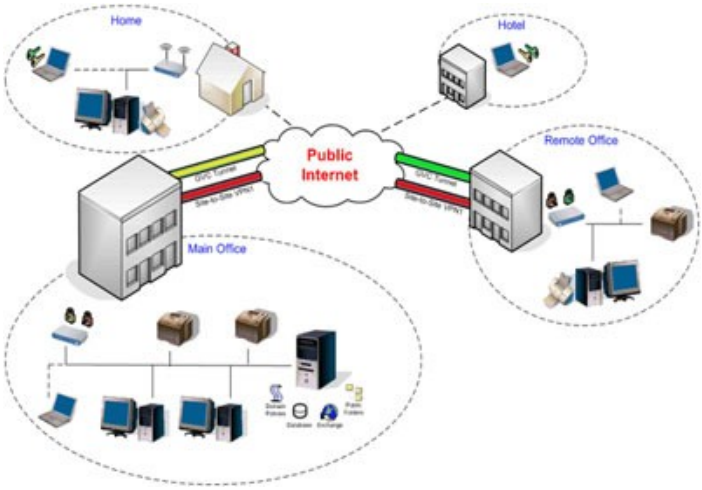
mínimas y necesarias para poder proveer el servicio. Por ello, la infraestructura hardware requerirá al menos de un *host servidor front-end* por sede, un *servidor de back-end de datos*, para alojar toda la información de buzones y de las aplicaciones colaborativas, un *servidor filtrador* de correo electrónico dedicado y aislando, por los altos requisitos de CPU y memoria que imponen el análisis de contenido, (lo que podría provocar la degradación de los otros servicios, si los hiciéramos convivir con este), y un servidor web de aplicaciones, a modo de *front-end* de datos.

La arquitectura hardware para estos 4 elementos será la de **Intel i686/x86_64**, plataforma hardware por excelencia para soportar sistemas operativos GNU/Linux. No obstantes, y como se analizará con cada tipo de componente software que interviene en la solución, se podría hacer uso de otras arquitecturas, dado que en su mayoría, el software a integrar es portable a una gran cantidad de tipos de esta.

Elementos transversales de comunicación

Adicionalmente al parque de servidores, será necesario una infraestructura de comunicación *ethernet* operativa y funcional, que al menos provea una red *LAN* de 100Mb/s en cada sede, y alguna línea de comunicación *P-t-P*, ya sea de forma dedicada o conmutada, que facilite la interconexión entre las distintas sedes, a nivel *WAN*/Internet, utilizando para ello cualquier tipo de solución de transmisión, como pueden ser los medios de transmisión y transporte basados en *xDSL* o *SDH*, y sobre estas, protocolos de control como *MPLS*.

Sobre estas tecnologías, y siempre desde el prisma de cada caso particular, se podría hacer uso de otras tecnologías específicas, que permitieran un mayor nivel de integración entre las sedes, como túneles VPN, que permitan dotar a las comunicaciones *P-t-P* de un mayor grado de aceptación por su bajo coste, en el caso de usar tecnologías de transmisión conmutadas, mediante algún proveedor de servicios *ISP:*



Es ajeno al propósito de este proyecto, el abordar toda la extensa parte relacionada con los servicios transversales de comunicación, si bien la solución requiere de los mismos, para su éxito final.

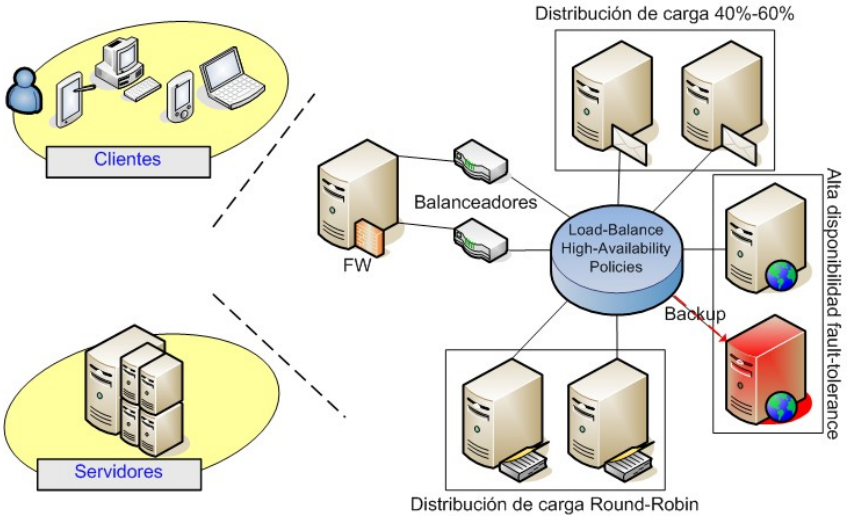
Tecnologías hardware de mejora de la solución

Balanceadores de red y de alta disponibilidad basados en hardware

Dada la plasticidad que ofrece el diseño de la solución, y desde el punto de vista de accesibilidad de red, es perfectamente asumible la utilización e integración de hardware de balanceo de carga y de alta disponibilidad, dentro de cada sub-sistema que se integra en la solución. Entre las aportaciones que pueden proveer este tipo de soluciones hardware, que por lo general, están muy lejos de ser accesibles a la mayoría de PYMES, por su lato costo económico, podemos destacar las siguientes:

- Alta disponibilidad de balanceo de servicios sobre distintos servidores, para proveer continuidad indefinida a los mismos, mediante control automatizado en hardware, de los elementos que componen nuestras granjas horizontales de servidores.
- Chequeo de servicios a nivel de aplicación: estos elementos, por regla general no sólo son capaces de detectar cualquier caída de servicio, (generalmente definidos por patrones de conexiones: tipo de protocolo TCP/UDP, número de puerto, persistencia de las conexiones, etc.), sino de también reconocer, a nivel de aplicación, si los servicios que responden detrás de este, están realmente funcionando correctamente, tomando decisiones como la de inhabilitar accesos, ante la detección de niveles altos de inoperatividad de algún servicio que se ejecute en un servidor.
- Balanceo uniforme y/o controlada de la carga soportada por los servicios en ejecución, sobre varios servidores horizontales que lo provean. Este balanceo puede estar basado en porcentajes de carga, baremadas por distintos tipos de patrones, como pueden ser: la frecuencia relativa del número de conexiones sobre el servicio, la carga a nivel de sistema que soporta cada servidor, etc.
- Etc.

Gráficamente podemos hacernos una aproximación topológica de red, en base al siguiente esquema:



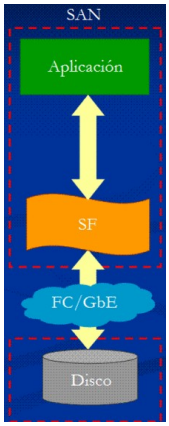
Todas y cada una de estas soluciones, que proveen valor añadido a la solución ofrecida con este sistema, son soluciones soluciones independientes del alcance de este proyecto, por lo que no se profundizará en la tipificación de cómo implementarlas, aunque sí que serán recordadas, como posibles opciones partícipes en el despliegue de la solución.

Algunas de estas osluciones hardware podrian ser las basadas en tecnologías de terceros como:

- *Cisco series ACE (Aplication Control Engine) - GSS (Global Site Selector)*
- *Cisco series CSS (Content Services Swithces)*
- *Etc.*

Soluciones de almacenamiento de red (SAN)

Pese a que la implementación más simple de la solución aquí tratada, se gestionará sobre los propios medios de almacenamiento de los servidores que la integran, es decir, discos magnéticos, es posible compatibilizar la solución con alternativas que aumentan exponencialmente la capacitación de espacio y velocidad de acceso a los volúmenes de datos, es decir, utilizar soluciones hardware de SAN (*Storage Área Network*), que descentralizan las operaciones de control I/O sobre los medios de almacenamiento, a los servidores de back-end:



Estas soluciones SAN, que generalmente ofrecen medios cuya eficiencia en el tratamiento de operaciones de I/O sobre discos, superan con creces las que habitualmente ofrecen los servidores sobre discos magnéticos del sistema, pues implementa por defecto, y de forma transparente, niveles *RAID* y de *stripe* basados en hardware, suelen estar sujetos a altos costos para su obtención en compañías de terceros, que por regla general, no son utilizadas en las PYMES.

Algunos manufacturadores y proveedores de soluciones de este tipo pueden ser:

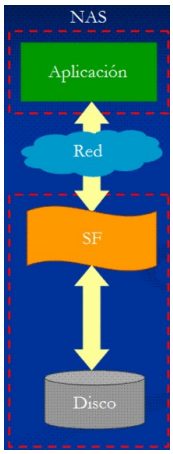
- *IBM*
- *HP*
- *Etc.*

Otra característica de este tipo de productos, es la posibilidad que dan de ofrece volúmenes compartidos de datos para distintos servidores, utilizando para ello sistemas de ficheros basados en cluster, como **GFS**, que serían gestionados desde los servidores que compartieran el volumen de datos.

Soluciones hardware de sistemas de ficheros de red (NAS)

El mercado hardware está abierto a ofrecer soluciones comerciales de alto rendimiento para la gestión de sistemas de fichero de red, como pueden ser NFS o CIFS. De igual manera, estos elementos pueden ser integrados y utilizados en el diseño de la solución propuesta en este proyecto, aunque esto que fuera del alcance del mismo.

Esta inclusión permitiría centralizar volúmenes de datos en un servidor de alta capacidad de espacio, compartido mediante protocolos de red como NFS o CIFS, entre distintos servidores, para así disponer en tiempo real, de los mismos contenidos, en sitios distintos:



Al igual que pasa con el resto de soluciones hardaware, esta no está carente de estar sujeta a altos costos impuestos por proveedores terceros, como pueden ser los da las siguientes soluciones de mercado:

- *EMC Celerra.*
- *NetApp File Services.*
- *Etc.*

Requisitos hardware mínimos

A continuación, se muestra una tabla con las necesidades hardware funcionales mínimas, que permitirán el despliegue de la solución ofrecida por este proyecto:

	HDD	RAM	CPU	Nº de unidades
Servidor de sede remota				
	8 GB	1 GB	2 GHz	1 por sede
Servidor de aplicaciones web				
	8 GB	2 GB	2 GHz	1 por solución
Servidor para filtrado				
	10 GB	2 GB	3 GHz	1 por solución
Servidor Back-End de datos				
	30 GB	2 GB	3 GHz	1 por solución

Estos servidores (ya sean físicos o virtuales), serán el número mínimo de servidores requeridos, para garantizar la puesta en marcha de la solución, con garantías de ser una plataforma funcionalmente fluida, para prestar el servicio soportando al menos a 2000 usuarios.

Así mismo, y dependiendo del uso de las necesidades de crecimiento de la plataforma, la solución podrá crecer horizontalmente, sin necesidad de cambiar configuraciones, o el propio diseño de la solución, incrementando con ello, una mayor capacitación para prestar los servicios integrados, a un mayor número de usuarios.

Sistemas operativos GNU/Linux involucrados

La solución ha sido testada sobre diferentes sistemas operativos Linux, en las que se ha distribuido la infraestructura de servidores, probando así su alto poder de integración, en casi cualquier sistema GNU/Linux, lo que brinda a la solución el estar desvinculado de proveedores exclusivos de sistemas operativos.

Para materializar el escenario, y dado que el principal propósito de este, es el de validar el concepto del proyecto, para conformar la granja mínima de servidores requeridos, se ha utilizado la solución de libre distribución para virtualización **VMWare Server 2**, probada su robustez y alto grado de uso en la comunidad de usuarios de Internet.

Acorde a esto, el escenario utilizado para testar la solución, se ha basado en el uso de la siguiente lista de instalaciones de servidores GNU/Linux:

	Versión	Info	Tipo
Sub-sistema de correo			
MTA Front-End			
Ubuntu Server	10.10	http://www.ubuntu.com/	Front-end
MTA filtrador			
Gentoo	2011	http://www.gentoo.org/	Front-end
Servidor de buzón			
Gentoo	2011	http://www.gentoo.org/	Back-end
Sub-sistema de directorio			
Gentoo	2011	http://www.gentoo.org/	Back-end
Sub-sistema de aplicaciones web			
Fedora	14	http://fedoraproject.org/	Back-end

Tecnologías software involucradas

Además de los sistemas operativos involucrados, sobre los que se consolida la solución objeto de este proyecto, se ha utilizado una amplia gama de productos software, basados en GNU/Linux y apadrinados bajo el concepto de open source:

OpenLDAP

Es una implementación libre y de código abierto del protocolo *Lightweight Directory Access Protocol* (*LDAP*), desarrollada por el proyecto que lleva su propio nombre. Está liberada bajo su propia licencia *OpenLDAP Public License*. *LDAP* es un protocolo de comunicación independiente de la plataforma. Muchas distribuciones GNU/Linux incluyen el software OpenLDAP, para proveer este soporte. A su vez, este está soportado por varias plataformas como *BSD*, *AIX*, *HP-UX*, *Mac OS X*, *Solaris*, *Microsoft Windows* (*NT* y derivados, incluyendo *Windows 2000*, *Windows XP*, *Windows Vista*), y *z/OS*.

El proyecto OpenLDAP se inició en 1998 por Kurt Zeilenga. Comenzó como un clon de la implementación *LDAP* de la Universidad de Michigan, entidad donde se desarrolló originalmente el protocolo *LDAP* y en donde actualmente se sigue trabajando en la evolución del mismo.

Históricamente la arquitectura del servidor OpenLDAP (*slapd*, *Standalone LDAP Daemon*) fue dividida entre una sección frontal que maneja las conexiones de redes y el procesamiento del protocolo, y una base de datos dorsal o de segundo plano (backend[1]) que trata únicamente el almacenamiento de datos. Su arquitectura es modular y posee una amplia variedad de tipos de

1 En versiones antiguas (1.x), los términos "*back-end*" y "*database"* (base de datos) podían intercambiarse. Para ser precisos, un "back-end" es una clase de interfaz de almacenamiento, y una base de datos es una instancia de un back-end. El servidor slapd puede utilizar arbitrariamente varios back-ends de una sóla vez, y puede tener arbitrariamente muchas instancias de cada back-end (por ejemplo varias bases de datos) activas a la vez.

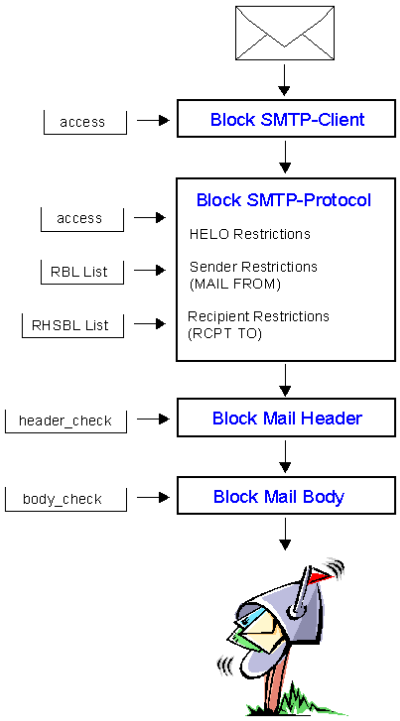
backends, que están disponibles para interactuar con otras tecnologías, y no sólo con bases de datos tradicionales.

Postfix

Es un servidor de correo basado en software libre y código abierto, utilizado para el enrutamiento y envío de correo electrónico, mediante protocolo *Simple Mail Transfer Protocol* (*SMTP*), y creado con la intención de ser una alternativa más rápida, fácil de administrar y segura, al ampliamente utilizado *Sendmail*. Anteriormente conocido como *VMailer* e *IBM Secure Mailer*, fue originalmente escrito por Wietse Venema durante su estancia en el Thomas J. Watson Research Center de IBM, y que en la actualidad, continúa desarrollándolo activamente.

Postfix es el agente de transporte (*MTA*) por defecto en diversas distribuciones de Linux y en las últimas versiones del *Mac OS X*, aunque puede ejecutarse sobre *AIX*, *BSD*, *HP-UX*, *IRIX*, *Solaris*, *Tru64 UNIX*, y otros sistemas UNIX. Para ello, se basa en los requisitos de *ANSI C*, y las librearías estándar *POSIX.1* y *BSD sockets*.

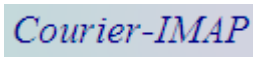
Una de los aspectos más potentes de Postfix, es el nivel de control que este ofrece sobre cada uno de los elementos que intervienen bajo los datagramas SMTP, permitiendo aplicar distintas políticas de acceso, en las distintas fases de procesado de un correo:



Cyrus-SASL

Es un paquete de librerías que contienen la implementación *Cyrus de SASL*. *SASL* viene de *Simple Authentication and Security Layer*, y en definitiva es un método para agregar soporte de autenticación a los protocolos basados en conexión. Entre algunos de estos soportes se encuentran:

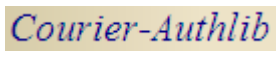
- cyrus-sasl-plain: contiene las extensiones (*plugins*) Cyrus SASL que soportan los esquemas de autenticación *PLAIN* y *LOGIN*.
- cyrus-sasl-gssapi: contiene las extensiones SASL que soportan la autenticación *GSSAPI*. *GSSAPI* se usa comúnmente en la autenticación *Kerberos*.
- cyrus-sasl-ldap: contiene las extensiones Cyrus SASL que soportan el uso de un servidor de directorio, accedido por medio de *LDAP*, para almacenar credenciales de usuarios.
- cyrus-sasl-md5: contiene las extensiones Cyrus SASL que soportan los esquemas de autenticación *CRAM-MD5* y *DIGEST-MD5*.
- cyrus-sasl-ntlm: contiene las extensiones Cyrus SASL que soportan los esquemas de autenticación *NTLM*.
- cyrus-sasl-sql: da soporte *SQL* auxprop para Cyrus SASL. Contiene las extensiones Cyrus SASL que soportan el uso de *RDBMS* para almacenar secretos compartidos.



Courier-imap

Es un servidor buzones de correo electrónico rápido, sencillo y escalable. Soporta *IMAP4* y *POP3*, permitiendo una configuración personalizada y óptima a todos los niveles. Según sus creadores, no impone límites para el administrador que haga uso de el, y su única limitación es ancho de banda con el cual se opere, para distribuir el servicio.

Courier-imap está vinculado con el gestor **Maildrop**, que es u agente de entrega de correo utilizado para depositar el correo electrónico, en el buzón de los usuarios. Se trata de una construcción independiente para uso con otros servidores de correo (*MTA*) como Postfix. Maildrop es un sustituto del agente local de entrega de correo: lee un mensaje de correo desde la entrada estándar, y a continuación, entrega el mensaje a su buzón de correo. Maildrop es compatible con los formatos de buzones de correo de estilo *mbox*, y *maildir*. Maildir es un formato de buzón utilizado por Courier y otros servidores de buzón de correo, que presenta muchos beneficios contra el tradicional mbox, como el utilizar múltiples ficheros para la gestión de los correos, y no un único fichero manejado por bloqueos, como utilizan las soluciones mbox.



Courier-authlib

Son un conjunto de librerías que ofrecen servicios de autenticación para aplicaciones de mensajería. En este contexto, el término "autenticación" se refiere a las siguientes

funciones: tomando un *ID de usuario*, y una contraseña, determina si el nombre de usuario y la contraseña son válidos. Así mismo, dado un identificador de usuario, obtienen la siguiente información sobre el ID de usuario (*loginID*):

- El directorio de usuario (*homedir*).
- El identificador de usuario del sistema numérico y *groupID* que posee todos los archivos asociados con esta cuenta.
- La ubicación del directorio de correo de la cuenta.
- Todos los contingentes Maildir definidos para esta cuenta.
- Otras opciones específicas de la cuenta, como: cambiar la contraseña asociada con un loginID, obtener una lista completa de todos los loginIDs, etc.

Además, la biblioteca de autenticación Courier ofrece implementaciones alternativas de estos servicios de autenticación:

- Usar los tradicionales archivos de sistema de contraseña: /etc/passwd y /etc/shadow, posiblemente en relación con la biblioteca *PAM*.
- Mantener toda esta información en una base de datos *GDBM*.
- Utilizar servidores LDAP para la autenticación.
- Utilizar tablas en distintos gestores de bases de datos como *MySQL* o *PostgreSQL*, para la autenticación.

Todos los componentes de Courier utilizan estas bibliotecas de autenticación, permitiendo autenticar las cuentas de correo electrónico, mediante cualquiera de los métodos expuestos anteriormente.

Perdition

Es un servidor POP3/IMAP4 *proxy* de alto rendimietno. Es capaz de manejar tanto conexiones en claro, como conexiones *SSL/TLS* cifradas, y redirigir a los usuarios a un servidor real, basándose en una base de datos de búsqueda.

Perdition admite el acceso modularizado a distintas base de datos. *ODBC*, *MySQL*, *PostgreSQL*, *GDBM*, etc., permitiendo además el uso de expresiones regulares, y utilizando los estándares *POSIX* y *NIS* en su compilación estándar. Además, y mediante el uso de *APIs*, está abierta a otros módulos arbitrarios, para permitir el acceso a cualquier almacén de datos, como por ejemplo *LDAP*.

Perdition permite muchos usos. Por ejemplo, la creación de grandes sistemas de correo donde el buzón de un usuario final está almacenado en uno de varios equipos o sistemas, la integración de distintos sistemas de correo en conjunto, la migración de correo electrónico entre diferentes infraestructuras, y la pasarela de conexión en claro, a cifrada, mediante servicios *SSL/TLS*. También

puede ser utilizado como parte de un servidor de seguridad.

AMaViS-new

Es una interfaz segura de alto rendimiento, que se ubica entre los agentes de correo (*MTA*) y uno o más *filtradores de contenido*, mediante encadenado: escáneres de virus y/o el módulo de *Perl Mail::SpamAssassin*. Está escrito en *Perl*, asegurando una alta fiabilidad de portabilidad, y facilidad de mantenimiento. Utiliza protocolos de *MTA* (*E*)*SMTP*, protocolos *LMTP*, u otros programas terceros que aporten valor añadido a la interfaz. No tiene *lags* horarios en el diseño, lo que podría causar una pérdida de correo.

Normalmente se coloca en, o cerca de, un servidor de correo, no necesariamente en los buzones de los usuarios, donde la entrega final se lleva a cabo.

Cuando en el encadenado interviene *Mail::SpamAssassin* (*SA*), las llamadas al SA son tratadas una sola vez por cada mensaje, independientemente del número de destinatarios, permitiendo mediante la configuración de las preferencias, la aprobación o rechazo, el check o nocheck de los mensajes, y la puntuación obtenida, con respecto a ser un posible correo no deseado, facilitando además la inserción de los campos relacionados con el análisis spam, en las cabeceras de los mensajes.

Otro beneficio de AmaViSd-new, es el del uso del módulo *Perl Net::Server,* que ofrece un rápido control de pre-proceso de *multichild bifurcada*. AMaViSd-new proporciona un servicio *SMTP* compatible con el *RFC2821*, *LMTP* compatible con el *RFC2033*, y otros estándares relacionado (RFC3462/rfc3464-compliant, RFC1892/RFC1894).

Estas características lo hacen propicio como solución de anti-virus y/o control anti-spam para, el servicio de correo electrónico, para el cumplimiento de fiabilidad y seguridad prefijado por las normas éticas de seguridad.

AMaViSd-new surgió de *AMaViSd*, (que a su vez es una versión demonizada de *AMaViSd-perl*), y que con más de cinco años de desarrollo, se convirtió en un producto separado, muy parecido a su original, con mejoras considerables sobre este: el código es varias veces el tamaño de su predecesor, pero más rápido en el rendimiento, más rica en características, conforme a las normas, incluyendo soportes opcionales para la detección de *spam*, y haciendo posible la detección de virus, con soluciones opcionales, y productos de terceros, y yodo ello configurable de manera fácil, sencilla y abierta.

ClamAv

Es un software antivirus open source (de licencia *GPL*) para las plataformas *Windows*, *Linux* y otros sistemas operativos semejantes a *Unix*.

El proyecto ClamAv Antivirus fue fundado en el año 2001 por Tomasz Kojm. Actualmente tiene

una implantación superior a los 500000 servidores en todo el mundo. Nació como un proyecto open source cuyo propósito es identificar y bloquear virus en el sistema. El primer objetivo de ClamAv fue combatir el correo electrónico *malware*. Como consecuencia de ello, ClamAv se está usando en un número elevado de servidores de correo electrónico.

Gracias a la colaboración de varias compañías, universidades y otras organizaciones, al proyecto ClamAv le ha sido posible poseer una red extensa de distribución mirror, rápida y fiable en todo el mundo, condición imprescindible para contar una reposición diaria de actualizaciones de los registros de *patterns* y/o *firmas de virus*..

Servidor HTTP Apache

Es un servidor web HTTP de código abierto para plataformas Unix (*BSD*, *GNU/Linux*, etc.), *Microsoft Windows*, *Macintosh* y otras, que implementa el protocolo HTTP/1.1[2] y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular *NCSA HTTPd 1.3*, pero más tarde fue reescrito por completo. Su nombre se debe a que Behelendorf quería que tuviese la connotación de algo que es firme y enérgico pero no agresivo, y la tribu Apache fue la última en rendirse al que pronto se convertiría en gobierno de EEUU, y en esos momentos la preocupación de su grupo era que llegasen las empresas y "civilizasen" el paisaje que habían creado los primeros ingenieros de Internet. Además Apache consistía solamente en un conjunto de parches a aplicar al servidor de *NCSA*. Era, en inglés, a patchy server (un servidor "parcheado").

El servidor Apache se desarrolla dentro del proyecto *HTTP Server* (*httpd*) de la *Apache Software Foundation*. Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años. (Estadísticas históricas y de uso diario proporcionadas por *Netcraft*).

La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan sólo pueden ser aprovechadas por usuarios locales y no remotamente. Sin embargo, algunas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales malévolos en las disposiciones de recibimiento compartidas que utilizan *PHP* como *módulo de Apache*.

PHP

Es un lenguaje de programación *interpretado*, diseñado originalmente para la creación de *páginas web dinámicas*. Es usado principalmente para la interpretación del lado del servidor (*server-side scripting*) pero actualmente puede ser utilizado desde una interfaz de línea de comandos o en la creación de otros tipos de programas, incluyendo aplicaciones con

interfaz gráfica usando las bibliotecas *Qt* o *GTK+*.

PHP es un acrónimo recursivo que significa *PHP Hypertext Pre-processor* (inicialmente *PHP Tools*, o, *Personal Home Page Tools*). Fue creado originalmente por Rasmus Lerdorf en 1994; sin embargo la implementación principal de PHP es producida ahora por *The PHP Group* y sirve como el estándar de facto para PHP, al no haber una especificación formal. Publicado bajo la *PHP License*, la *Free Software Foundation* considera esta licencia como software libre.

Puede ser desplegado en la mayoría de los servidores web y en casi todos los sistemas operativos y plataformas, sin costo alguno. El lenguaje PHP se encuentra instalado en más de 20 millones de sitios web y en un millón de servidores. Es también el *módulo Apache* más popular entre las computadoras que utilizan *Apache* como servidor web.

EGroupWare

Es una suite de programas libres para la empresa, que están diseñados para el trabajo en grupo (software colaborativo), en redes corporativas. Permite la gestión de contactos, citas, tareas y muchas más cosas a nivel corporativo. Está desarrollada sobre lenguaje PHP.

EGroupWare se puede considerar un servidor de trabajo en grupo. Viene con una interfaz web nativa que permite el acceso a los datos desde cualquier plataforma, y desde cualquier punto del planeta, mediante la red de Internet. También permite la elección abierta de clientes dedicados, para acceder a los datos del servidor, como pueden ser *Kontact*, *Evolution*, y *Outlook*, y también mediante teléfono móvil o PDA, haciendo uso de un servido de *SyncML*.

EGroupWare es independiente de la plataforma. El servidor corre bajo *Linux*, *Mac*, *Windows* y otros muchos sistemas operativos. En el lado del cliente, lo único que hace falta es un navegador de internet como *Firefox*, *Konqueror*, *Internet Explorer* y otros muchos más.

phpLDAPadmin

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

Posee una vista jerárquica basada en árbol, en donde se puede navegar por toda la estructura de directorio (*DIT*). Permite ver los esquemas *LDAP*, realizar búsquedas, crear, borrar, copiar y editar entradas *LDAP*, e incluso copiar entradas entre servidores *LDAP*.

Versiones mínimas recomendadas

Aunque la gran mayoría de del software es actualizable, sin pérdida de continuidad en sus líneas de configuración y características previas, se recomiendan una serie de mínimos, que garanticen cierto nivel de seguridad y funcionalidad:

	Versión	Protocolos	Servidor/Cliente/Proxy/Aplicación
Sub-sistema de correo			
MAT Front-End			
Postfix	≥2.4	SMTP/SSMTP	Servidor
Perdition	≥1.0	POP3/POP3S/IMAP4/IMAP4S	Proxy
Cyrus-sasl	≥2.1	-	Servidor
OpenLDAP	≥2.4	LDAP/LDAPS	Cliente
MTA filtrador			
Postfix	≥2.4	SMTP/SSMTP	Proxy
ClamAV	≥0.96	-	Servidor
SpamAssasin	≥3.3	-	Aplicación
AMaViS	≥2.6	-	Proxy
Servidor de buzón			
Courier-imap	≥4.0	POP3/POP3S/IMAP4/IMAP4S	Servidor
Courier-authlib	≥0.6	-	Servidor
Postfix	≥2.4	SMTP/SSMTP	Proxy
OpenLDAP	≥2.4	LDAP/LDAPS	Cliente
Sub-sistema de directorio			
OpenLDAP	≥2.4	LDAP/LDAPS	Servidor
Sub-sistema de aplicaciones web			
Apache	≥2.2	HTTP/HTTPS	Servidor
PHP	≥5	-	Servidor
EGroupWare	≥1.6	-	Aplicación
phpLDAPadmin	≥1.1	-	Aplicación
OpenLDAP	≥2.4	LDAP/LDAPS	Cliente
MySQL	≥5.0	-	Cliente

Distribución de las tecnologías software por host servidor

En la siguiente tabla se establece una relación que vincula el software integrante en cada tipo de host, que interviene en la el escenario desarrollado, para probar la solución de este trabajo:

	Nombre	Especificación	Descripción
Servicios trasversales			
Servicio de resolución de nombres primario (DNS)	BIND	SOA y NS principal del dominio: tfc-uoc.dyndns.org	Existirá un servidor DNS primario de resolución nombres, para nuestros dominios principales, que además replicarán la zona sobre tantos servidores frontales como sedes disponga nuestra organización.
Servicios de resolución de nombres esclavos (DNS)	BIND	NS esclavo del dominio: lanzarote.tfc-uoc.dyndns.org	Existirán tantos servidores DNS esclavos como servidores frontales para cada una de las sedes de que disponga nuestra organización.
Servicio maestro de sincronización de tiempo (NTP)	NTP.ORG	Servidor NTP de la organización, sincronizado con servidores de stratum 16 externos	Existirá un servidor NTP primario para nuestros dominios principales, que servirá de servidor NTP de sincronización, para el resto de servidores frontales, como los de las sedes de que disponga nuestra organización.
Servicios cliente de sincronización de tiempo (NTP)	NTP.ORG	Servidores NTP clientes de la organización	Servidores NTP clientes de la organización
Servicios de Firewall	iptables	Linux kernel ≥ 2.6	No es objeto de este proyecto el abarcar la parte de seguridad de red entre las sedes, pero se supondrá que la organización cuenta con un sistema de filtrado y acceso bien controlado y perfectamente capacitado para dotar de una comunicación transparente, a las distintas sedes, tanto a nivel geográfico, como entre los propios servidores, a nivel de la red LAN de cada sede.
Servicios de electrónica de red	LAN emulation	Emulación de electrónica de red para proveer de comunicación ethernet a todos los servidores de la organización.	No es objeto de este proyecto el abarcar la parte de conectividad de red entre las sedes, pero se supondrá que la organización cuenta con un sistema de red perfectamente habilitado, para dotar de una comunicación transparente, a las distintas sedes, tanto a nivel geográfico, como entre los propios servidores, a nivel de la red LAN de cada sede.
Servidores			
Servidor de buzones	MAILBOX	mailbox.tfc-uoc.dyndns.org: Servidor de buzones de correo de la organización.	Software integrado: Courier-IMAP, Courier-authlib, Postfix
Servidor maestro de directorio de usuarios	LDAPMASTER	ldapmaster.tfc-uoc.dyndns.org	Software integrado: OpenLDAP
Servidor filtrador de correo	MTA-FILTER	mta-filter.tfc-uoc.dyndns.org: Servidor de filtrado de correo de la organización.	Software integrado: Postfix, ClamAV, SpamAssasin, AMaViS

Servidor de aplicaciones web	WWW	www.tfc-uoc.dyndns.org: Servidor de aplicaciones web de la organización.	Software integrado: Apache, PHP, EgroupWare, phpLDAPadmin, OpenLDAP, MySQL
Servidor frontal para sede filial	LANZAROTE	lanzarote.tfc-uoc.dyndns.org: Servidor frontal que incluirá los servicios de réplica LDAP, y MTA de correo (envío SMTP e IMAP4/POP3 proxy). lanzarote.tfc-uoc.dyndns.org	Software integrado: Postfix, Perdition, Cyrus-sasl, OpenLDAP

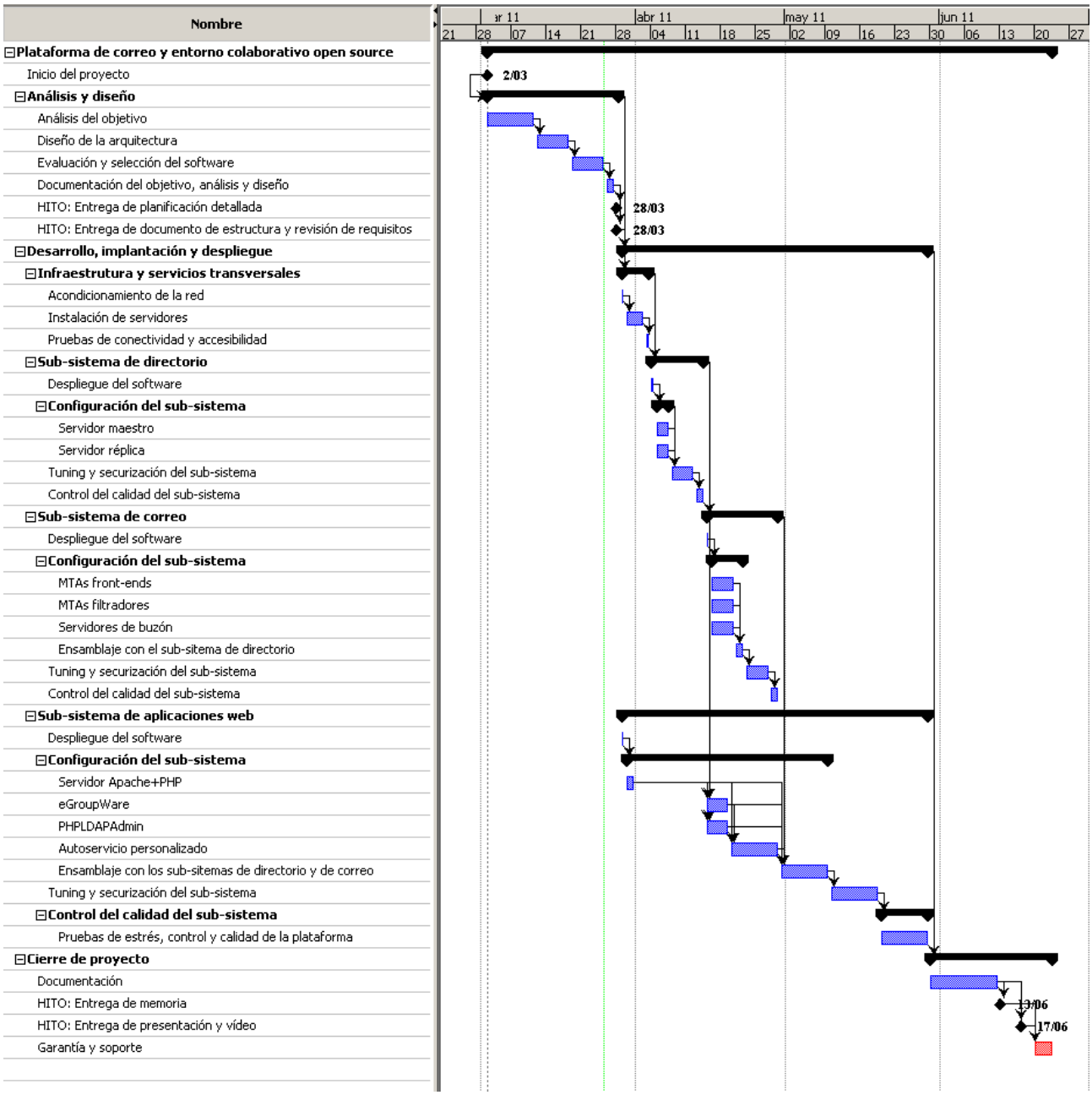
PLANIFICACIÓN

Para la implementación de la solución, se ejecutarán distintas tareas acotadas a los siguientes tiempos de ejecución:

	Nombre	Duración	Inicio	Terminado	Predecesores
1	**Plataforma de correo y entorno colaborativo open source**	114 days?	**2/03/11 8:00**	**23/06/11 17:00**	
2	Inicio del proyecto	1 day?	2/03/11 8:00	2/03/11 17:00	
3	**Análisis y diseño**	27 days?	**2/03/11 8:00**	**28/03/11 17:00**	**255**
4	Análisis del objetivo	10 days?	2/03/11 8:00	11/03/11 17:00	
5	Diseño de la arquitectura	7 days?	12/03/11 8:00	18/03/11 17:00	4
6	Evaluación y selección del software	7 days?	19/03/11 8:00	25/03/11 17:00	5
7	Documentación del objetivo, análisis y diseño	2 days?	26/03/11 8:00	27/03/11 17:00	6
8	HITO: Entrega de planificación detallada	1 day?	28/03/11 8:00	28/03/11 17:00	7
9	HITO: Entrega de documento de estructura y revisión de requisitos	1 day?	28/03/11 8:00	28/03/11 17:00	7
10	**Desarrollo, implantación y despliegue**	62 days?	**29/03/11 8:00**	**29/05/11 17:00**	**3**
11	**Infraestrutura y servicios transversales**	6 days?	**29/03/11 8:00**	**3/04/11 17:00**	**9**
12	Acondicionamiento de la red	1 day?	29/03/11 8:00	29/03/11 17:00	
13	Instalación de servidores	4 days?	30/03/11 8:00	2/04/11 17:00	12
14	Pruebas de conectividad y accesibilidad	1 day?	3/04/11 8:00	3/04/11 17:00	13
15	**Sub-sistema de directorio**	11 days?	**4/04/11 8:00**	**14/04/11 17:00**	**11**
16	Despliegue del software	1 day?	4/04/11 8:00	4/04/11 17:00	
17	**Configuración del sub-sistema**	3 days?	**5/04/11 8:00**	**7/04/11 17:00**	**16**
18	Servidor maestro	3 days?	5/04/11 8:00	7/04/11 17:00	
19	Servidor réplica	3 days?	5/04/11 8:00	7/04/11 17:00	
20	Tuning y securización del sub-sistema	5 days?	8/04/11 8:00	12/04/11 17:00	17;19;18
21	Control del calidad del sub-sistema	2 days?	13/04/11 8:00	14/04/11 17:00	20
22	**Sub-sistema de correo**	15 days?	**15/04/11 8:00**	**29/04/11 17:00**	**15**
23	Despliegue del software	1 day?	15/04/11 8:00	15/04/11 17:00	
24	**Configuración del sub-sistema**	7 days?	**16/04/11 8:00**	**22/04/11 17:00**	**23**
25	MTAs front-ends	5 days?	16/04/11 8:00	20/04/11 17:00	
26	MTAs filtradores	5 days?	16/04/11 8:00	20/04/11 17:00	
27	Servidores de buzón	5 days?	16/04/11 8:00	20/04/11 17:00	
28	Ensamblaje con el sub-sitema de directorio	2 days?	21/04/11 8:00	22/04/11 17:00	27;26;25
29	Tuning y securización del sub-sistema	5 days?	23/04/11 8:00	27/04/11 17:00	28
30	Control del calidad del sub-sistema	2 days?	28/04/11 8:00	29/04/11 17:00	29
31	**Sub-sistema de aplicaciones web**	62 days?	**29/03/11 8:00**	**29/05/11 17:00**	
32	Despliegue del software	1 day?	29/03/11 8:00	29/03/11 17:00	
33	**Configuración del sub-sistema**	41 days?	**30/03/11 8:00**	**9/05/11 17:00**	**32**
34	Servidor Apache+PHP	2 days?	30/03/11 8:00	31/03/11 17:00	
35	eGroupWare	5 days?	15/04/11 8:00	19/04/11 17:00	34;15
36	PHPLDAPAdmin	5 days?	15/04/11 8:00	19/04/11 17:00	34;15
37	Autoservicio personalizado	10 days?	20/04/11 8:00	29/04/11 17:00	34;35
38	Ensamblaje con los sub-sitemas de directorio y de correo	10 days?	30/04/11 8:00	9/05/11 17:00	22;37;36;35;34
39	Tuning y securización del sub-sistema	10 days?	10/05/11 8:00	19/05/11 17:00	38
40	**Control del calidad del sub-sistema**	10 days?	**20/05/11 8:00**	**29/05/11 17:00**	**39**
41	Pruebas de estrés, control y calidad de la plataforma	10 days?	20/05/11 8:00	29/05/11 17:00	
42	**Cierre de proyecto**	25 days?	**30/05/11 8:00**	**23/06/11 17:00**	**10**
43	Documentación	14 days?	30/05/11 8:00	12/06/11 17:00	
44	HITO: Entrega de memoria	1 day?	13/06/11 8:00	13/06/11 17:00	43
45	HITO: Entrega de presentación y vídeo	1 day?	17/06/11 8:00	17/06/11 17:00	43
46	Garantía y soporte	4 days?	20/06/11 8:00	23/06/11 17:00	45;44

Diagrama de GANT

Esquemáticamente podemos ver el el siguiente diagrama de GANT, la representación de cada uno de las fases e hitos asociadas, que nos dejan ver a golpe de vista, el camino crítico y las posibles paralelizaciones de tareas:



IMPLEMENTACIÓN DE LA SOLUCIÓN

La implementación de la solución se describirá inicialmente anotando y mostrando los servicios trasversales de que requiere la plataforma, y que constituyen la base operativa del sistema, para después entrar en las especificaciones de despliegue de cada sub-sistema.

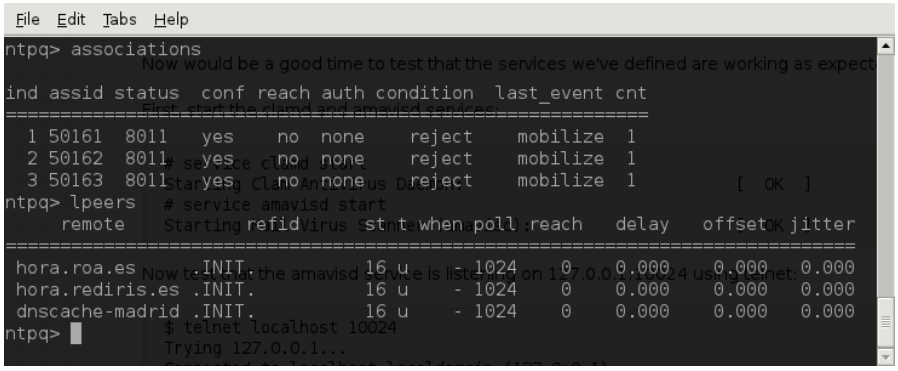
Esta parte del documento no incluirá las especificaciones que finalmente quedarán configuradas a nivel de servicios y servidor, las cuales vendrán anexadas al final de este documento.

Sub-sistemas de servicios transversales para la solución

Se describirá la implementación de algunos servicios trasversales a toda la solución.

Servicio de sincronización horaria (NTP)

Es difícil concebir un servicio de correo electrónico y agendas electrónicas, en el que no se controle de forma predeterminada, los ajustes horarios de todos los sistemas que intervienen en la solución, pues esto puede incurrir en una mala impresión de tiempos, en los eventos que estén sujetos a esta medida. Por ejemplo, no sería consecuente recibir mensajes de correo, antes de su fecha de envío, todo ello consecuencia de posibles desfases horarios en los relojes de los sistemas que intervienen en la prestación de los servicios. Para ello, se ha configura un servidor NTP principal, en el host de back-end de datos de buzones de correo electrónico, (aunque este servicio pudiera implantarse en cualquier otro servidor de los involucrados). Así mismo, este dependerá de la sincronización con los servidores atómicos de reloj públicos de internet:

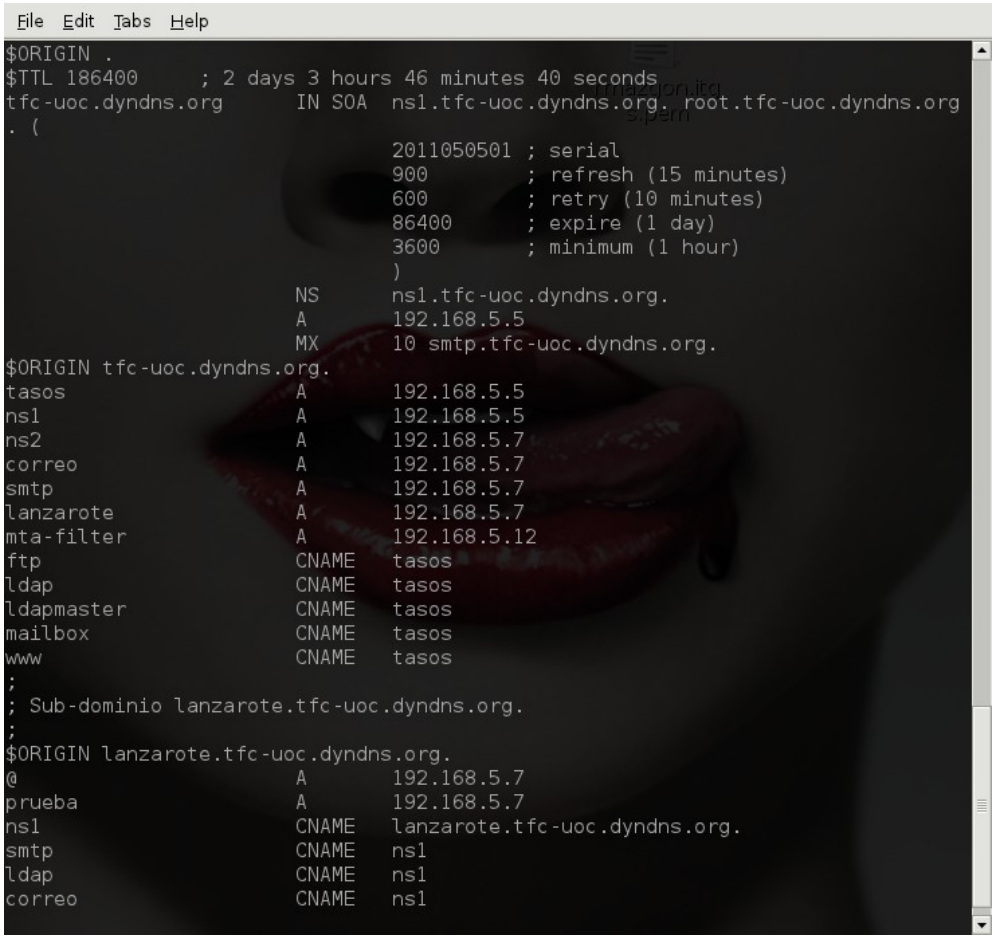


Una vez configurado este servidor, en el resto de servidores se han configurado servidores cliente que sincronicen los datos horarios de este servidor principal.

Servicio de resolución de nombres (DNS)

Bajo un entorno de implementación reducido, como es este, es medianamente fácil para los administradores de la solución, el memorizar las direcciones de red TCP/IP de cada servidor, con el fin de poder acceder a ellas, así como de configurarlas en donde se requieran. Si esto lo miramos

desde el prisma de un usuario de la solución, el costo de no tener un servicio de nombres que humanamente nos permita referenciar a esas direcciones de red TCP/IP, medianamente un nombre asociado, empieza a aumentar. Si todo eso lo extrapolamos a un entorno complejo, donde se cuenta con varias sedes distribuidas por distintos puntos geográficos, el sobre-costo es aún mayor. Es por ello que se ha configurado un servicio de resolución de nombres (DNS), con un servidor primario y dueño de la zona del espacio de nombres (para nuestro escenario, y tanto a nivel de internet como de intranet, llamado como **tfc-uoc.dyndns.org**):



Adicionalmente a este servidor primario, y de cara a no imponer un sobre costo en operaciones transversales de red, a los hosts que remotamente cooperen, se ha instalado en cada servidor, un servidor DNS esclavo de la zona definida en el primario, y que también haga las de servidor de caché para la resolución de nombres.

Servicio de base de datos MySQL Server

En cada organización, y por regla general, se mantienen distintas soluciones de BBDD que permiten

a las aplicaciones el alojar y consumir datos. Para nuestro caso de estudio, el escenario requerirá de una base de datos sobre un SGBD (*Sistema Gestor de Bases de Datos*) basado en la solución de MySQL Server, que será utilizado por la suite de software colaborativo EGrouopWare. Para ello, será necesario con una base de datos, que para nuestro caso, y por simplicidad, hemos llamado `egroupware`:

```
File  Edit  Tabs  Help
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| egroupware         |
| test               |
+--------------------+
3 rows in set (0.00 sec)
```

Despliegue de certificados X.509, para soporte SSL/TLS

De manera transversal a todos los sub-sistemas, se han llevado a cabo tareas mecánicas como la de generación de *certificados auto-firmados* (*self-signed certificates*), que permitan proveer a los servidores, de un certificado digital basado en el uso de *PKI* (*Public Key Infrastruture*), para poder establecer negociaciones de cifrado, en los canales de comunicación, mediante el intercambio de claves públicas, mediante la utilización de la suite criptográfica *OpenSSL*, disponible para todas las plataformas GNU/Linux:

```
Remote Console  Devices

root@LANZAROTE:/etc/ssl/slapd# ls
lanzarote.tfc-uoc.dyndns.org.crt  lanzarote.tfc-uoc.dyndns.org.key
lanzarote.tfc-uoc.dyndns.org.csr
root@LANZAROTE:/etc/ssl/slapd# openssl x509 -text -in lanzarote.tfc-uoc.dyndns.o
rg.crt
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            83:ad:6b:19:d9:47:c5:5c
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ES, ST=Canary Islands, L=Lanzarote, O=TFC-UOC, OU=GNU-Linux, C
N=lanzarote.tfc-uoc.dyndns.org/emailAddress=postmaster@tfc-uoc.dyndns.org
        Validity
            Not Before: Apr 11 14:52:22 2011 GMT
            Not After : Apr 10 14:52:22 2013 GMT
        Subject: C=ES, ST=Canary Islands, L=Lanzarote, O=TFC-UOC, OU=GNU-Linux,
CN=lanzarote.tfc-uoc.dyndns.org/emailAddress=postmaster@tfc-uoc.dyndns.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c5:ff:93:02:23:da:de:a3:dc:6e:73:f8:31:0b:
                    67:eb:09:3a:cf:f6:0c:1d:1b:13:65:ef:e8:21:42:
                    7b:eb:f9:d6:2e:c4:2e:99:3d:34:33:0e:60:33:04:

To grab input, press Ctrl+G
```

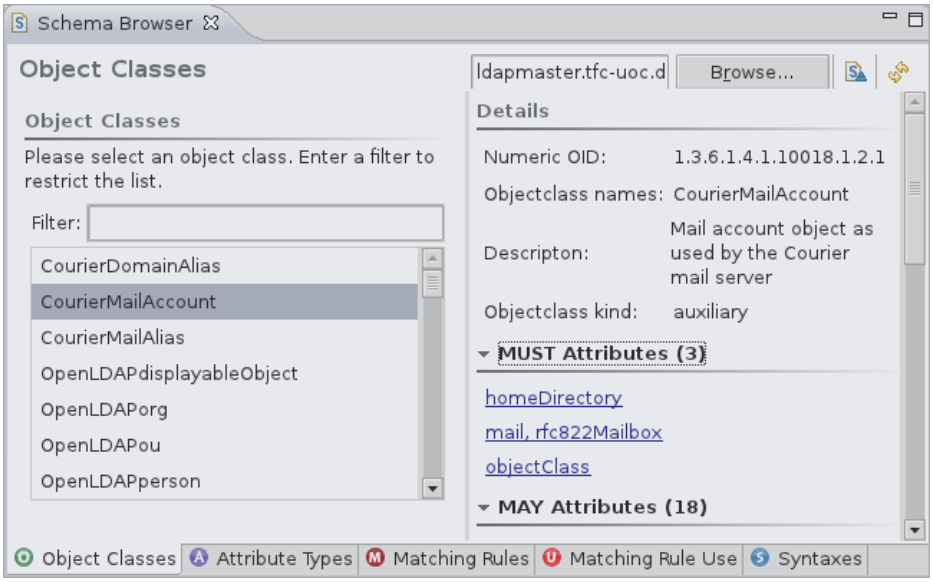
Sub-sistema de directorio de usuarios

Se desplegó de manera funcional y operativa el software de OpenLDAP, en todos aquellos servidores que hacen uso de él, destacando dos roles, el rol de **servidor de directorio maestro**, único capacitado para procesar operaciones de escritura, y **servidor de directorio réplica**, habilitado únicamente para procesar peticiones de sólo lectura, y continuamente en sincronización de contenidos (datos), con el servidor maestro.

Configuración

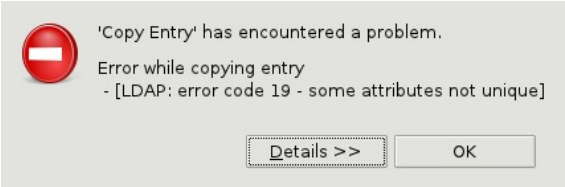
Para la configuración del sub-sistema, se llevaron a acabo trabajos sobre distintos hitos y aspectos del servicio de directorio:

- **Esquema del directorio**: el esquema de un directorio LDAP es la definición de los distintos tipos de objetos que un servidor LDAP puede incluir. Dentro de estos objetos, existen dos tipos que son los más orientados al consumo del servicio, y que permitirán a los administradores, el aprovisionar a las entradas del directorio (en nuestro caso, los usuarios), información relacionado con la identidad de la entrada y con los servicios que este posee. Estos objetos son los atributos (*attributes*) y la clases (*objectClasses*). Para nuestro caso, se ha ampliado el esquema para hacer posible la inclusión de información específica de los servicios de correo, en las entradas representativas de los usuarios:

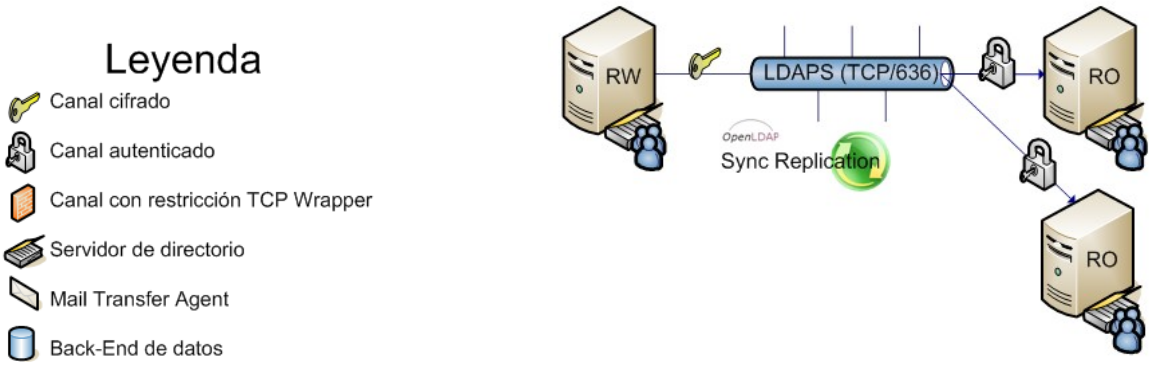


- **Overlays de configuración**: desde su versión 2.3, OpenLDAP permite la inclusión de una serie de *plugins* que le dan valor añadido al servicio de directorio, que recordemos, es fiel al estándar de directorio X.500, y que por defecto, no abastece servicios adicionales, más allá de para lo que está diseñado. Entre estos plugins se ha incluido el propio de replicación

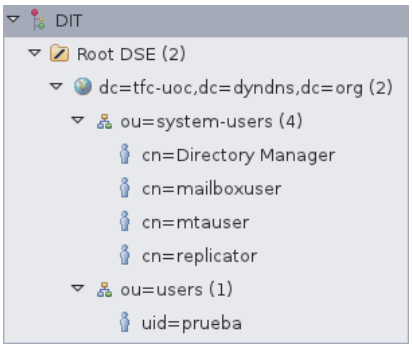
"*syncprov*", obligatorio para hacer efectivo el sistema de replicación LDAP, y el de unicidad de atributos "*unique*", que nos da la posibilidad de establece una *constraint* en el servidor maestro, para evitar que se duplique atributos como el identificado único de usuario (*uid*), o como las direcciones de mail entre usuarios (*mail*):



- **Sistema de replicación**: se ha optado por una opción de replicación sin multi-master, ya que un entorno multi-master no produce ventajas significativas ni en rendimiento ni en alta disponibilidad, por lo que se ha designado un único rol de servidor de directorio maestro (`ldapmaster.tfc-uoc.dyndns.org`), para nuestra solución. Adicionalmente al servidor maestro, que aceptará peticiones tanto de consulta (`bind`, `srch`, `comp`), como de escritura (`add`, `del`, `mod`), cada sede contará con un servidor réplica de LDAP, que solamente servirá de acceso en modo de lectura, a cualquier cliente que se conecte.



- **Diseño del DIT y plantillas de objetos**: LDAP basa su estructura de objetos, en una disposición jerárquica y arbórea, reconocida como DIT. Es crucial contar con un buen diseño organizativo, que no sólo infunda lógica de negocio en la estructura, sino que permita escalar e incluir nuevas modificaciones en la estructura:



Adicionalmente y muy relacionado con el DIT, hemos de tener claro el uso de plantillas estándar de objetos, que finalmente vayan a representar a nuestra comunidad de usuarios:

Atributos de información personal
uid: Identificador único personal. *cn*: Nombre + Apellidos. *givenName*: Nombre. *sn*: Apellidos. *manager*: DN puntero al responsable. *mobile*: Teléfono(s) móvil(es). *telephoneNumber*: Teléfono(s) fijo(s). *ou*: Departamente. *o*: Área del departamente. *postalAddress*: Dirección postal. *st*: Provincia. *l*: Localidad. *postalCode*: Código postal. *title*: Titulación académica. *employeeNumber*: DNI. *employeeType*: Ocupación. *destinationIndicator*: Permitir acceso público. *gecos*: Pregunta de recuperación de password.

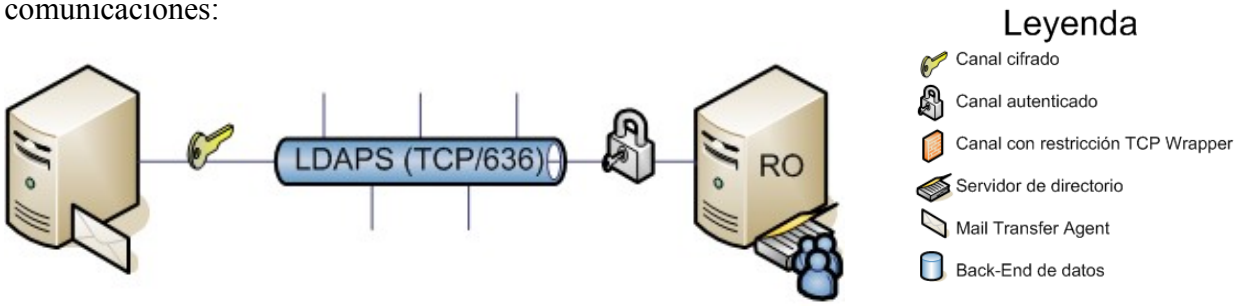
Atributos de usuario de correo
mail: Direcciones de correo. *mailHost*: Servidor de buzón. *mailLocalAddress*: Direcciones de correo para forwards y listas de distribución. *mailRoutingAddress*: Correo electrónica de lista de distribución. *mailBox*: Directorio maildir del usuario (ruta relativa sobre homeDirectory). *defaultDelivery*: Opciones sobre el delivery. *quota*: Cuota de correo. *disableImap*: Inhabilita el buzón IMAP4. *disablePop3*: Inhabilita el buzón POP3.

Clases necesarias
top *person* *organizationalPerson* *inetOrgPerson* *inetLocalMailRecipient* *CourierMailAccount*

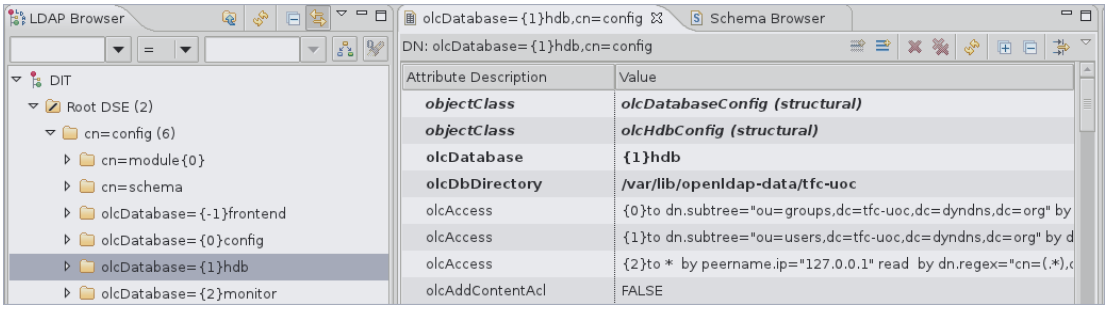
Tuning y seguridad

Para que nuestro sistema de directorio sea eficiente, ha de contar con una buena indexación de atributos, para lo cual, tendremos que conocer bien el nivel de filtros de búsqueda que el resto de sub-sistemas y aplicaciones usarán, para consultar a nuestros servidores de LDAP. Además esta labor está directamente asociada a la labor de tuning de los back-end de datos que usará nuestro servidor de LDAP, y que generalmente será una base de datos del tipo **SleepyCat** o **BerckleyDB**, que deberán llevar su parte de tuning, haciendo especial hincapié, en la parte relativa a las operaciones de *checkpoint* y de caché de memoria a utilizar.

Adicionalmente al tuning de datos, tenemos que cubrir los aspectos de seguridad, en cuanto al acceso a datos. Para nuestro sistema se hace obligatorio el uso de acceso autenticado al servicio de LDAP, (no se permite acceso anónimo), y el uso de nivel de cifrado TLS/SSL en las comunicaciones:



- Requerimiento de conexiones mediante canal cifrado (LDAPS).
- Replicación mediante canal cifrado (LDAPS).
- Inclusión de reglas de acceso a contenidos (ACL).
- Accesos identificados individualmente por usuario, mediante la inhabilitación del acceso anónimo.
- Trazabilidad de accesos, mediante registro de sucesos.
- Trazabilidad de errores de servidor y replicación.
- Creación de configuración dinámica basado en el uso de atributos y clases OLC, para los servidores SLAPD de OpenLDAP:

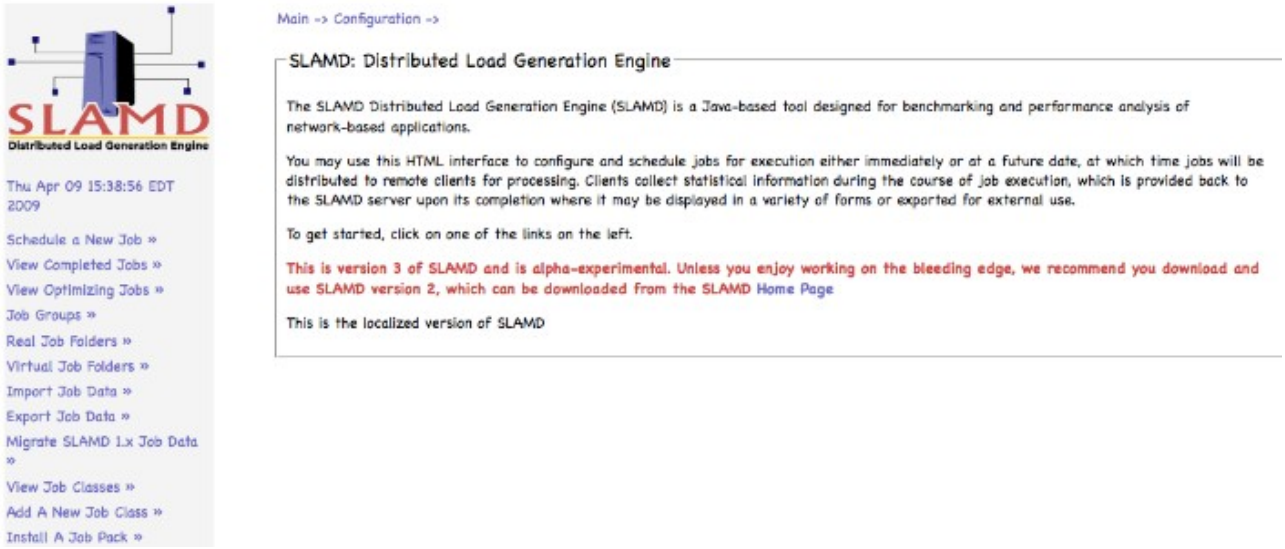


Pruebas de control

Una vez implementada la solución del sub-sistema, es buena práctica el invertir tiempo en auditar la el nivel de capacidad de nuestra plataforma de directorio, así como testar el nivel de fiabilidad en algo tan crítico como la replicación de datos, entre el servidor maestro y el servidor réplica.

Para todo ello, existen distintas herramientas gratuitas o liberadas, que permiten estresar los niveles de capacitación de nuestras plataforma.

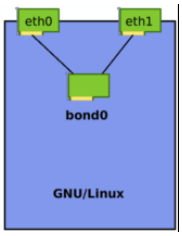
Un ejemplo de este tipo de herramientas puede ser el **SLAMD**, una aplicación Java que permite distribuir tareas de estrés sobre distintos clientes, con el fin de atacar a un servidor LDAP:



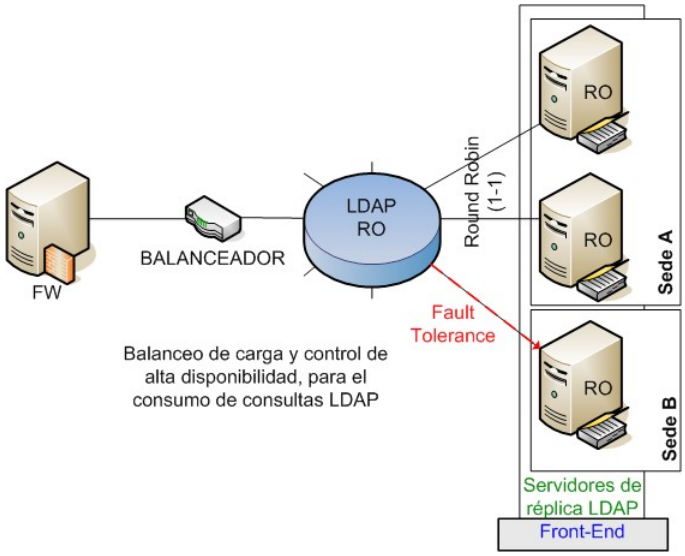
Como referencia, indicar que un nivel de aceptación óptimo para una plataforma de LDAP, puede ser el de aceptar y procesar de manera correcta, entre 500 y 1000 operaciones por segundo.

Alta disponibilidad, balanceo de carga y mejora de rendimiento

Una opción interesante para estos servidores, es la opción de usar interfaces ethernet en bonding, de cara a proveer una solución *fault-tolerant*, que paralelamente ofrezca balanceo de carga, a nivel comunicación LAN:



Respecto a opciones hardware adicionales, como el del uso de balanceadores, dado el complejo y delicado funcionamiento del sistema de replicación de cambios del sistema de directorio, el balanceo de carga y la alta disponibilidad a nivel de servidores maestros, no supone una mejora sustancial en el sistema, sino que puede dar pie a mayores perjuicios que beneficios. Por el contrario, los servidores réplica LDAP pueden estar perfectamente asociados en grupos de balanceo de carga, así como en sistemas de alta disponibilidad, mejorando así el servicio de consultas de los clientes:



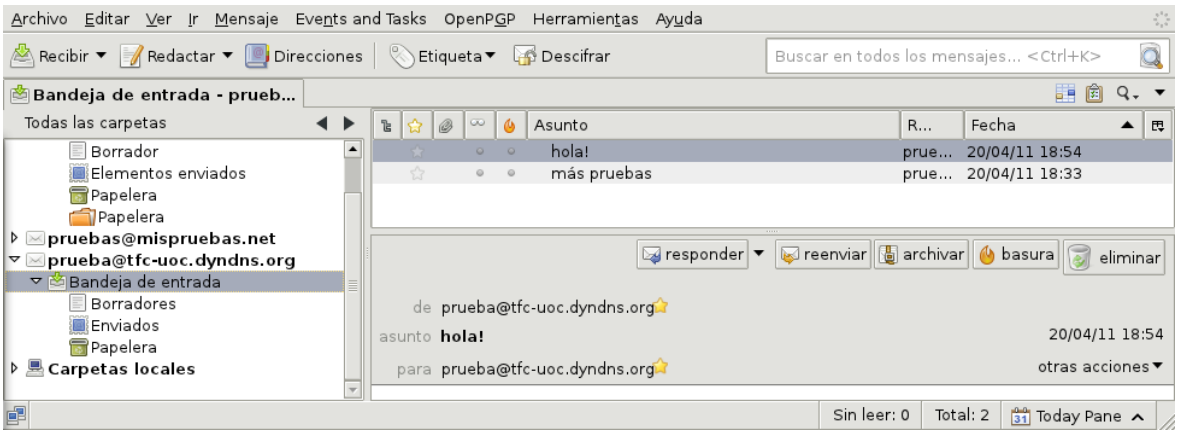
De cara a los actuales servicios de virtualización de alto nivel que están disponibles en el mercado, los servidores LDAP son posibles candidato a ser virtualizados, ahorrando así en infraestructura hardware.

Si analizamos las opciones opciones relacionadas con los recursos hardware de datos, carece de sentido el utilizar volúmenes de datos basados en SAN, o basados en NAS, pues cada instancia de servidor LDAP está optimizado para trabajar con back-ends de datos del tipo Sleepy-Cat o BerckleyDB.

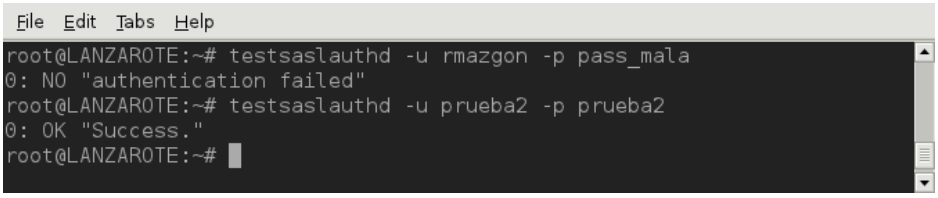
Sub-sistema de correo electrónico

Se desplegó de manera funcional y operativa todo el software requerido para cada uno de los tres roles de servidor, de que se compone el sub-sistema de correo, cada uno de estos, en host diferentes:

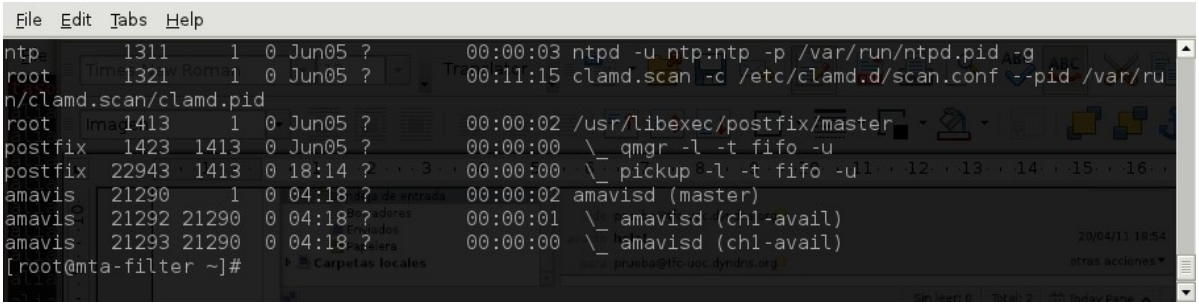
- Rol de **servidor de mailbox (buzón) de back-end**, que habilita el acceso IMAP4 y POP3, a cualquier *MUA* (*Mail Client Agent*), como pueden ser clientes de correo del tipo *Mozilla Thunderbird*, o a clientes del tipo *webmail*.



- Rol de **servidor MTA front-end**, capacitado para procesar operaciones de envío y recepción SMTP, y de acceso a buzón de correo IMAP4 y POP3, mediante servicio proxy, utilizando para ello rigurosos mecanismos de acceso y control, apoyándose en servidores de directorio LDAP, para los procesos de autenticación y verificación de direcciones de correo electrónico, entre otros, utilizando para las librerías Cyrus SASL y OpenLDAP:

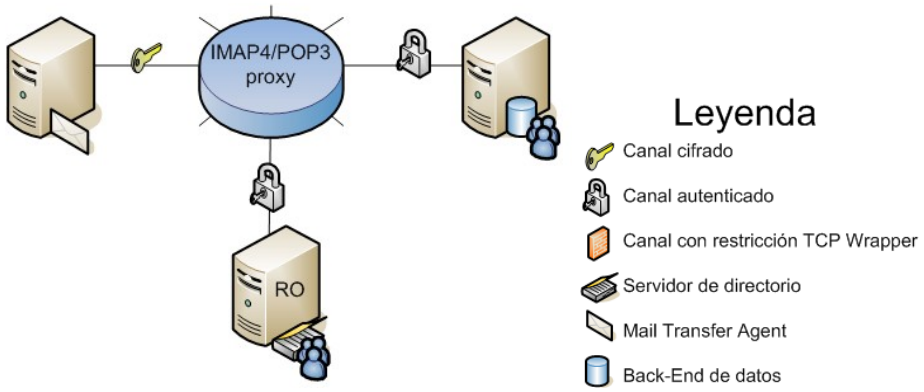


- Rol de **servidor MTA filtrador**, diseñado para encadenar mediante **AMaViS**, distintas soluciones de filtrado de correo malicioso, ya sea por indicios de ser *spam* o contener *virus*. El acceso al encadenado está provisto por una interfaz Postfix, que solamente estará habilitada para permitir *relay* desde los servidores corporativos y reconocidos, como servidores con el rol de MTA frontal, usando para ello restricciones *TCP Wrapper*:

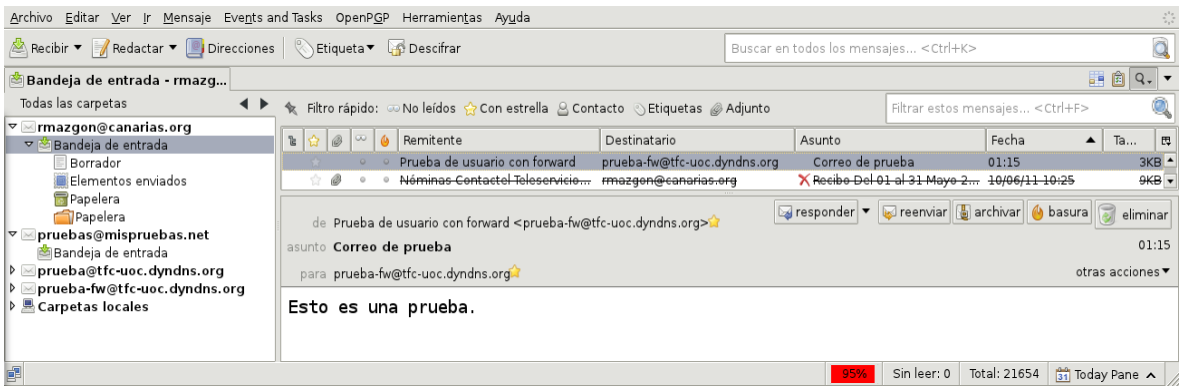


Configuración

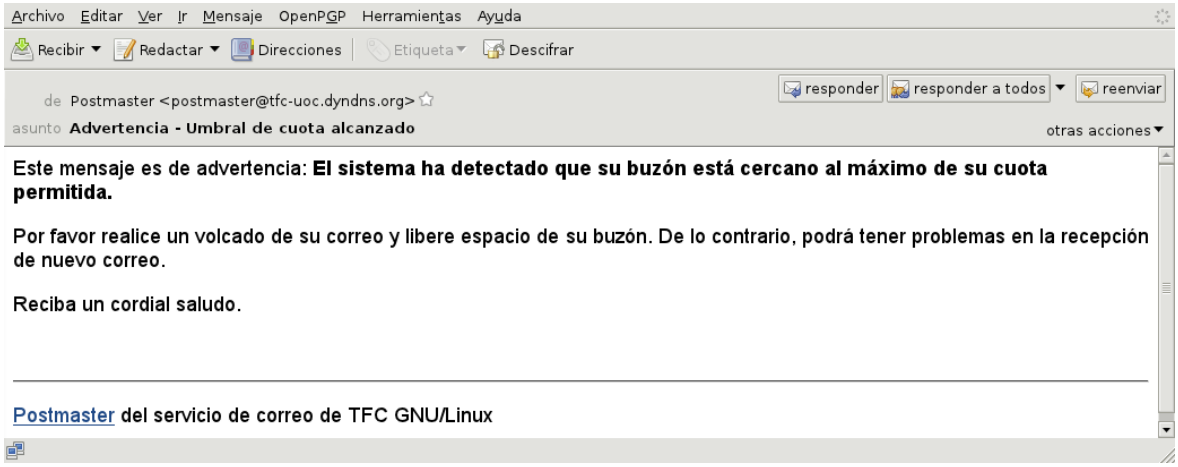
- **Servidor back-end de mailbox (buzón)**: ofrece el acceso a los buzones de mensajes particulares de los usuarios, identificado unívocamente mediante acreditación y atributos de configuración residentes en los servidores de directorio LDAP. Adicionalmente, cabe destacar que el acceso a este, ha sido totalmente restringido a los servidores MTA frontales de correo, mediante los servicios IMAP4/POP3 proxy Perdition instalados en los front-end de correo, y que serán los únicos que podrá hacer *delivery* SMTP sobre el servidor de buzón. A esta regla es necesario añadir una excepción, que es la del servidor o servidores de aplicaciones web, que publiquen la suite de aplicaciones colaborativas, a los que también se les ha dado acceso autenticado a los buzones, mediante el cliente embebido de webmail de que dispone:



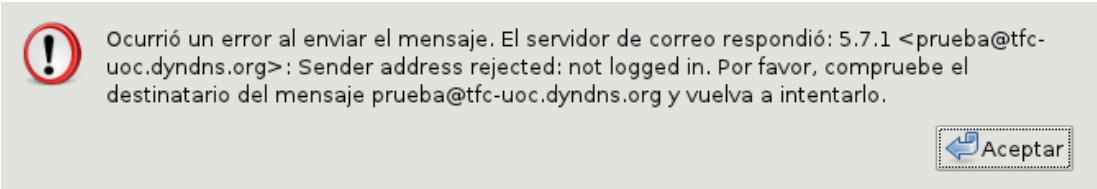
Bajo este servidor, también es destacable la funcionalidad añadida a la plataforma, mediante configuración del servicio Postfix, (servicio que se utiliza en la recepción de los delivery a buzón, a través del agente de entrega Maildrop), que permite hacer *forwards* automáticos, en aquellos usuarios que lo requieran, para re-enviar de forma automática, todo el correo recepcionado en su o sus cuentas de correo. El forward se podrá hacer sobre cualquier cuenta de correo, tanto dentro del dominio local, como de dominios externos, utilizando para ello la adición de los atributos pre-establecidos en LDAP para ello:



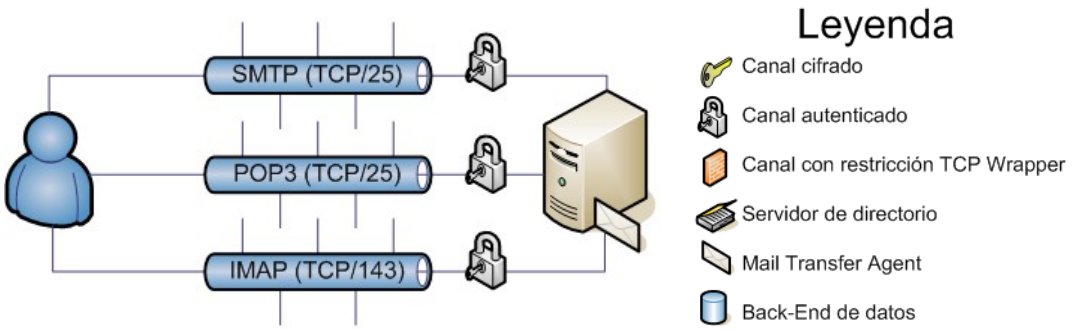
De igual forma, no se han escatimado esfuerzos en ofrecer detalles como el aviso de alcance próximo de las cuotas de correo que se establezcan por buzón, mediante su atributo LDAP correspondiente:



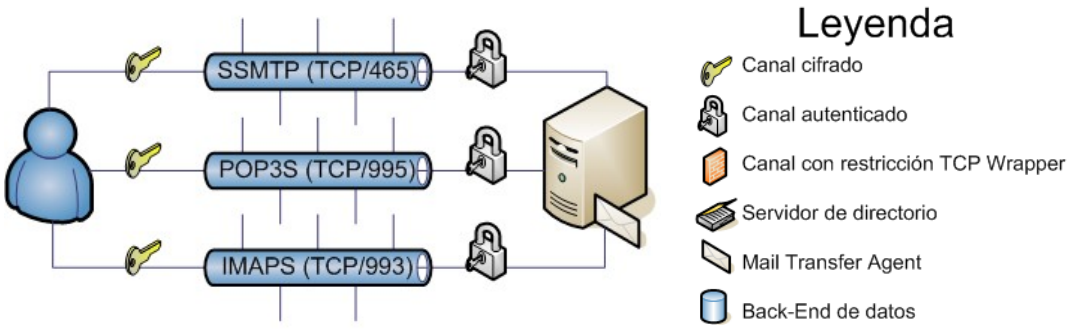
- **Servidor MTA front-end de correo**: a nivel de **servicios de MTA frontal** se han integrado una serie de restricciones que garanticen una buena utilización de los servicios SMTP:
  - *Autenticación para el envío de correo*: cualquier usuario estará obligado a autenticar la conexión SMTP:



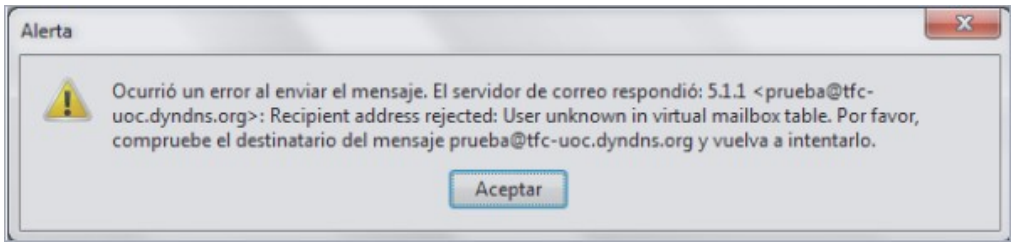
Adicionalmente, y de cara a los canales de acceso autenticado para los usuarios, a estos se les deja a elección el modo de conexión, entre el utilizar conexiones mediante canales no cifrados, que requieren menor peso en la comunicación y gestión de la conexión:



O por el contrario, la utilización de canales cifrados, mediante negociación SSL/TLS:



De igual modo, aquellas recepciones destinadas a los dominios locales, (por ejemplo y para nuestro caso *@tfc-uod.dyndns.org*), que no tengan un usuario final propietario, serán rechazados:



- *Anti-falsificación de direcciones de correo*: un usuario, previo proceso de autenticación, sólo podrá enviar correo electrónico desde las direcciones de correo que le pertenezcan:

- *Denegación de open-relay*: No se permitirá relay de correo de dominios ajenos a los propios de la organización:

- *Comprobación de RBLs para clientes externos*: el sistema comprobará mediante consultas DNS, a los distintos proveedores gratuitos de RBLs, que incluyen nombre y direcciones de clientes maliciosos, susceptibles de crear correo malicioso.

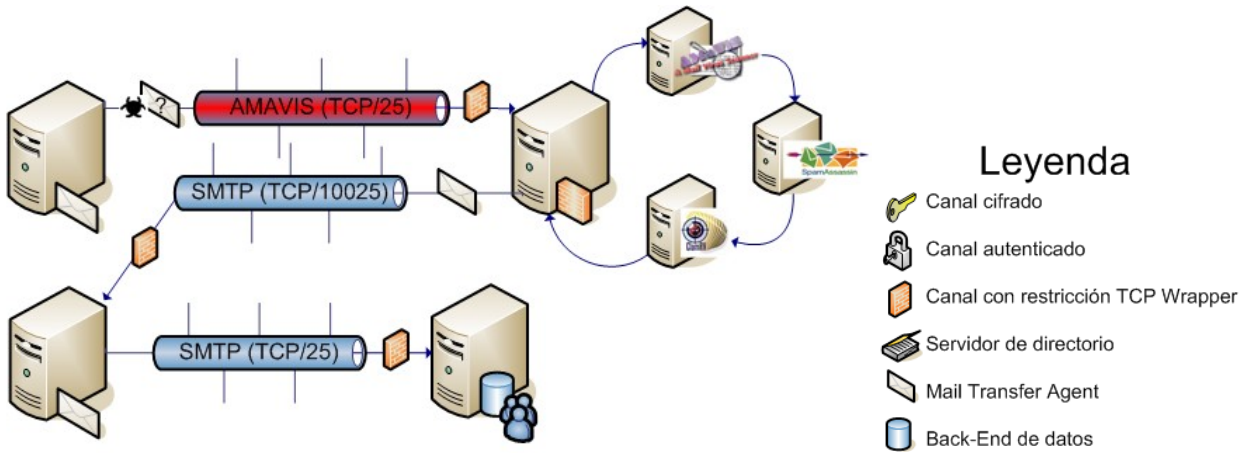
  Entre el listado de servidores RBLs que se han incluido, destacan:

```
File  Edit  Tabs  Help
reject_rhsbl_client blackhole.securitysage.com,
reject_rhsbl_sender blackhole.securitysage.com,
reject_rbl_client relays.ordb.org,
reject_rbl_client blackholes.easynet.nl,
reject_rbl_client cbl.abuseat.org,
reject_rbl_client proxies.blackholes.wirehub.net,
reject_rbl_client bl.spamcop.net,
reject_rbl_client sbl.spamhaus.org,
reject_rbl_client opm.blitzed.org,
reject_rbl_client dnsbl.njabl.org
```

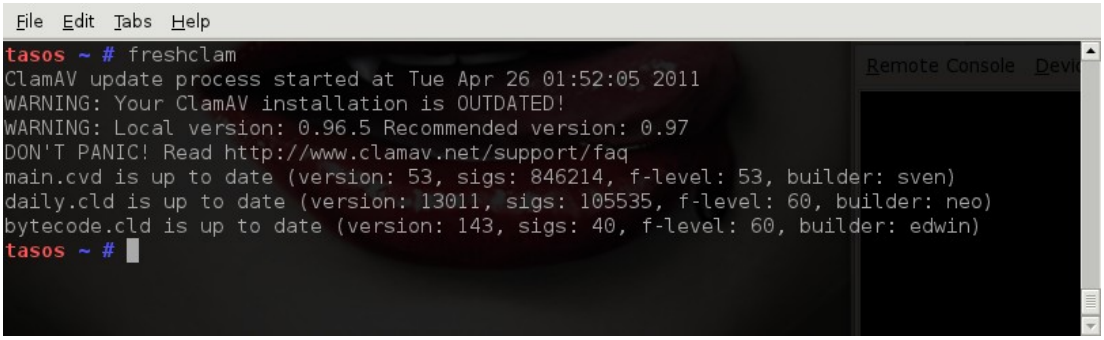
- *Gestión de listas de distribución basadas en LDAP*: los frontales de correo son capaces de gestionar envíos a listas de distribución de correo, que bajo una entrada LDAP, contengan los atributos necesarios que provean de esta capacidad de distribución, a la cuenta de correo destinataria:

Attribute Description	Value
objectClass	***inetLocalMailRecipient (auxiliary)***
objectClass	***inetOrgPerson (structural)***
objectClass	***organizationalPerson (structural)***
objectClass	***person (structural)***
objectClass	***top (abstract)***
cn	**Lista de prueba**
sn	**Prueba con lista**
mailLocalAddress	cc-rmazgon@canarias.org
mailLocalAddress	prueba@tfc-uoc.dyndns.org
mailLocalAddress	rmazgon@gmail.com
mailRoutingAddress	prueba-lista@tfc-uoc.dyndns.org
uid	prueba-lista

- **Servidor MTA de filtrado:** en este servidor se ha establecido un encadenado de filtrado, basado en un primer filtro anti-spam, mediante la solución de SpamAssasin, un segundo filtro de anti-visrus, mediante la solución ClamAV, y finalmente una devolución del correo, a los servidores frontales de correo, a través de un "canal asegurado" en los MTA frontales, al que sólo puede acceder el MTA filtrador, dado que este canal asegurado se encuentra supervisado por TCP Wrappers:



Cabe destacar que un punto crítico en este rol, es el proceso de actualizaciones de los distintos motores de escaneo, ya que si los patrones de virus y spam no son convenientemente actualizados, el sistema de filtrado puede degenerar en un sistema poco útil para la organización:



Adicionalmente también se han parametrizados distintos tipos de opciones, que de cara a la administración, permitan hacer rigurosos análisis del tratamiento de nuestra solución de filtrado, dejando para ello marcas de checking en las cabeceras SMTP de cada correo tratado:

Tuning y seguridad

Desde el punto de vista del rendimiento de la plataforma, el tuning del sistema juega un papel importantísimo, que afectará de manera directa a la forma en que nuestro servidor gestione las distintas colas de mensajes (*spool de correo*). Así mismo, y dentro de este mismo escenario, los límites impongamos en las opciones de envío, garantizarán que usuarios mal-intencionados aprovechen descuidos de parametrización, para provocar ataques de denegación de servicio (DoS) sobre los servicios MTA. Es por todo esto que se han incluido distintas directivas de configuración, tanto preventivas como de tuning:

```
File  Edit  Tabs  Help

# Limites sobre los envios:
#  Size maximo del mensaje.
#
message_size_limit=52428800

# TUNING

# Tiempo maximo de espera en cola:
#  Minimizamos el tiempo de vida en las colas de correo deferred.
#  Minimizamos el tiempo de vida en las colas de correo bounce.
#  The minimal amount of time a message won't be looked at, and the minimal amount of time to stay
 away from a "dead" destination.
#  How long a message stays in the queue before it is sent back as undeliverable. Specify 0 for ma
il that should be returned immediately after the first unsuccessful delivery attempt.
#
maximal_queue_lifetime=2d
bounce_queue_lifetime=2d
minimal_backoff_time= 2000s
maximal_backoff_time= 6000s
```

Otro de los aspectos de seguridad que más han de estar controlados, bajo un sistema de correo distribuido, como es esta solución, es el de los accesos mediante autorización TCP Wrapper que incorpora el software de Postfix, y que permitirá a los hosts MTA conocidos de la solución, el poder usarse de *relay* entre ellos, sin necesidad de requerir autenticación mediante el uso de credenciales de usuario LDAP:

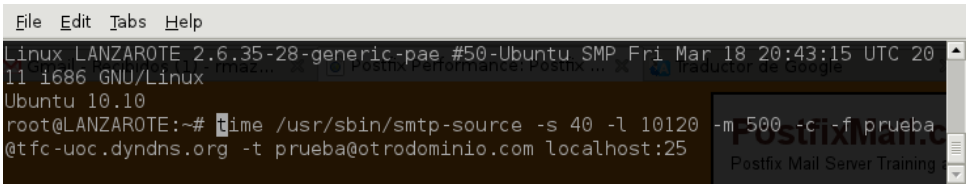
```
File  Edit  Tabs  Help

#
# Retorno desde el MTA filtrador (antivirus-antispam)
#
10025     inet  n       -       n       -       -       smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_client_restrictions=permit_mynetworks
  -o smtpd_recipient_restrictions=permit_mynetworks,check_relay_domains,reject
  -o mynetworks=127.0.0.1,192.168.5.5,192.168.5.12
```

Pruebas de control

Una vez implementada la solución del sub-sistema, es buena práctica el invertir tiempo en auditar la el nivel de capacidad de nuestra plataforma de correo, así como testar el nivel de fiabilidad a nivel de filtrado de correo.

Con el fin de evaluar estos parámetros, podemos hacer uso de herramientas puede como *smtp-source* y que en combinación combinan con otras herramientas de análisis del sisema (top, etc.), nos servirán para evaluar la carga en el servidor:

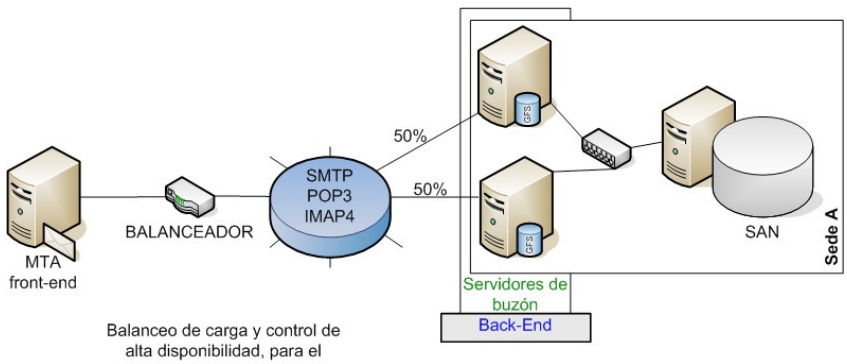


Como referencia, indicar que un nivel de aceptación óptimo para una plataforma de correo, puede ser el de aceptar y procesar de manera correcta, entre 300 y 600 correos electrónicos por minuto.

Alta disponibilidad, balanceo de carga y mejora de rendimiento

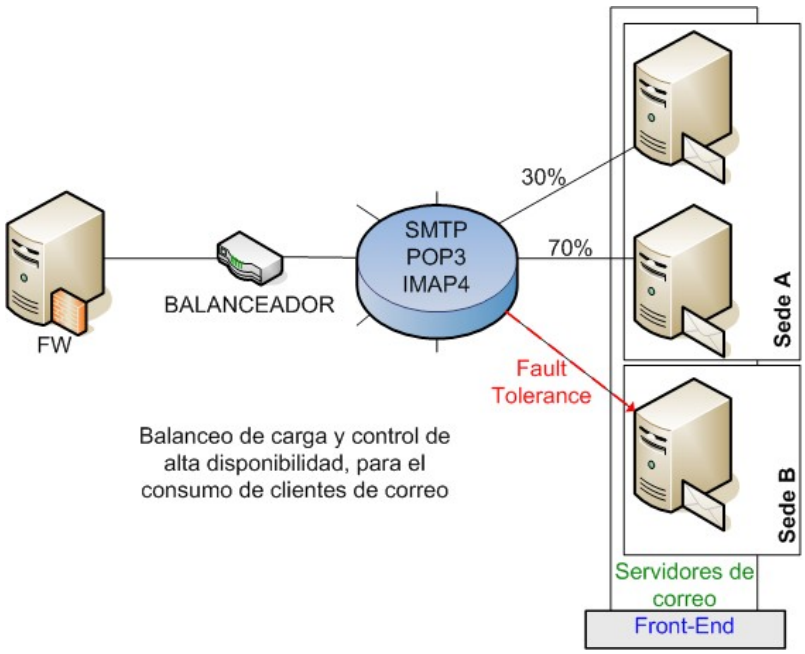
Al igual que en el caso de los servidores del sub-sistema de directorio de usuario, sería altamente recomendable para cualquiera de los tipos de servidores de la solución de correo, la opción de usar interfaces ethernet en bonding, de cara a proveer una solución *fault-tolerant*, que paralelamente ofrezca balanceo de carga, a nivel comunicación LAN.

Respecto a opciones hardware adicionales, el balanceo de carga y la alta disponibilidad a nivel de servidores de buzón puede estar gestionado por un balanceador hardware, configurado en alta disponibilidad y balanceo de carga, para satisfacer las peticiones de acceso POP3/IMAP4 a buzón. Además y con respecto a los servidores de buzón, dado que un buzón de correo ha de ser único, la opción de balanceo debería estar apoyada en alguna de solución de acceso concurrente al volumen de datos sobre el que se almacenen los buzones, que por ejemplo podría ser un volumen SAN, montado mediante sistema de ficheros GFS en todos los nodos que conformaran la plataforma de back-end de datos de buzón:



Balanceo de carga y control de alta disponibilidad, para el acceso a buzones de correo

Si atendemos al resto de servidores de la solución del sub-sistema de correo, el contar con electrónica hardware que permita balanceo de carga y alta disponibilidad, a nivel de granjas horizontales de servidores, supondría una mayor capacitación de procesamiento, además de una garantía de fiabilidad y continuidad para el servicio:



Sub-sistema de aplicaciones web

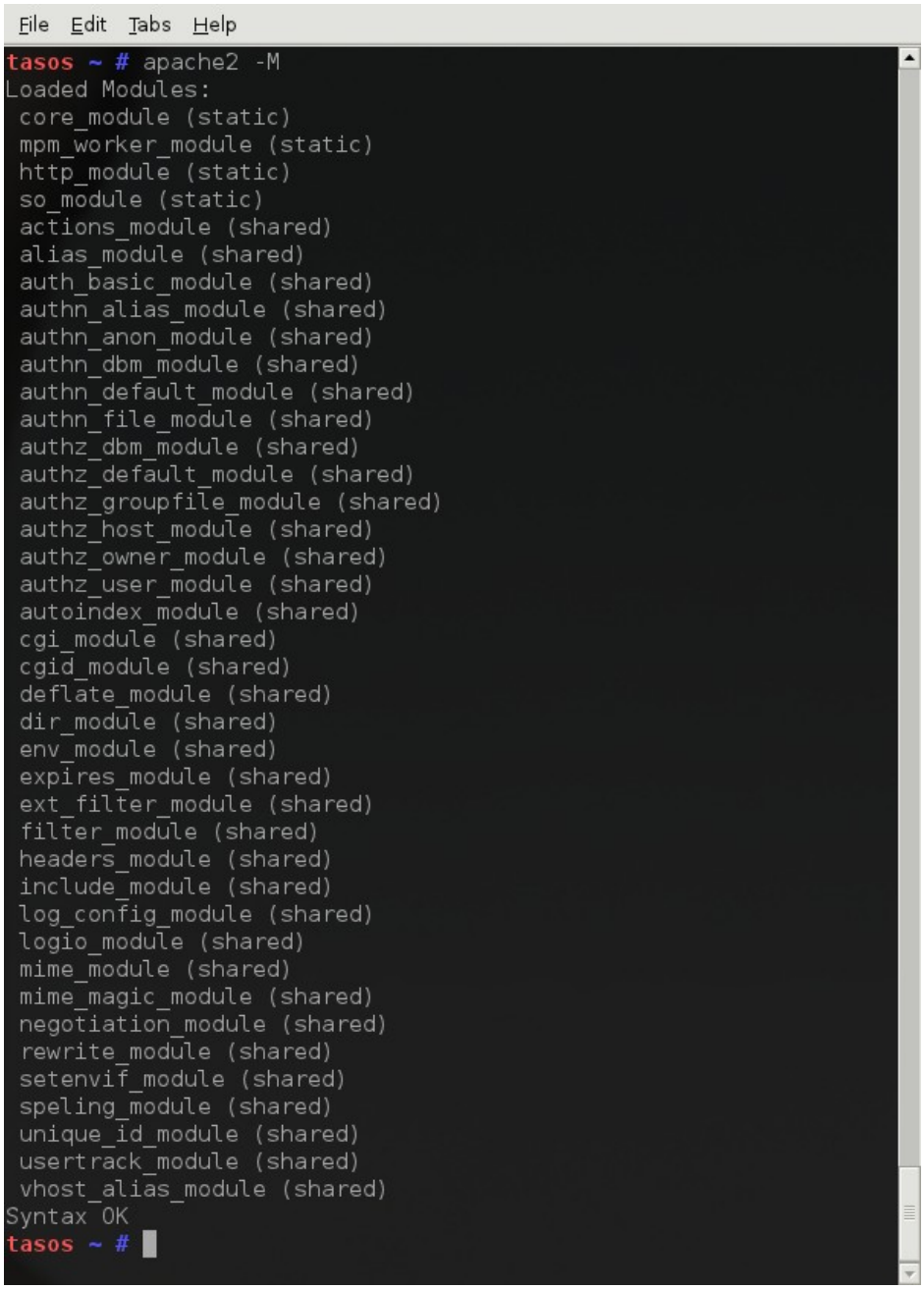
Se ha desplegado un sub-sistema de alojamiento web, que transversalmente han requerido una serie de servicios de base, sobre los que servir las aplicaciones de la solución:

- Suite de aplicaciones colaborativas escogido (EGroupWare).
- Aplicación de administración LDAP (phpLDAPadmin), para la gestión de cuentas de usuario del sistema.
- Aplciación a medida, a modo de auto-servicio de aprovisionado y desaprovisionado de usuarios.

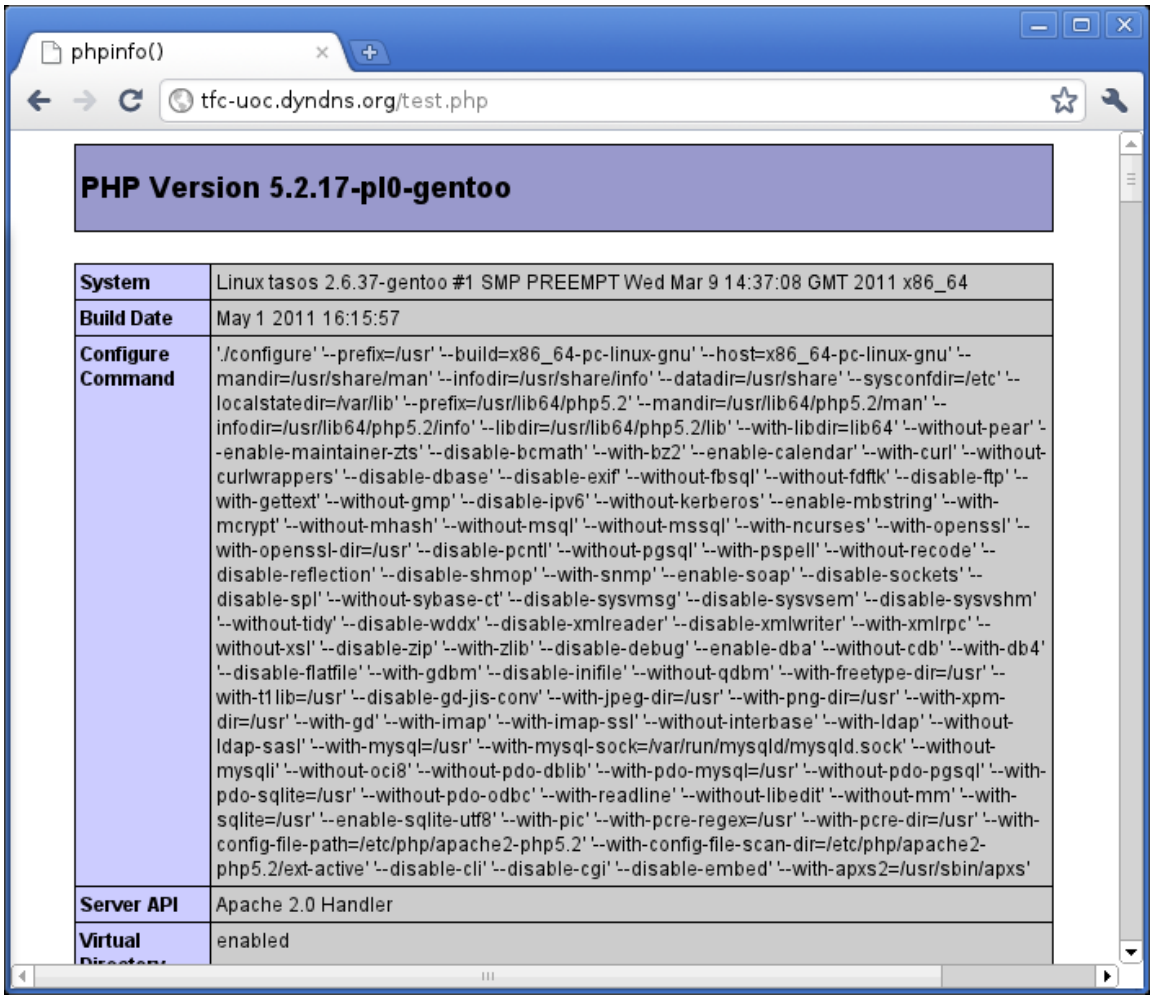
De cara a los servicios base comentados, (a modo de servicios transversales y necesarios para desplegar las aplicaciones que se incluyen en la plataforma), se han despegados las siguientes soluciones open source:

- **Servidor web Apache** montado sobre la línea de versionado 2.2. A su vez, y con respecto al soporte de las funcionalidades extra que puede proveer Apache web server, en base al linkado y asociación con otros módulos de terceros, se le ha provisto de capacidades como la de *mod_rewrite*, para gestionar reglas de re-direcciones y manipulaciones de URLs,

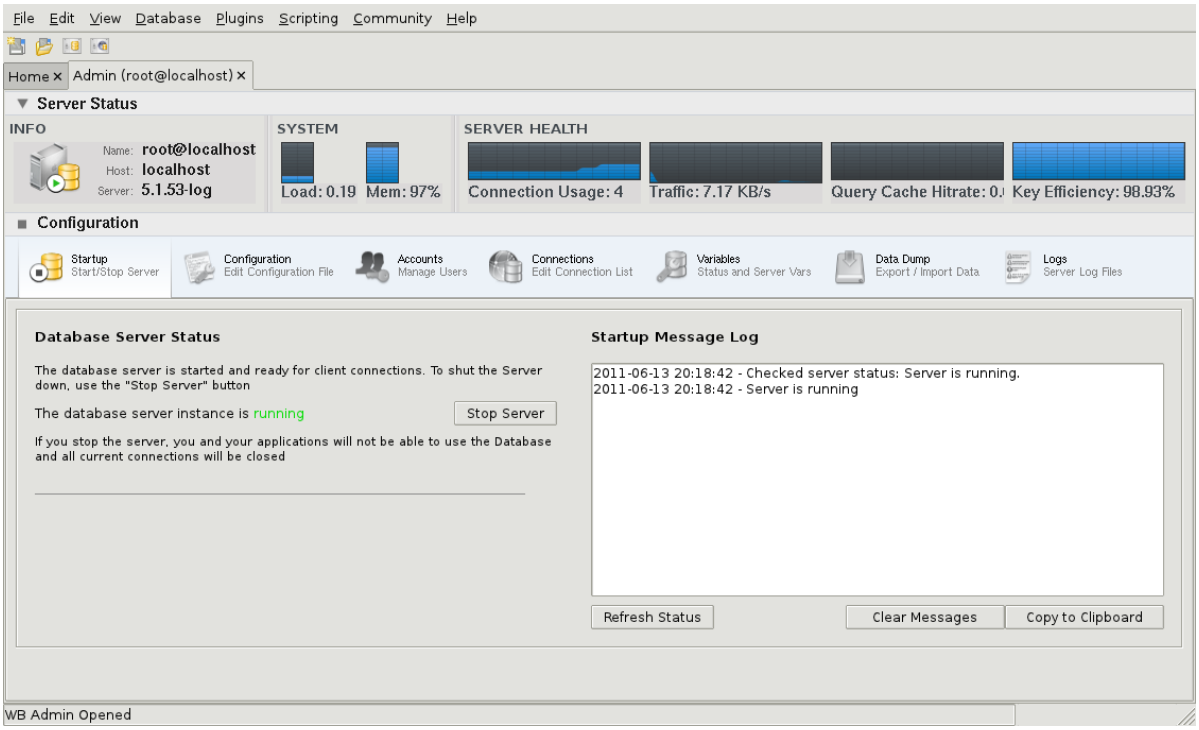
mod_php, para poder interpretar aplicaciones web dinámicas, programadas en PHP, y otra serie de módulos que pudieran ser interesantes, de cara a futuras utilizaciones:



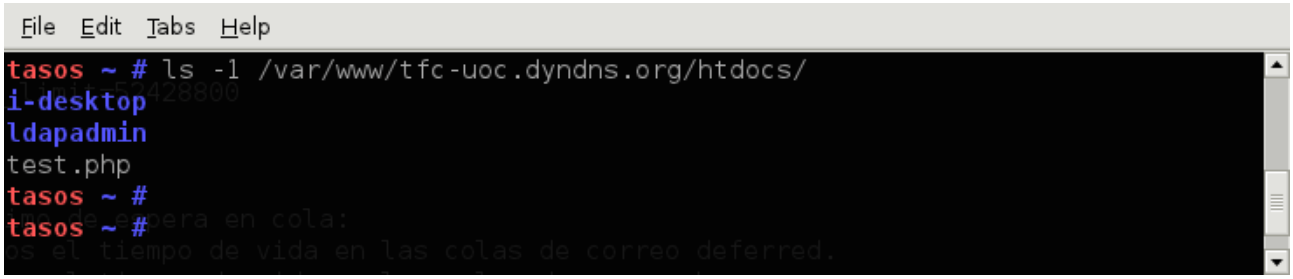
- **Intérprete PHP 5.2**, con linkado de compilación contra distintas librerías de sistema, que capaciten al intérprete del lenguaje PHP, de distintas funcionalidades y facilidades como:
  - Acceso a distintos soportes de bases de datos (PDO), entre ellos y específicamente, contra MySQL Server.
  - Acceso a buzones IMAP.
  - Acceso a LDAP.
  - *Etc*.



- **Gestor de bases de datos MySQL Server**, para albergar el back-end de datos, que requerirá el frame-work de aplicaciones colaborativas:



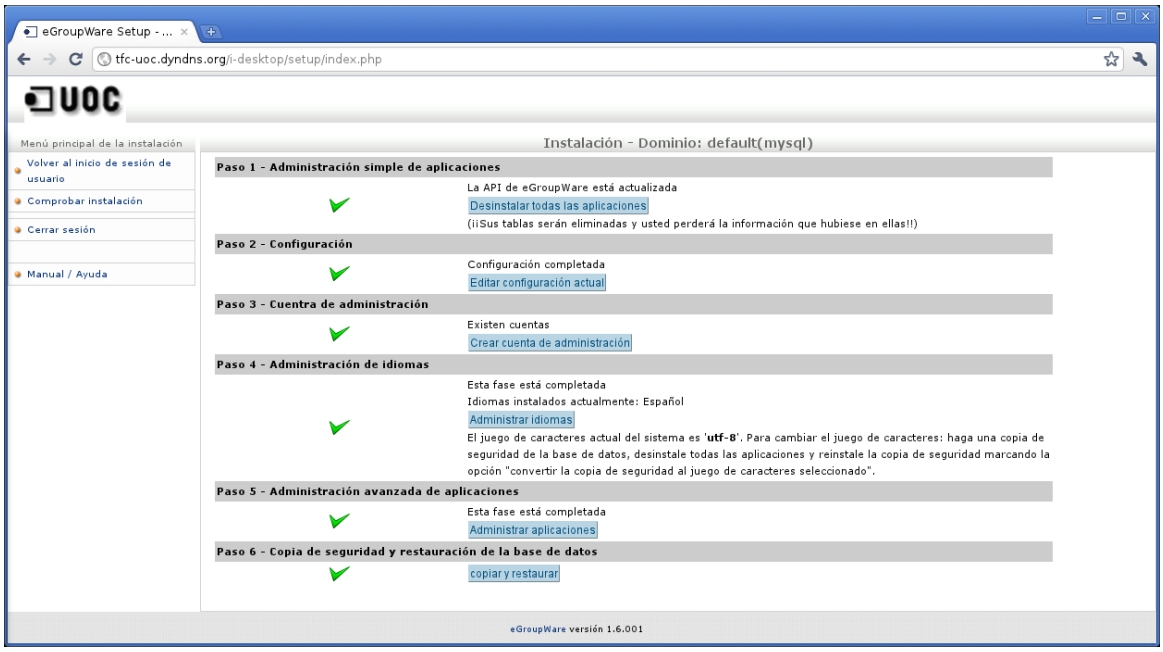
Una vez desplegados los servicios trasversales de este sub-sistema, el resto de acciones fue el de desplegar las aplicaciones de la solución, sobre el "`DocumentRoot`" del servidor Apache, y una vez desplegadas, proceder a su configuración e integración con el resto de los sub-sistemas:



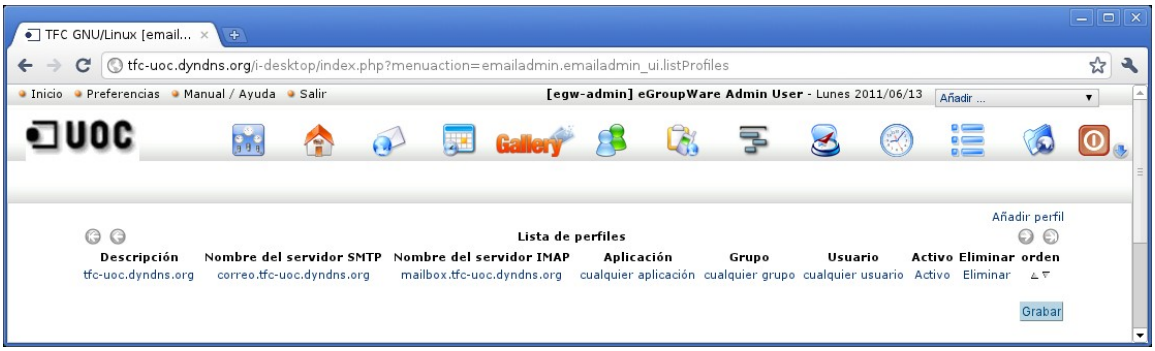
Configuración

Una ves desplegados los servicios transversales, se procedió a la instalación de la suite de aplicaciones colaborativas **EGroupWare**. Esta suite de aplicaciones requiere, entre otras cosas, de una base de datos, sobre la que almacenar preferencias individuales de cada una de las aplicaciones, por usuario y/o por grupo. Por el contrario, para el catálogo de usuarios de la suite, se ha utilizado el servicio de directorio de usuarios configurado previamente.

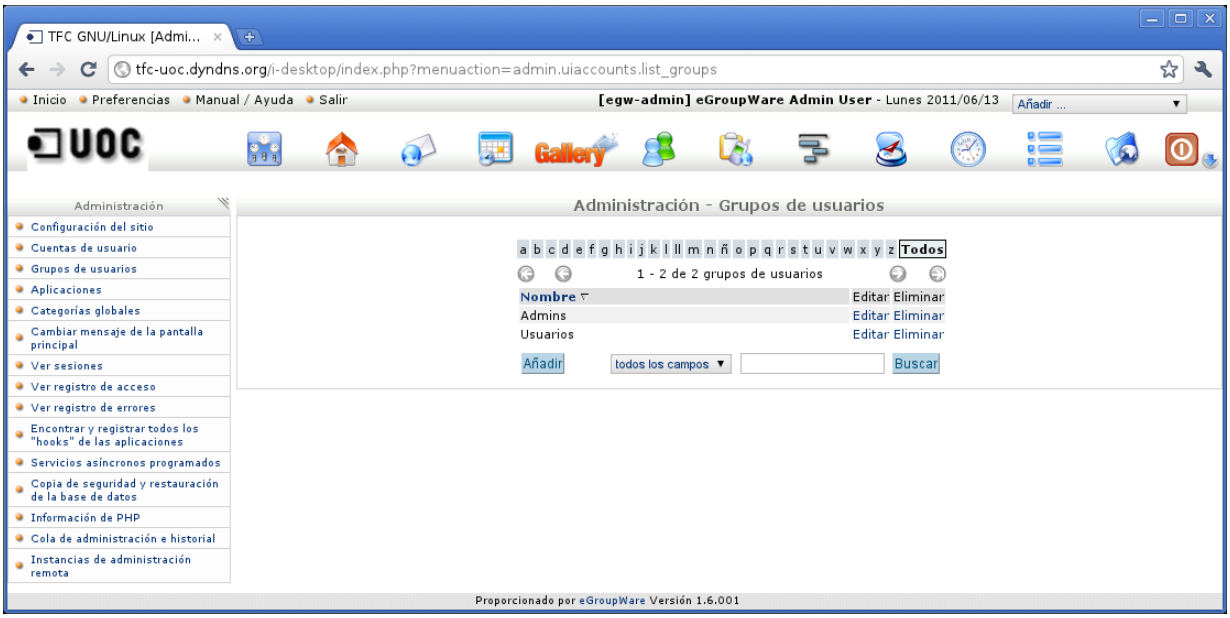
Durante la fase de despliegue de la suite, se establece la configuración básica del modo de funcionamiento, y tras esto, de procede a la instalación y puesta en producción de la suite:



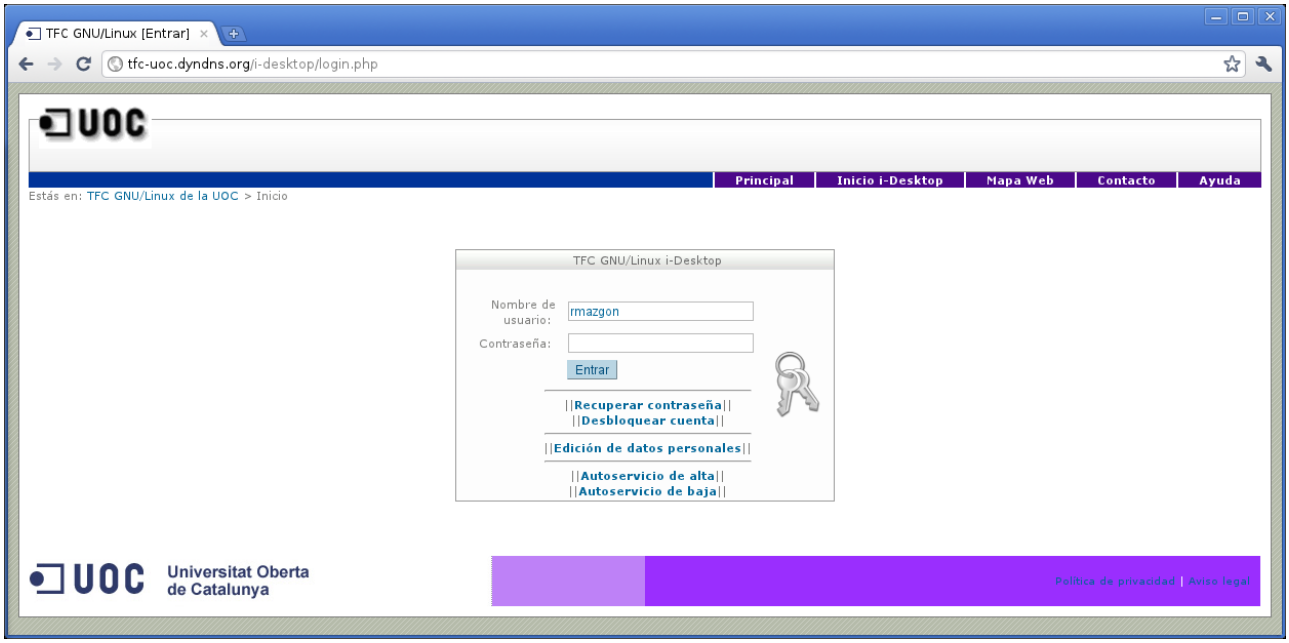
Después de estar finalizada la parte de instalación, se procedió a configurar la misma, también se procedió al anclaje entre el sub-sistema de correo, con el cliente webmail embebido de la suite, utilizando así mismo, el sub-sistema de directorio LDAP previamente configurado en la fase de despliegue e instalación de la suite:



Adicionalmente y de cara a proveer un nivel cómodo de administración de la accesibilidad a las aplicaciones, mediante el uso de grupos de usuarios, se configuraron los perfiles de aplicaciones asociados a estos:

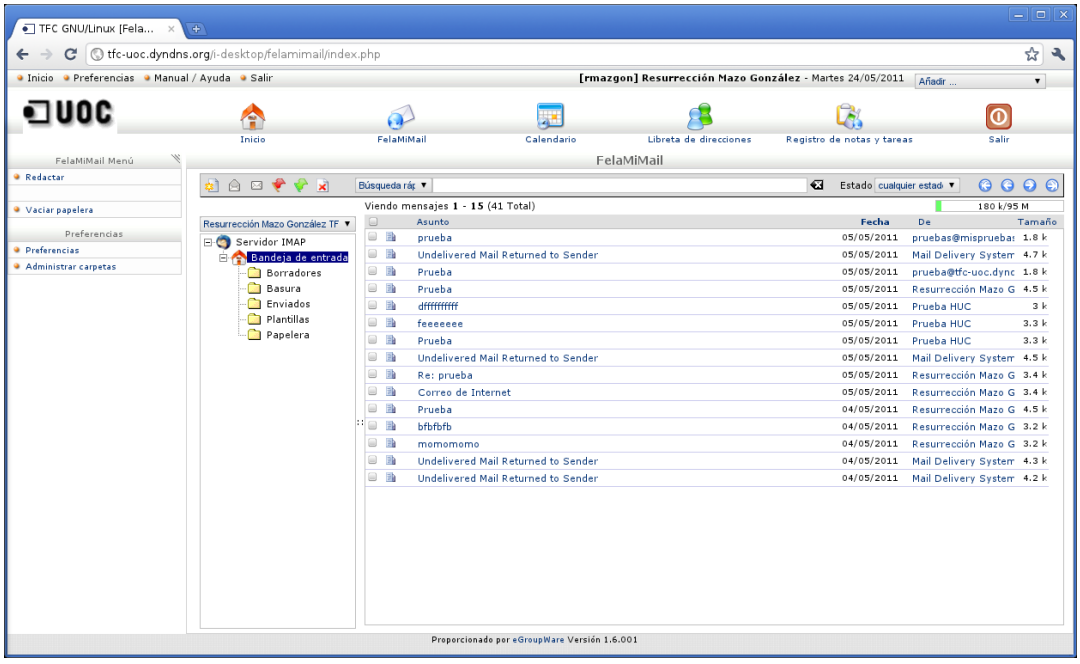


Una vez completada la configuración de grupos, se llevó a acabo la personalización del entorno web, de tal forma que la suite presentara un aspecto personalizado, acorde a la imagen corporativa que se escogió:

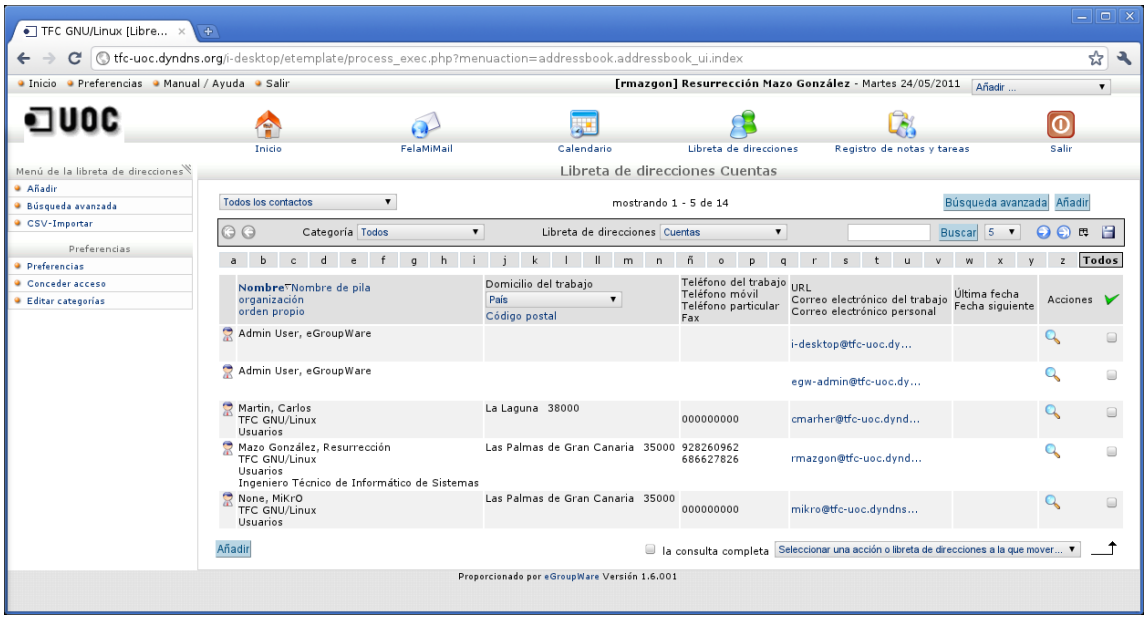


Finalmente se procedió a comprobar las distintas aplicaciones de que está provista la suite, con el resto de servicios provistos por los sub-sistemas que integran la solución:

- Integración de la aplicación **FelMiMail** de la suite, con el sub-sistema de correo:



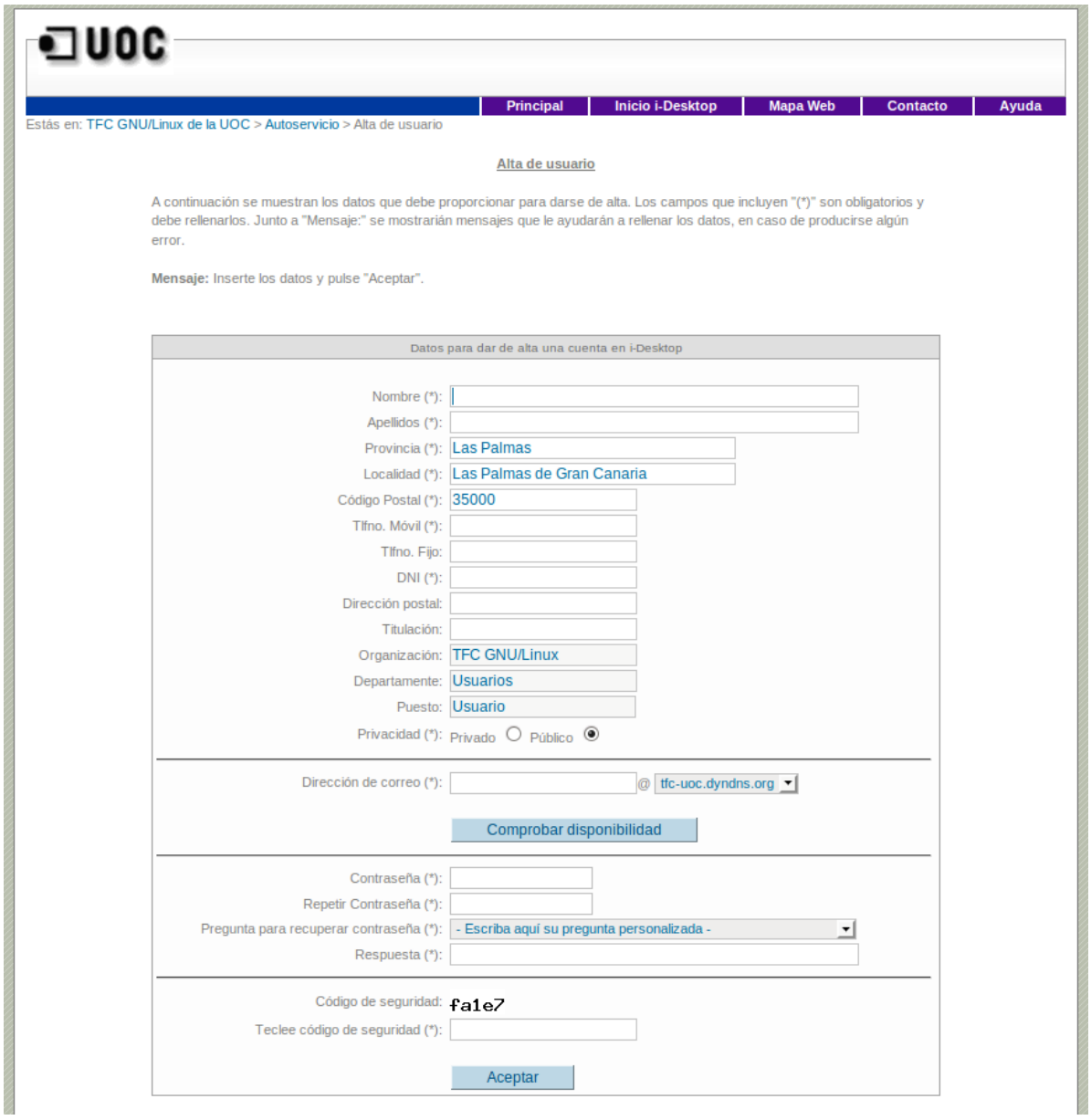
- Integración de la aplicación de **Libreta de direcciones**, con el sub-sistema de directorio:



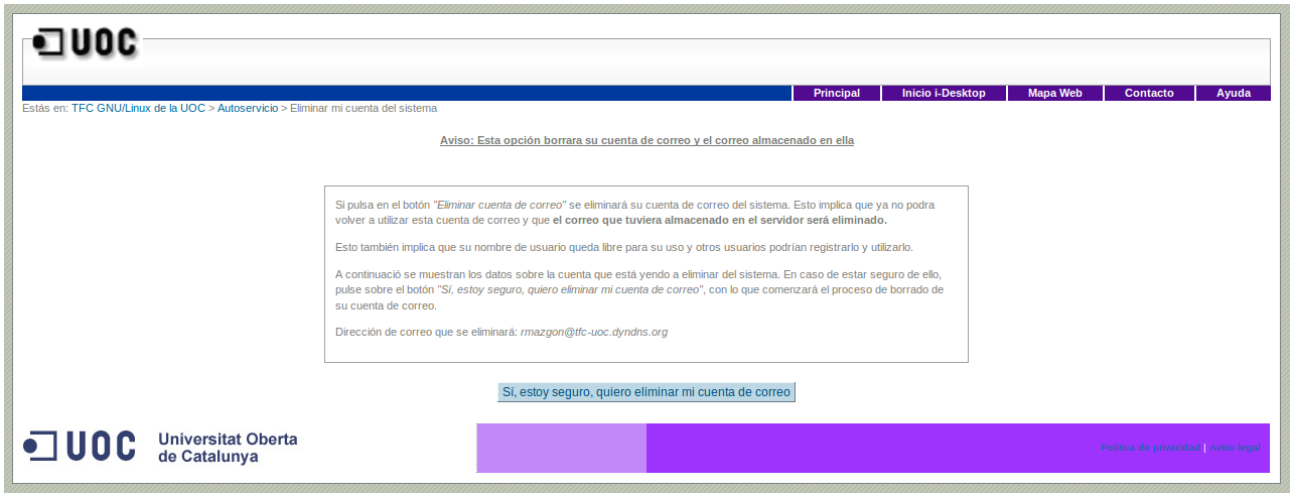
Después da la fase de vinculación entre los distintos sub-sistemas, se procedió a la elaboración de un completo autoservicio de aprovisionado, modificación y eliminación de usuarios del sistema, lo que dota a la corporación, de una solución de *service provider* personalizada y orientada a la incorporación de identidades en su haber de usuarios.

Entre las funcionalidades que este service provider provee al sistema, podemos incluir las siguientes:

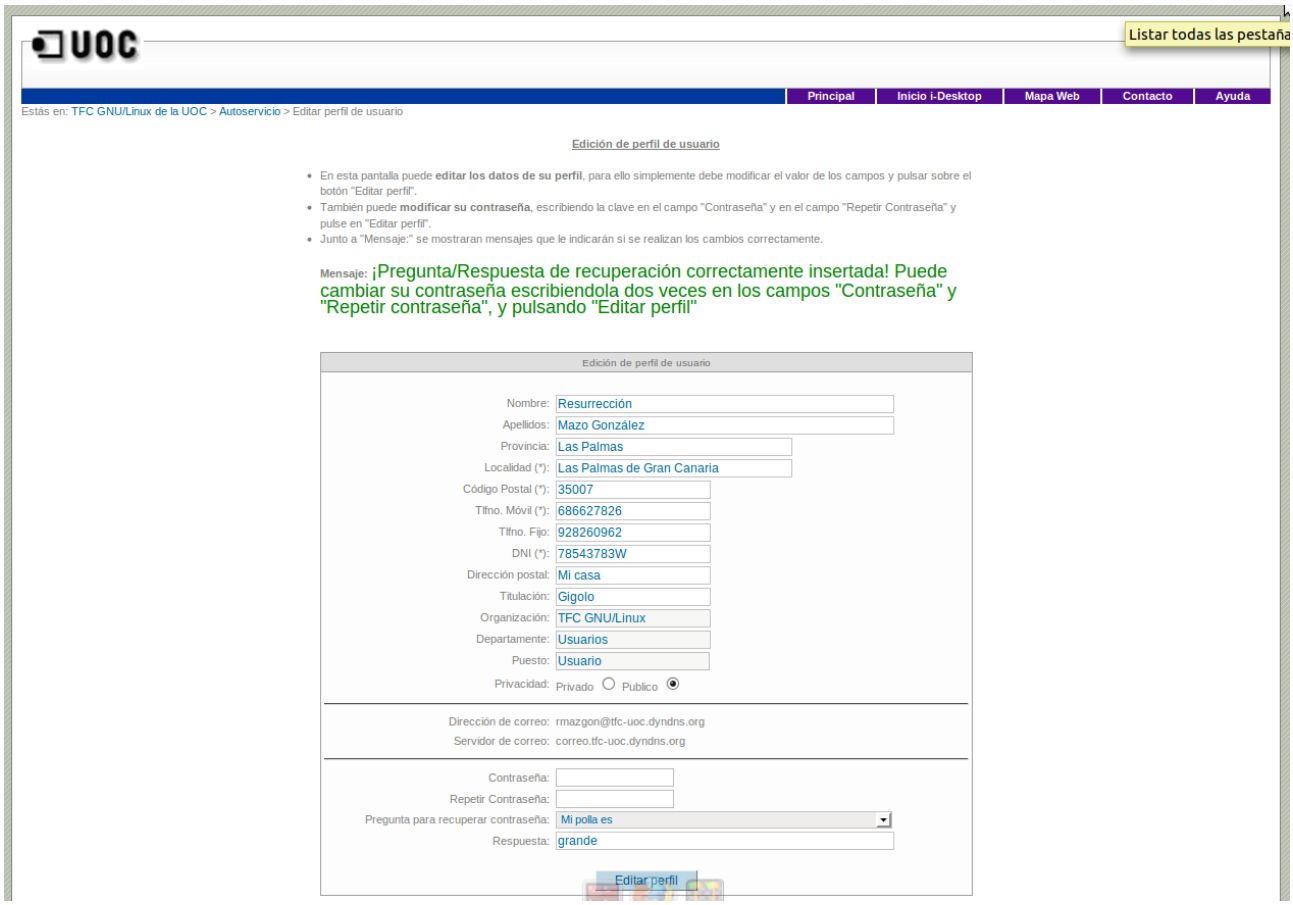
- Sistema de **auto-servicio de altas**:



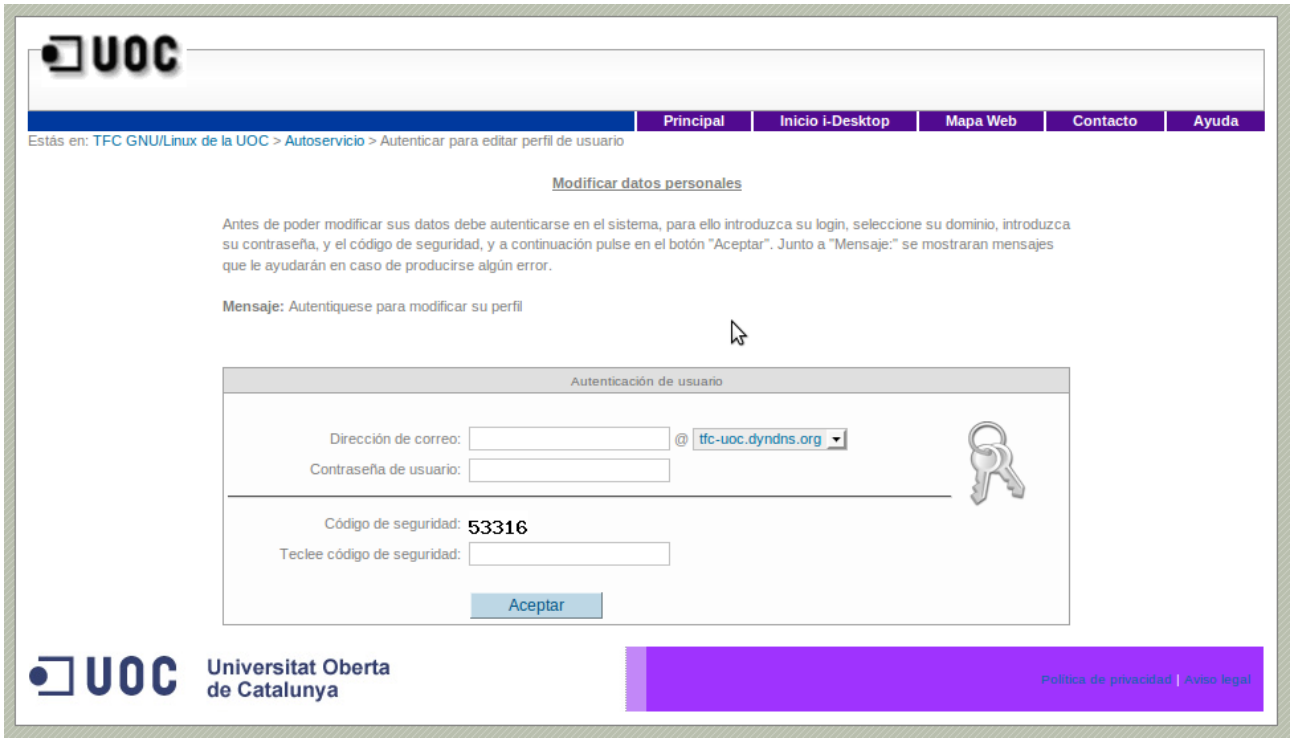
- Sistema de **auto-servicio de bajas**:



- Sistema de **recuperación de claves** y **desbloqueo de cuentas**:



- Sistema de **edición de perfiles de usuarios**:



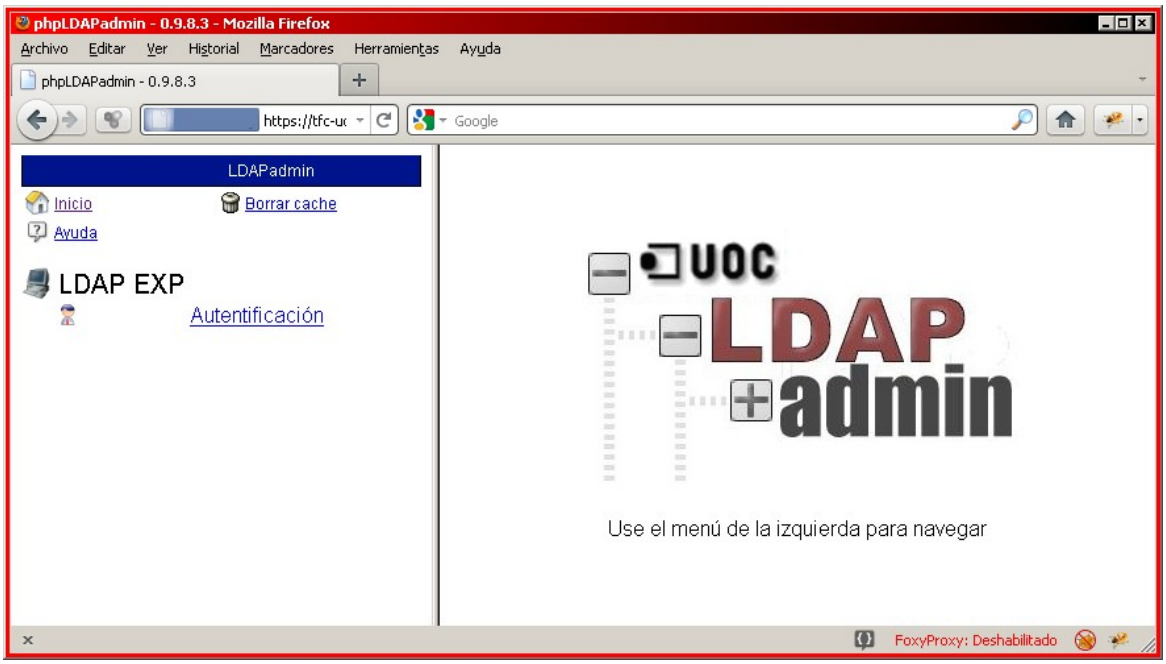
Cabe destacar que todo este conjunto de herramientas de service provider ha sido elaborado y programado, como solución a medida para este proyecto, lo que dota a la solución, de cierto valor añadido, con respecto a lo que supondría una simple labor de integración.

Para finalizar, y dentro del susb-sistema de aplicaciones web, y adicionalmente al autoservicio, se incluyó un front-end de gestión LDAP, basado en el software open source phpLDAPAdmin, que permite un fácil acoplamiento con cualquier servidor de directorio, que esté sujeto a los estándares LDAP.

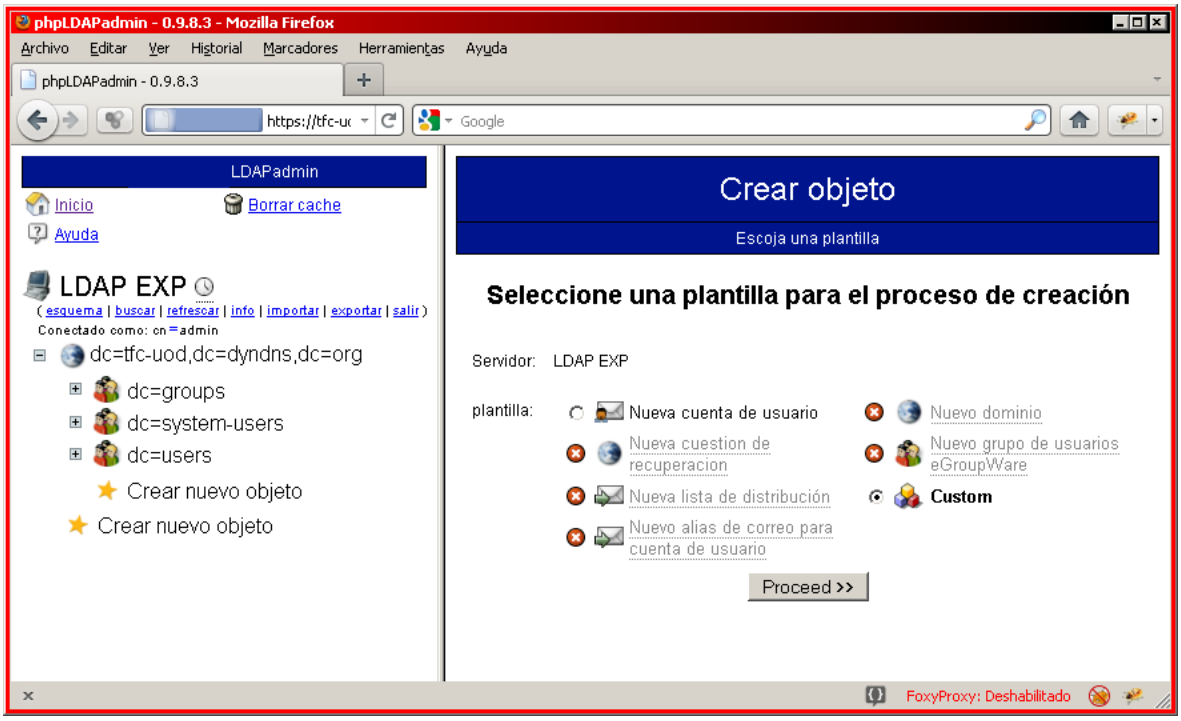
Mediante esta aplicación, la cual se reserva el acceso exclusivo para los administradores del entorno, se permite, de una forma cómoda y rápida, la gestión de los contenidos del directorio de usuarios. Para ello, se habilitaron distintas plantillas que permiten la creación de objetos del tipo usuario, así como otras plantillas, destinadas a la creación de cuentas de correo de listas de distribución. Así mismo, y de cara a la sincronización de datos de usuarios de la suite EGroupWare, se asociaron a las diferentes plantillas, una serie de los denominados "hooks" usados por esta aplicación, a modo de tareas SQL, para el aprovisionado a nivel de BBDD.

Algunas de las características de esta herramienta de gestión de cuentas son:

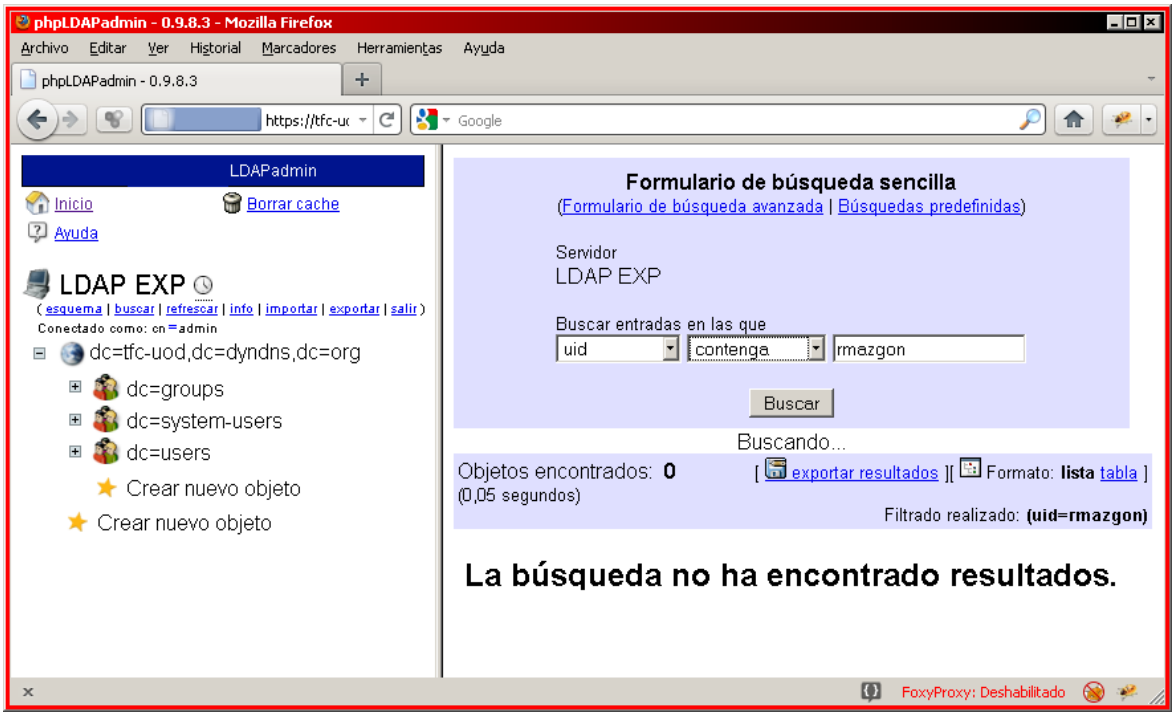
- Acceso a la aplicación de administración:



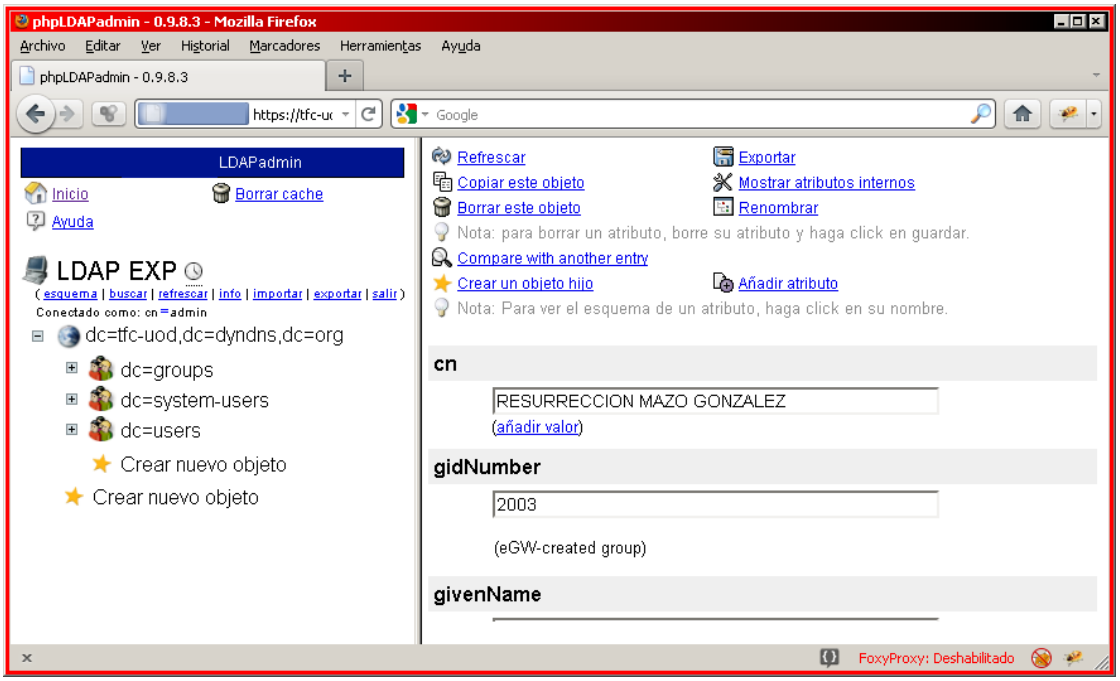
- Consola principal de gestión:



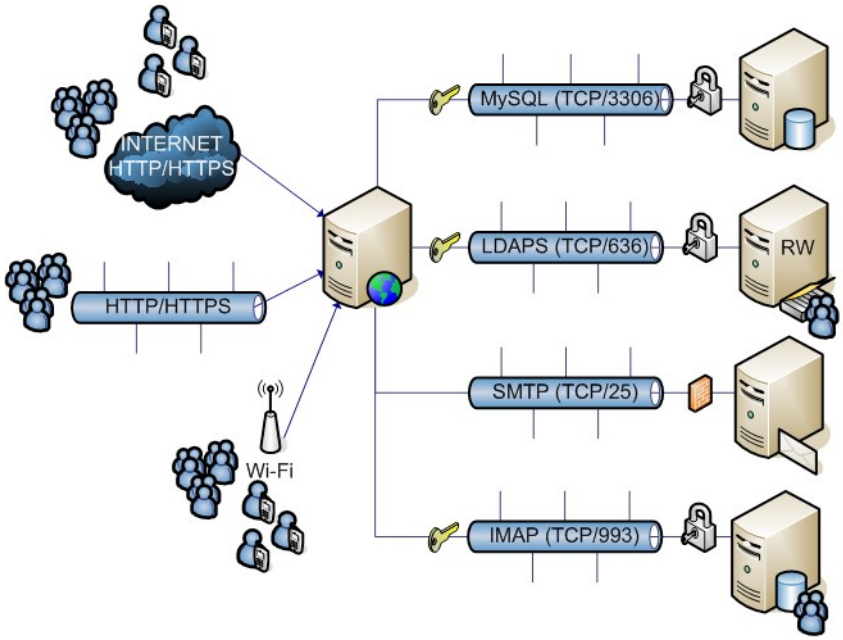
- Búsqueda de usuarios del sistema:



- Edición de usuarios:



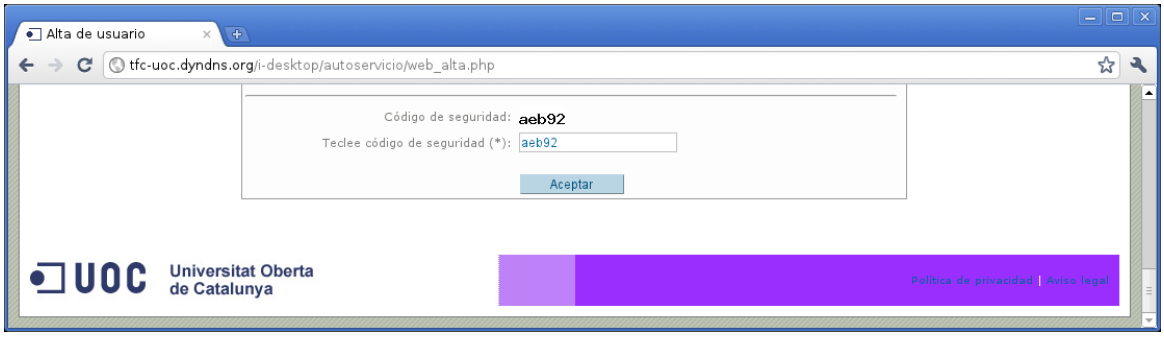
Como resultado final a todo este despliegue, la imagen final de este sub-sistemas, engranado con el resto de los sub-sistemas de correo y de directorio de usuarios, vendría descrito mediante el siguiente esquema topológico:



Tuning y seguridad

Aunque los niveles de seguridad web exceden el propósito de este proyecto, se ha puesto especial atención en la publicación de los contenidos en sólo lectura, de cara a que cualquier error de las aplicaciones PHP pudieran provocar accesos intrusivos no deseados a los file systems del servidor.

Además de esta medida, y ya de cara a la securización de las aplicaciones web de que se compone este sub-sistema, se han incluido métodos de control a nivel de autenticación, como el uso de HTTPS, el uso de bloque de cuentas, ante exceso de intentos fallidos de validación de usuario, para evitar ataques de fuerza bruta, o la utilización de dispositivos *captcha*, para evitar robots que puedan causar un desbordamiento del sistema, mediante el autoservicio de aprovisionado:



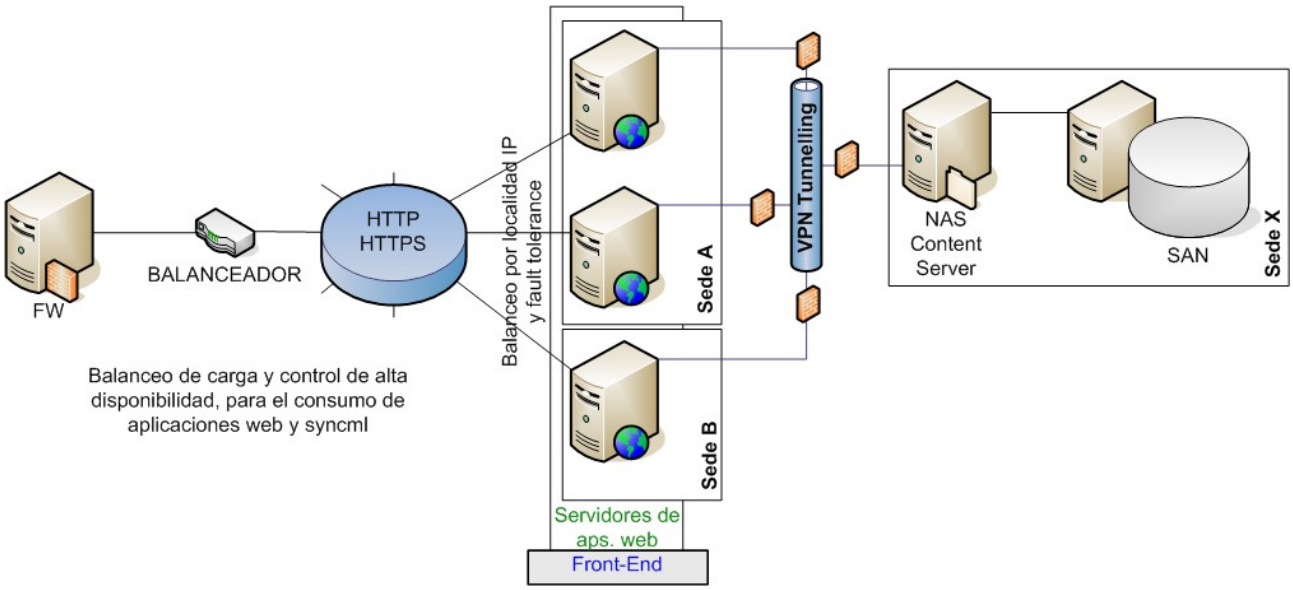
Pruebas de control

Bajo este sub-sistema, es viable el utilizar software de estrés web, para poder testar la capacidad de nuestra plataforma, pero no garantizará que las aplicaciones web alojadas en el, puedan presentar errores de configuración, o *bugs*. Es por ello que para este sub-sistema, se exige una labor profunda de pruebas, que muchas veces será diferente, en base a las pretensiones que la organización tenga para con la suite EGroupWare.

Alta disponibilidad, balanceo de carga y mejora de rendimiento

Análogamente que en el caso de los servidores de los otros sub-sistemas, sería altamente recomendable para cualquiera de los tipos de servidores de la solución de correo, la opción de usar interfaces ethernet en bonding, de cara a proveer una solución *fault-tolerant*, que paralelamente ofrezca balanceo de carga, a nivel comunicación LAN.

Respecto a opciones hardware adicionales, el balanceo de carga y la alta disponibilidad a nivel del servicio web puede estar gestionado por un balanceador hardware, configurado en alta disponibilidad y balanceo de carga, para satisfacer las peticiones de acceso HTTP. Además y con respecto a los contenidos servidos por la granja horizontal de estos servidores web, se podría usar alguna solución de acceso concurrente al volumen de datos sobre el que se almacenen, por ejemplo mediante un servidor físico de NAS, que publique los susodichos contenidos en modo RO (*read only*), mediante el protocolos NFS:



PLAN DE PRUEBAS

Sub-sistema de directorio de usuarios

Dentro de este sub-sistema se tendrán que verificar una serie de mínimos funcionales, para garantizar la operatividad del mismo:

- ✔ Verificación de adición de entradas.
- ✔ Verificación de edición de entradas.
- ✔ Verificación de eliminación de entradas.
- ✔ Verificación de autenticación mediante BIND.

Adicionalmente a estas verificaciones básicas, se han de comprobar otros aspecto más operativos, de acuerdo a la política de explotación definida por la organización:

- ✔ Comprobación de reglas de acceso.
- ✔ Comprobación del correcto funcionamiento de constraints (por ejemplo, el de unicidad del atributo mail).
- ✔ Comprobación de límites de cliente, para evitar la denegación del servicio (DoS).
- ✔ Comprobación de la indexación de atributos.
- ✔ Comprobación de la correcta replicación entre nodos maestro y réplicas.

Control de calidad y del riesgo

La medida de calidad vendrá dado por el nivel de estrés que nuestro servidor o servidores de directorio soporten. Para ello y mediante herramientas de test y estrés, será necesario no sólo calcular la capacidad de nuestra plataforma de directorio, sino asegurar unos servicios mínimos. Entre estos tests podemos estudiar:

- ✔ Capacidad media de búsquedas (entradas por segundo).
- ✔ Capacidad media de modificaciones (entradas por segundo).
- ✔ Capacidad media de eliminaciones (entradas por segundo).
- ✔ Capacidad media de autenticaciones (entradas por segundo).
- ✔ Capacidad media de operaciones combinadas (entradas por segundo).

Sub-sistema de correo electrónico

Dentro de este sub-sistema se tendrán que verificar una serie de mínimos funcionales, para garantizar la operatividad del mismo:

- ✔ Verificación de envío autenticado de correo vía SMTP.
- ✔ Verificación de envío autenticado de correo vía SSMTP.
- ✔ Verificación de acceso a buzón de correo vía POP3.
- ✔ Verificación de acceso a buzón de correo vía POP3S.
- ✔ Verificación de acceso a buzón de correo vía IMAP.
- ✔ Verificación de acceso a buzón de correo vía IMAPS.
- ✔ Verificación de suscripciones a carpetas IMAP.

Adicionalmente a estas verificaciones básicas, se han de comprobar otros aspecto más operativos, de acuerdo a la política de explotación definida por la organización:

- ✔ Comprobación de open relay no permitido.
- ✔ Comprobación de antifalsificación de emisor.
- ✔ Comprobación de RBLs.
- ✔ Comprobación de filtrado antivirus.
- ✔ Comprobación de filtrado antispam.
- ✔ Comprobación de límites de correo.
- ✔ Tamaño máximo del mensaje enviado.
- ✔ Número máximo de destinatarios en un envío.
- ✔ Cuotas de buzón.
- ✔ Funcionamiento de forwards de cuentas de correo de usuario.
- ✔ Funcionamiento de listas de distribución de correo.

Control de calidad y del riesgo

La medida de calidad vendrá dado por el nivel de estrés que nuestro servidor o servidores de correo soporten. Para ello y mediante herramientas de test y estrés, será necesario no sólo calcular la capacidad de nuestra plataforma de correo electrónico, sino asegurar unos servicios mínimos. Entre estos tests podemos estudiar:

- ✔ Capacidad de tramitación SMTP de correos (número de mensajes por minuto).
- ✔ Capacidad de filtrado de correos (número de mensajes por minuto).
- ✔ Velocidad de descarga de mensajes de buzón vía POP3 (número de mensajes por minuto).
- ✔ Velocidad de descarga de cabeceras de mensajes de buzón vía IMAP4 (número de mensajes por minuto).
- ✔ Velocidad de descarga de mensajes de buzón vía IMAP4 (número de mensajes por minuto).
- ✔ Capacidad de concurrencia de accesos a buzón vía POP3.
- ✔ Capacidad de concurrencia de accesos a buzón vía IMAP4.

Sub-sistema de aplicaciones web

Dentro de este sub-sistema se tendrán que verificar una serie de mínimos funcionales, para garantizar la operatividad del mismo:

- ✔ Verificación de las funcionalidades de la suite EGrouWare:
  - ■ Acceso autenticado.
  - ■ Acceso a los buzones de correo, mediante el cliente web embebido.
  - ■ Acceso a los contactos del directorio LDAP.
- ✔ Verificación de las funcionalidades del autoservicio:
  - ■ Auto-aprovisionado.
  - ■ Auto-desprovisionado.
  - ■ Modificación de datos personales.
  - ■ Desbloqueo de cuenta.
  - ■ Recuperación de contraseña mediante pregunta secreta.
- ✔ Verificación de las funcionalidades del phpLDAPadmin:
  - ■ Acceso autenticado para administradores.
  - ■ Búsquedas de entradas.
  - ■ Modificaciones de entradas.
  - ■ Aprovisionado de entradas.

Adicionalmente a estas verificaciones básicas, se han de comprobar otros aspecto más operativos,

de acuerdo a la política de explotación definida por la organización:

- ✔ Comprobación de reglas de acceso.
- ✔ Comprobación de reglas mod_rewrite.
- ✔ Comprobación de interpretación de contenidos PHP.
- ✔ Comprobación de gestión de sesiones PHP.
- ✔ Comprobación de tipos MIME soportados.
- ✔ Comprobación de permisos de los contenidos en sólo lectura.

Ya dentro de cada una de las aplicaciones web, y dependiendo del modo en que los administradores hayan decidido configurarlas, serán necesario probar distintas funcionalidades de uso, como pueden ser:

- ➢ Compartir eventos de calendario.
- ➢ Crear contactos en la libreta de direcciones.
- ➢ Sincronizar los datos PIM con dispositivos compatibles con SyncML.
- ➢ *Etc*.

Queda fuera del alcance de este proyecto, el llegar a abordar al completos las distintas aplicaciones que soporta, pues estas están sujetas a infinidad de posibilidades, todas ellas caracterizables según necesidades de la organización.

Control de calidad y del riesgo

La medida de calidad vendrá dado por el nivel de estrés que nuestro o nuestros servidores de aplicaciones web. Para ello y mediante herramientas de test y estrés, será necesario no sólo calcular la capacidad de nuestra plataforma de web, sino asegurar unos servicios mínimos. Entre estos tests podemos estudiar:

- ✔ Capacidad de transacciones servidas (HITs por minuto).
- ✔ Capacidad de conexiones concurrentes.
- ✔ Capacidad de conexiones sobre SSL/TLS (HTTPS).

PLAN DE GARANTÍA Y SOPORTE

Los profesores que evalúan esta memoria podrán formular preguntas por correo electrónico sobre aspectos que consideren importantes, a raíz del siguiente SLA:

- **Vigencia**: del 20 al 24 de junio.
- **Cobertura**: 24x7.
- **Tiempo máximo de respuesta**: no más de 24 horas.
- **Medios de comunicación disponibles**: correo electrónico.

GLOSARIO

Alta disponibilidad: alta disponibilidad (*High availability*) es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado. Disponibilidad se refiere a la habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un usuario no puede acceder al sistema se dice que está no disponible. El término tiempo de inactividad (*downtime*) es usado para definir cuándo el sistema no está disponible.

Arquitectura Intel: es la denominación genérica dada a ciertos microprocesadores de la familia Intel, sus compatibles y la arquitectura básica a la que estos procesadores pertenecen, por la terminación de sus nombres numéricos: 8086, 80286, 80386, 80486, etc. Han constituido desde su nacimiento un estándar para los ordenadores del tipo Compatible IBM PC.

Back-end: en el mundo software, los back-end son responsables del acceso en último instancia, a los datos de aplicación, y que generalmente son accedidas desde sistemas front-end.

Balanceo de carga: el balance o balanceo de carga es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.

Bonding: es una técnica para unir dos tarjetas de red como una sola. Está implementado con el protocolo de agregación de enlaces (803.2ad) y permite configuraciones que son resistentes a cambiar, enlace ascendente, NIC y tolerancia a fallos.

Bug: es un defecto de software (computer bug en inglés), resultado de un fallo o deficiencia durante el proceso de creación de programas de ordenador o computadora (software). Dicho fallo puede presentarse en cualquiera de las etapas del ciclo de vida del software aunque los más evidentes se dan en la etapa de desarrollo y programación. Los errores pueden suceder en cualquier etapa de la creación de software.

CAPTCHA: es el acrónimo de *Completely Automated Public Turing test to tell Computers and Humans Apart* (Prueba de Turing pública y automática para diferenciar máquinas y humanos). Se basa en un test de secuencia que dificulta el reconocimiento de la máquina, distorsionando las letras y añadiendo un degradado de fondo.

CIFS: *Common Internet File System* (CIFS) es un protocolo de red (que pertenece a la capa de aplicación en el modelo OSI), que permite compartir archivos e impresoras (entre otras cosas) entre los nodos de una red de ordenadores. Fue originalmente llamado SMB (S*erver Message Block*), pero Microsoft lo renombró SMB a CIFS en 1998, añadiéndole más características, que incluyen soporte para enlaces simbólicos, enlaces duros (hard links), y mayores tamaños de archivo.

Cluster: el término cluster se aplica a los conjuntos o conglomerados de computadoras construidos

mediante la utilización de componentes de hardware comunes y que se comportan como si fuesen una única computadora.

Datos PIM: acrónimo usado comúnmente en referencia a la gestión de información personal, como un campo de estudio. El propósito de una herramienta de PIM es el de facilitar el registro, seguimiento y gestión de determinados tipos de "información personal"

Directorio de usuario: es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Además, los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos.

DIT: un árbol de información de directorio (*Directory Information Tree*, DIT) es la representación de datos en una estructura jerárquica de árbol formado por los nombres completos (DN) de las entradas de servicio de directorio.

DNS: *Domain Name System* o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (*resolver*) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Ethernet: es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD. (*Acceso Múltiple por Detección de Portadora con Detección de Colisiones*), es una técnica usada en redes Ethernet para mejorar sus prestaciones.

Fault-tolerant: bajo computación, es la propiedad que permite a un sistema seguir funcionando correctamente en el caso de la falta de (o una o más faltas dentro de) algunos de sus componentes. Es particularmente sobre sistemas críticos en un organización.

Forward de correo: se utiliza para la operación de mandar a otra dirección de correo electrónico, un mensaje que se ha recibido.

Front-end: en el mundo software, los front-end son responsables de la vinculación de las aplicaciones cliente y sus redes asociadas a las aplicaciones basadas en hosts de back end. Con el advenimiento de Internet y del protocolo TCP/IP, como un protocolo universal, a menudo hay necesidad los front end, de cara a optimizar comunicaciones, o implementar niveles de seguridad.

Host: el término host es usado en informática para referirse a las computadoras conectados a una red, que proveen y utilizan servicios de ella.

HTTP: *Hypertext Transfer Protocol* o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la *World Wide Web*. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que

especifica la versión 1.1.

IMAP: *Internet Message Access Protocol*, o su acrónimo IMAP, es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

Inbound (traffic): son los datos que se reciben en un ordenador, desde otro equipo.

ISP: un proveedor de servicios de Internet (o ISP, por la sigla en inglés de **Internet Service Provider**) es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cablemódem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, servidores de noticias, etc.

LAN: una red de área local, red local o LAN (del inglés *local area network*) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.

LDAP: son las siglas de *Lightweight Directory Access Protocol* (en español Protocolo Ligero de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Lista de distribución de correo electrónico: las listas de correo electrónico son un uso especial del correo electrónico que permite la distribución masiva de información, entre múltiples usuarios de Internet, a la misma vez. En una lista de correo se escribe un correo a la dirección de la lista (ej: silet@correo.org) y le llega masivamente a todas las personas inscritas en la lista, dependiendo de como esté configurada la lista de correo, el receptor podrá o no tener la posibilidad de enviar correos.

MPLS: siglas de *Multiprotocol Label Switching*, es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MTA: Agente de Transferencia de Correo (del inglés *Mail Transport Agent* o MTA; también *Message Transport Agent*, Agente de Transporte de Mensajes) es uno de los programas que ejecutan los servidores de correo, y tiene como fin transferir un conjunto de datos de una computadora a otra.

MySQL: es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones. MySQL AB —desde enero de 2008 una subsidiaria de Sun Microsystems y ésta a su vez de Oracle Corporation desde abril de 2009— desarrolla MySQL como software libre en un esquema de licenciamiento dual.

NAS: del inglés *Network Attached Storage*, es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

NFS: el *Network File System* (Sistema de Archivos de Red), o NFS, es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.

NTP: *Network Time Protocol* (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

OpenSSL: es un proyecto de software desarrollado por los miembros de la comunidad Open Source para libre descarga y está basado en SSLeay, desarrollado por Eric Young y Tim Hudson.

Outbound (traffic): son los datos que se transmiten desde un ordenador, a otro equipo.

P-t-P: un enlace *Poit-To-Point* topológicamente es un enlace simple y permanente entre dos extremos de una red. Las topologías de conmutación de punto a punto son el modelo básico de la telefonía convencional. El valor de una red permanente de punto a punto es libre comunicación entre los dos extremos.

POP: *Post Office Protocol* (POP3, Protocolo de la Oficina de Correo) es un protocolo que se utiliza en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.

Proxy: en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina “a” solicita un recurso a una “c”, lo hará mediante una petición a “b”; “c” entonces no sabrá que la petición procedió originalmente de “a”.

PYME: la *Pequeña Y Mediana Empresa* (conocida también por el acrónimo PYME, actualmente sustantivizado como pyme) es una empresa con características distintivas, y tiene dimensiones con ciertos límites ocupacionales y financieros prefijados por los estados o regiones. Las pymes son agentes con lógicas, culturas, intereses y un espíritu emprendedor específicos.

RBL: en términos de correo electrónico, una RBL, también llamada DNSBL (*Lista Blackhole basadas en DNS, lista de bloqueo, o lista negra*) es una lista de direcciones IP accesible mediante consultas de nombres (DNS), que se puede consultar en tiempo real, que se utiliza para publicar las direcciones de los ordenadores o redes relacionadas con correos no deseados. La mayoría de software de servidor de correo puede ser configurado para rechazar o marcar los mensajes que han sido enviados desde un sitio protegido por una o más listas.

RFC: las *Request For Comments* (Petición De Comentarios, en español) son una serie de notas

sobre Internet, que comenzaron a publicarse en 1969. Se abrevian como RFC y que resultas lo suficientemente interesante, pueden llegar a convertirse en estándares de Internet.

SAN: una red de área de almacenamiento, (en inglés *Storage Area Network*), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

SDH: la jerarquía digital síncrona (*Synchronous Digital Hierarchy*) , se puede considerar como la revolución de los sistemas de transmisión, como consecuencia de la utilización de la fibra óptica como medio de transmisión, así como de la necesidad de sistemas más flexibles y que soporten anchos de banda elevados. La jerarquía SDH se desarrolló en EE. UU. bajo el nombre de SONET o ANSI T1X1 y posteriormente el CCITT (Hoy UIT-T) en 1989 publicó una serie de recomendaciones donde quedaba definida con el nombre de SDH.

SLA: Un acuerdo de nivel de servicio o *Service Level Agreement*, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

SMTP: *Simple Mail Transfer Protocol* o Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

Software colaborativo: se refiere al conjunto de programas informáticos que integran el trabajo en un sólo proyecto con muchos usuarios concurrentes que se encuentran en diversas estaciones de trabajo, conectadas a través de una red (internet o intranet).

Spam: se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

SSL/TLS: *Secure Sockets Layer* (SSL; protocolo de capa de conexión segura) y su sucesor *Transport Layer Security* (TLS; seguridad de la capa de transporte) son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente internet.

SyncML: es un protocolo de la familia de XML, usado para proveer sincronización remota para dispositivos móviles. Está integrado en muchos dispositivos móviles, como teléfonos móviles o PDAs.

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

WAN: una red de área amplia, con frecuencia denominada WAN, acrónimo de la expresión en idioma inglés *Wide Area Network*, es un tipo de red de computadoras capaz de cubrir distancias

desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).

X.500: es un conjunto de estándares de redes de ordenadores de la ITU-T sobre servicios de directorio, entendidos estos como bases de datos de direcciones electrónicas (o de otros tipos). El estándar se desarrolló conjuntamente con la ISO como parte del Modelo de interconexión de sistemas abiertos, para usarlo como soporte del correo electrónico X.400. Los protocolos definidos por X.500 incluyen, protocolo de acceso al directorio (DAP), el protocolo de sistema de directorio, el protocolo de ocultación de información de directorio, y el protocolo de gestión de enlaces operativos de directorio.

X.509: En criptografía, X.509 es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. Su sintaxis, se define empleando el lenguaje ASN.1 (Abstract Syntax Notation One), y los formatos de codificación más comunes son DER (Distinguish Encoding Rules) o PEM (Privacy Enhanced Mail).

xSDL: DSL (siglas de *Digital Subscriber Line*, "línea de suscripción digital") es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica básica o conmutada: ADSL, ADSL2, ADSL2+, SDSL, IDSL, HDSL, SHDSL, VDSL y VDSL2. Tienen en común que utilizan el par trenzado de hilos de cobre convencionales de las líneas telefónicas para la transmisión de datos a gran velocidad.

BIBLIOGRAFÍA

Todo el material y fuentes utilizadas para la elaboración de este trabajo de fin de carrera, ha sido obtenido desde publicaciones de internet, sin que ninguno de los contenidos aquí descritos o referenciados, hayan sido consultados de manera explícita en bibliografía alguna.

Referencias

Principales links relacionados con el Sub-sistema de directorio

- http://kkalev.wordpress.com/2009/01/27/openldap-performance-tips/
- http://ubuntuforums.org/showthread.php?t=1492043
- http://www.linuxtopia.org/online_books/network_administration_guides/ldap_administratio/tuning_BDB_HDB_Database_Caching.html
- http://www.openldap.org/doc/admin24/

Principales links relacionados con el Sub-sistema de correo

- http://nakedape.cc/info/Defending-Email-HOWTO/configuration.html
- http://www.akadia.com/services/postfix_uce.html
- http://www.akadia.com/services/ssh_test_certificate.html
- http://www.postfix.org/documentation.html
- http://www.postfix.org/SASL_README.html
- http://www.yellowpigs.net/computers/smtp_auth

Principales links relacionados con el Sub-sistema de aplicaciones web

- http://egroupware.org/specialpages/index.php?page_name=wiki&wikipage=ManualSetup
- http://k.noc.de/index.php?option=com_content&view=article&id=6&Itemid=8
- http://www.egroupware.org/forum#nabble-td254630
- http://www.egroupware.org/forum#nabble-td261612
- http://www.egroupware.org/forum#nabble-td268974
- http://www.egroupware.org/index.php?page_name=sync&wikipage=SyncMLInstallHowto
- http://www.egroupware.org/index.php?page_name=wiki&wikipage=ManualSetupUpdate

ANEXOS

Anexo A – Fichero de configuración courier-imap/imapd

ADDRESS=192.168.5.5

PORT=143

MAXDAEMONS=40

MAXPERIP=512

PIDFILE=/var/run/imapd.pid

TCPDOPTS="-nodnslookup -noidentlookup"

LOGGEROPTS="-name=imapd"

IMAP_CAPABILITY="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE"

IMAP_KEYWORDS=1

IMAP_ACL=1

IMAP_CAPABILITY_ORIG="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA AUTH=CRAM-MD5 AUTH=CRAM-SHA1 AUTH=CRAM-SHA256 IDLE"

IMAP_PROXY=0

IMAP_PROXY_FOREIGN=0

IMAP_IDLE_TIMEOUT=60

IMAP_MAILBOX_SANITY_CHECK=1

IMAP_CAPABILITY_TLS="$IMAP_CAPABILITY AUTH=PLAIN"

IMAP_CAPABILITY_TLS_ORIG="$IMAP_CAPABILITY_ORIG AUTH=PLAIN"

IMAP_DISABLETHREADSORT=0

IMAP_CHECK_ALL_FOLDERS=1

IMAP_OBSOLETE_CLIENT=0

IMAP_UMASK=022

IMAP_ULIMITD=65536

IMAP_USELOCKS=1

IMAP_SHAREDINDEXFILE=/etc/courier-imap/shared/index

IMAP_ENHANCEDIDLE=0

IMAP_TRASHFOLDERNAME=Trash

IMAP_EMPTYTRASH=Trash:7

IMAP_MOVE_EXPUNGE_TO_TRASH=0

SENDMAIL=/usr/sbin/sendmail

HEADERFROM=X-IMAP-Sender

IMAPDSTART=YES

MAILDIRPATH=Maildir

MAILDIR=.maildir

MAILDIRPATH=.maildir

PRERUN=

LOGINRUN=

Anexo B – Fichero de configuración courier-imap/pop3d

ADDRESS=192.168.5.5

PORT=143

MAXDAEMONS=40

MAXPERIP=512

PIDFILE=/var/run/imapd.pid

TCPDOPTS="-nodnslookup -noidentlookup"

LOGGEROPTS="-name=imapd"

IMAP_CAPABILITY="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE"

IMAP_KEYWORDS=1

IMAP_ACL=1

IMAP_CAPABILITY_ORIG="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA AUTH=CRAM-MD5 AUTH=CRAM-SHA1 AUTH=CRAM-SHA256 IDLE"

IMAP_PROXY=0

IMAP_PROXY_FOREIGN=0

IMAP_IDLE_TIMEOUT=60

IMAP_MAILBOX_SANITY_CHECK=1

IMAP_CAPABILITY_TLS="$IMAP_CAPABILITY AUTH=PLAIN"

IMAP_CAPABILITY_TLS_ORIG="$IMAP_CAPABILITY_ORIG AUTH=PLAIN"

IMAP_DISABLETHREADSORT=0

IMAP_CHECK_ALL_FOLDERS=1

IMAP_OBSOLETE_CLIENT=0

IMAP_UMASK=022

IMAP_ULIMITD=65536

IMAP_USELOCKS=1

IMAP_SHAREDINDEXFILE=/etc/courier-imap/shared/index

IMAP_ENHANCEDIDLE=0

IMAP_TRASHFOLDERNAME=Trash

IMAP_EMPTYTRASH=Trash:7

IMAP_MOVE_EXPUNGE_TO_TRASH=0

SENDMAIL=/usr/sbin/sendmail

HEADERFROM=X-IMAP-Sender

IMAPDSTART=YES

MAILDIRPATH=Maildir

MAILDIR=.maildir

MAILDIRPATH=.maildir

PRERUN=

LOGINRUN=

Anexo C – Fichero de configuración courier-imap/imapd-ssl

SSLPORT=993

SSLADDRESS=192.168.5.5

SSLPIDFILE=/var/run/imapd-ssl.pid

SSLLOGGEROPTS="-name=imapd-ssl"

IMAPDSSLSTART=NO

IMAPDSSLSTART=YES

IMAPDSTARTTLS=YES

IMAP_TLS_REQUIRED=0

COURIERTLS=/usr/sbin/couriertls

TLS_KX_LIST=ALL

TLS_COMPRESSION=ALL

TLS_CERTS=X509

TLS_CERTFILE=/etc/ssl/courier/mailbox.tfc-uoc.dyndns.org.pem

TLS_TRUSTCERTS=/etc/ssl/certs

TLS_VERIFYPEER=NONE

TLS_CACHEFILE=/var/lib/courier-imap/couriersslcache

TLS_CACHESIZE=524288

MAILDIRPATH=Maildir

MAILDIR=.maildir

MAILDIRPATH=.maildir

Anexo D – Fichero de configuración courier-imap/pop3d-ssl

SSLPORT=995

SSLADDRESS=192.168.5.5

SSLPIDFILE=/var/run/pop3d-ssl.pid

SSLLOGGEROPTS="-name=pop3d-ssl"

POP3DSSLSTART=YES

POP3_STARTTLS=YES

POP3_TLS_REQUIRED=0

COURIERTLS=/usr/sbin/couriertls

TLS_STARTTLS_PROTOCOL=TLS1

TLS_KX_LIST=ALL

TLS_COMPRESSION=ALL

TLS_CERTS=X509

TLS_CERTFILE=/etc/ssl/courier/mailbox.tfc-uoc.dyndns.org.pem

TLS_TRUSTCERTS=/etc/ssl/certs

TLS_VERIFYPEER=NONE

TLS_CACHEFILE=/var/lib/courier-imap/couriersslcache

TLS_CACHESIZE=524288

MAILDIRPATH=Maildir

MAILDIR=.maildir

MAILDIRPATH=.maildir

Anexo E – Fichero de configuración courier/authlib/authdaemonrc

authmodulelist="authldap"

authmodulelistorig="authuserdb authpam authshadow authldap authmysql authcustom authpipe"

daemons=5

```
authdaemonvar=/var/lib/courier/authdaemon

DEBUG_LOGIN=0

DEFAULTOPTIONS=""

LOGGEROPTS=""
```

Anexo F – Fichero de configuración courier/authlib/authldaprc

```
LDAP_URI                ldaps://ldapmaster.tfc-uoc.dyndns.org:636

LDAP_PROTOCOL_VERSION   3

LDAP_BASEDN             dc=tfc-uoc,dc=dyndns,dc=org

LDAP_BINDDN             cn=mailboxuser,ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org

LDAP_BINDPW             12345678Ab

LDAP_TIMEOUT            5

LDAP_AUTHBIND                   1

LDAP_MAIL               uid

LDAP_FILTER             (objectClass=CourierMailAccount)

LDAP_GLOB_UID                   vmail

LDAP_GLOB_GID                   vmail

LDAP_HOMEDIR            homeDirectory

LDAP_MAILDIR            mailbox

LDAP_DEFAULTDELIVERY    defaultDelivery

LDAP_MAILDIRQUOTA       quota

LDAP_FULLNAME                   cn

LDAP_AUXOPTIONS         disableImap=disableImap,disablePop3=disablePop3

LDAP_DEREF              never
```

Anexo G – Fichero de configuración postfix/master.cf (buzón)

```
smtp      inet  n       -       n       -       -       smtpd
```

```
smtps     inet  n       -       n       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
pickup    fifo  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
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
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       n       -       -       smtp
relay     unix  -       -       n       -       -       smtp
            -o smtp_fallback_relay=
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
retry     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
```

```
maildrop  unix -      n      n      -      -      pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${user} -w 90 ${user}@${nexthop} ${extension} ${recipient} ${user} $
{nexthop} ${sender}
10025     inet  n     -      n      -      -      smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_client_restrictions=permit_mynetworks
  -o smtpd_recipient_restrictions=permit_mynetworks,check_relay_domains,reject
  -o mynetworks=127.0.0.1,192.168.5.5,192.168.5.12
```

Anexo H – Fichero de configuración postfix/main.cf (buzón)

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/lib64/postfix
data_directory = /var/lib/postfix
mail_owner = postfix
myhostname = mailbox.tfc-uoc.dyndns.org
inet_interfaces = $myhostname
mydestination = $myhostname, localhost.$mydomain, localhost
local_recipient_maps = unix:passwd.byname $alias_maps
unknown_local_recipient_reject_code = 550
virtual_mailbox_domains = $virtual_mailbox_maps hash:/etc/postfix/vmaildomains
mynetworks = cidr:/etc/postfix/mynetworks.cidr
```

```
relayhost = smtp:mta-filter.tfc-uoc.dyndns.org

virtual_transport = maildrop

maildrop_destination_recipient_limit = 1

virtual_minimum_uid = 1001

virtual_uid_maps = static:1001

virtual_gid_maps = static:1001

alias_maps = hash:/etc/mail/aliases

virtual_alias_maps = ldap:vforward

vforward_server_host = ldaps://ldapmaster.tfc-uoc.dyndns.org:636

vforward_search_base = dc=tfc-uoc,dc=dyndns,dc=org

vforward_version = 3

vforward_bind = yes

vforward_bind_dn = cn=mtauser,ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org

vforward_query_filter = (&(mail=%s)(objectClass=inetLocalMailRecipient)(objectClass=CourierMailAccount)
(mailLocalAddress=*)(!(mailHost=inactive)))

vforward_bind_pw = 12345678Ab

vforward_result_attribute = mailLocalAddress

alias_database = hash:/etc/mail/aliases

transport_maps = hash:/etc/postfix/transport

smtpd_banner = mailbox.tfc-uoc.dyndns.org - ESMTP - Servicio de correo

local_destination_concurrency_limit = 1

debug_peer_level = 2

debugger_command =

        PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin

        ddd $daemon_directory/$process_name $process_id & sleep 5

sendmail_path = /usr/sbin/sendmail

newaliases_path = /usr/bin/newaliases
```

```
mailq_path = /usr/bin/mailq
setgid_group = postdrop
html_directory = /usr/share/doc/postfix-2.8.0-r1/html
manpage_directory = /usr/share/man
sample_directory = /etc/postfix
readme_directory = /usr/share/doc/postfix-2.8.0-r1/readme
disable_vrfy_command = yes
smtpd_helo_required = yes
smtpd_recipient_restrictions =
 permit_mynetworks,
 check_relay_domains
smtpd_client_restrictions =
 permit_mynetworks,
smtpd_use_tls = yes
smtpd_tls_key_file = /etc/ssl/postfix/server.key
smtpd_tls_cert_file = /etc/ssl/postfix/server.crt
smtpd_tls_CApath = /etc/ssl/certs
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
message_size_limit=52428800
mailbox_size_limit=52428800
virtual_mailbox_limit=52428800
maximal_queue_lifetime=2d
bounce_queue_lifetime=2d
```

Anexo I – Fichero de configuración postfix/vmaildomains (común)

tfc-uoc.dyndns.org required

Anexo J – Fichero de configuración postfix/rbl_reply (buzón)

Your addres has been marked in RBLs.

Anexo K – Fichero de configuración postfix/mynetworks.cidr (común)

127.0.0.0/8 OK

192.168.5.5/32 OK

192.168.5.7/32 OK

192.168.5.12/32 OK

Anexo L – Fichero de configuración postfix/transport (común)

no-reply@tfc-uoc.dyndns.org discard:

Anexo M – Fichero de configuración apache2/vhosts.d/tfc-uoc.dyndns.org_vhost.conf

```
<IfDefine tfc-uoc.dyndns.org_VHOST>

Listen 80

<VirtualHost 192.168.5.5:80>

        ServerName tfc-uoc.dyndns.org

        Include /etc/apache2/vhosts.d/tfc-uoc.dyndns.org_vhost.include

        ErrorLog /var/log/apache2/tfc-uoc.dyndns.org_error_log

        <IfModule log_config_module>

                TransferLog /var/log/apache2/tfc-uoc.dyndns.org_access_log

        </IfModule>

        <IfModule log_config_module>

                CustomLog /var/log/apache2/tfc-uoc.dyndns.org_request_log \

                        "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
```

```
        </IfModule>

        <IfModule mpm_peruser_module>
                ServerEnvironment apache apache
        </IfModule>
</VirtualHost>
</IfDefine>
```

Anexo N – Fichero de configuración apache2/httpd.conf

```
ServerRoot "/usr/lib64/apache2"
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule authn_alias_module modules/mod_authn_alias.so
LoadModule authn_anon_module modules/mod_authn_anon.so
LoadModule authn_dbm_module modules/mod_authn_dbm.so
LoadModule authn_default_module modules/mod_authn_default.so
LoadModule authn_file_module modules/mod_authn_file.so
<IfDefine AUTHNZ_LDAP>
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
</IfDefine>
LoadModule authz_dbm_module modules/mod_authz_dbm.so
LoadModule authz_default_module modules/mod_authz_default.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_owner_module modules/mod_authz_owner.so
LoadModule authz_user_module modules/mod_authz_user.so
```

```
LoadModule autoindex_module modules/mod_autoindex.so
<IfDefine CACHE>
LoadModule cache_module modules/mod_cache.so
</IfDefine>
LoadModule cgi_module modules/mod_cgi.so
LoadModule cgid_module modules/mod_cgid.so
<IfDefine DAV>
LoadModule dav_module modules/mod_dav.so
</IfDefine>
<IfDefine DAV>
LoadModule dav_fs_module modules/mod_dav_fs.so
</IfDefine>
<IfDefine DAV>
LoadModule dav_lock_module modules/mod_dav_lock.so
</IfDefine>
LoadModule deflate_module modules/mod_deflate.so
LoadModule dir_module modules/mod_dir.so
<IfDefine CACHE>
LoadModule disk_cache_module modules/mod_disk_cache.so
</IfDefine>
LoadModule env_module modules/mod_env.so
LoadModule expires_module modules/mod_expires.so
LoadModule ext_filter_module modules/mod_ext_filter.so
<IfDefine CACHE>
LoadModule file_cache_module modules/mod_file_cache.so
</IfDefine>
LoadModule filter_module modules/mod_filter.so
```

```
LoadModule headers_module modules/mod_headers.so
LoadModule include_module modules/mod_include.so
<IfDefine INFO>
LoadModule info_module modules/mod_info.so
</IfDefine>
<IfDefine LDAP>
LoadModule ldap_module modules/mod_ldap.so
</IfDefine>
LoadModule log_config_module modules/mod_log_config.so
LoadModule logio_module modules/mod_logio.so
<IfDefine CACHE>
LoadModule mem_cache_module modules/mod_mem_cache.so
</IfDefine>
LoadModule mime_module modules/mod_mime.so
LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule speling_module modules/mod_speling.so
<IfDefine SSL>
LoadModule ssl_module modules/mod_ssl.so
</IfDefine>
<IfDefine STATUS>
LoadModule status_module modules/mod_status.so
</IfDefine>
LoadModule unique_id_module modules/mod_unique_id.so
<IfDefine USERDIR>
```

```
LoadModule userdir_module modules/mod_userdir.so
</IfDefine>
LoadModule usertrack_module modules/mod_usertrack.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
User apache
Group apache
Include /etc/apache2/modules.d/*.conf
Include /etc/apache2/vhosts.d/*.conf
```

Anexo O – Fichero de configuración apache2/vhosts.d/tfc-uoc.dyndns.org_vhost.include

```
<Directory "/var/www/tfc-uoc.dyndns.org/htdocs">
        Options FollowSymLinks
        AllowOverride All
        Order allow,deny
        Allow from all
</Directory>
<IfModule alias_module>
        ScriptAlias /cgi-bin/ "/var/www/tfc-uoc.dyndns.org/cgi-bin/"
</IfModule>
<Directory "/var/www/tfc-uoc.dyndns.org/cgi-bin">
        AllowOverride None
        Options None
        Order allow,deny
        Allow from all
</Directory>
<Location "/i-desktop/rpc.php">
```

```
        php_value mbstring.func_overload 0
        php_admin_value mbstring.func_overload 0
        Order allow,deny
        Allow from all
</Location>
```

Anexo P – Fichero de configuración php/apache2-php5.2/php.ini

```
[PHP]
engine = On
zend.ze1_compatibility_mode = Off
short_open_tag = On
asp_tags = Off
precision    =  12
y2k_compliance = On
output_buffering = Off
zlib.output_compression = Off
implicit_flush = Off
unserialize_callback_func=
serialize_precision = 100
allow_call_time_pass_reference = On
safe_mode = Off
safe_mode_gid = Off
safe_mode_include_dir =
safe_mode_exec_dir =
safe_mode_allowed_env_vars = PHP_
safe_mode_protected_env_vars = LD_LIBRARY_PATH
disable_functions =
```

```
disable_classes =
expose_php = Off
max_execution_time = 30     ; Maximum execution time of each script, in seconds
max_input_time = 60         ; Maximum amount of time each script may spend parsing request data
memory_limit = 128M      ; Maximum amount of memory a script may consume (128MB)
error_reporting = E_ALL & ~E_NOTICE
display_errors = "stderr"
display_startup_errors = On
log_errors = On
log_errors_max_len = 1024
ignore_repeated_errors = Off
ignore_repeated_source = Off
report_memleaks = On
track_errors = Off
error_log = "/var/log/apache2/php.log"
variables_order = "EGPCS"
register_globals = Off
register_long_arrays = On
register_argc_argv = On
auto_globals_jit = On
post_max_size = 8M
magic_quotes_gpc = On
magic_quotes_runtime = Off
magic_quotes_sybase = Off
auto_prepend_file =
auto_append_file =
default_mimetype = "text/html"
```

```
include_path = ".:/usr/share/php5:/usr/share/php"

doc_root =

user_dir =

extension_dir = /usr/lib64/php5.2/lib/extensions/no-debug-zts-20060613

enable_dl = On

file_uploads = On

upload_max_filesize = 2M

max_file_uploads = 20

allow_url_fopen = Off

allow_url_include = Off

default_socket_timeout = 60

[Date]

[filter]

[iconv]

[sqlite]

[Pcre]

[Syslog]

define_syslog_variables  = Off

[mail function]

SMTP = localhost

smtp_port = 25

[SQL]

sql.safe_mode = Off

[ODBC]

odbc.allow_persistent = On

odbc.check_persistent = On

odbc.max_persistent = -1
```

odbc.max_links = -1

odbc.defaultlrl = 4096

odbc.defaultbinmode = 1

[MySQL]

mysql.allow_persistent = On

mysql.max_persistent = -1

mysql.max_links = -1

mysql.default_port =

mysql.default_socket =

mysql.default_host =

mysql.default_user =

mysql.default_password =

mysql.connect_timeout = 60

mysql.trace_mode = Off

[MySQLi]

mysqli.max_links = -1

mysqli.default_port = 3306

mysqli.default_socket =

mysqli.default_host =

mysqli.default_user =

mysqli.default_pw =

mysqli.reconnect = Off

[mSQL]

msql.allow_persistent = On

msql.max_persistent = -1

msql.max_links = -1

[OCI8]

```
[PostgresSQL]
pgsql.allow_persistent = On
pgsql.auto_reset_persistent = Off
pgsql.max_persistent = -1
pgsql.max_links = -1
pgsql.ignore_notice = 0
pgsql.log_notice = 0
[Sybase]
sybase.allow_persistent = On
sybase.max_persistent = -1
sybase.max_links = -1
sybase.min_error_severity = 10
sybase.min_message_severity = 10
sybase.compatability_mode = Off
[Sybase-CT]
sybct.allow_persistent = On
sybct.max_persistent = -1
sybct.max_links = -1
sybct.min_server_severity = 10
sybct.min_client_severity = 10
[bcmath]
bcmath.scale = 0
[browscap]
[Informix]
ifx.default_host =
ifx.default_user =
ifx.default_password =
```

```
ifx.allow_persistent = On
ifx.max_persistent = -1
ifx.max_links = -1
ifx.textasvarchar = 0
ifx.byteasvarchar = 0
ifx.charasvarchar = 0
ifx.blobinfile = 0
ifx.nullformat = 0
[Session]
session.save_handler = files
session.save_path = "/tmp"
session.use_cookies = 1
session.name = PHPSESSID
session.auto_start = 0
session.cookie_lifetime = 0
session.cookie_path = /
session.cookie_domain =
session.cookie_httponly =
session.serialize_handler = php
session.gc_probability = 1
session.gc_divisor     = 100
session.gc_maxlifetime = 1440
session.bug_compat_42 = 1
session.bug_compat_warn = 1
session.referer_check =
session.entropy_length = 0
session.entropy_file =
```

session.cache_limiter = nocache

session.cache_expire = 180

session.use_trans_sid = 0

session.hash_function = 0

session.hash_bits_per_character = 4

url_rewriter.tags = "a=href,area=href,frame=src,input=src,form=,fieldset="

[MSSQL]

mssql.allow_persistent = On

mssql.max_persistent = -1

mssql.max_links = -1

mssql.min_error_severity = 10

mssql.min_message_severity = 10

mssql.compatability_mode = Off

mssql.secure_connection = Off

[Assertion]

[COM]

[mbstring]

mbstring.func_overload = 7

[FrontBase]

[gd]

[exif]

[Tidy]

tidy.clean_output = Off

[soap]

soap.wsdl_cache_enabled=1

soap.wsdl_cache_dir="/tmp"

soap.wsdl_cache_ttl=86400

Anexo Q – Fichero de configuración mysql/my.cnf

```
[client]
port                                    = 3306
socket                                  = /var/run/mysqld/mysqld.sock
[mysql]
character-sets-dir=/usr/share/mysql/charsets
default-character-set=latin1
[mysqladmin]
character-sets-dir=/usr/share/mysql/charsets
default-character-set=latin1
[mysqlcheck]
character-sets-dir=/usr/share/mysql/charsets
default-character-set=latin1
[mysqldump]
character-sets-dir=/usr/share/mysql/charsets
default-character-set=latin1
[mysqlimport]
character-sets-dir=/usr/share/mysql/charsets
default-character-set=latin1
[mysqlshow]
character-sets-dir=/usr/share/mysql/charsets
default-character-set=latin1
[myisamchk]
character-sets-dir=/usr/share/mysql/charsets
[myisampack]
character-sets-dir=/usr/share/mysql/charsets
[mysqld_safe]
```

```
err-log                                 = /var/log/mysql/mysql.err
[mysqld]
character-set-server            = latin1
user                                    = mysql
port                                    = 3306
socket                                  = /var/run/mysqld/mysqld.sock
pid-file                                = /var/run/mysqld/mysqld.pid
log-error                               = /var/log/mysql/mysqld.err
basedir                                 = /usr
datadir                                 = /var/lib/mysql
skip-external-locking
key_buffer                              = 16M
max_allowed_packet                      = 1M
table_cache                             = 64
sort_buffer_size                = 512K
net_buffer_length                       = 8K
read_buffer_size                = 256K
read_rnd_buffer_size            = 512K
myisam_sort_buffer_size   = 8M
language                                = /usr/share/mysql/english
bind-address                            = 127.0.0.1
log-bin
server-id                               = 1
tmpdir                                  = /tmp/
innodb_buffer_pool_size = 16M
innodb_additional_mem_pool_size = 2M
innodb_data_file_path = ibdata1:10M:autoextend:max:128M
```

```
innodb_log_file_size = 5M
innodb_log_buffer_size = 8M
innodb_log_files_in_group=2
innodb_flush_log_at_trx_commit = 1
innodb_lock_wait_timeout = 50
innodb_file_per_table
[mysqldump]
quick
max_allowed_packet              = 16M
[mysql]
[isamchk]
key_buffer                      = 20M
sort_buffer_size        = 20M
read_buffer                     = 2M
write_buffer                    = 2M
[myisamchk]
key_buffer                      = 20M
sort_buffer_size        = 20M
read_buffer                     = 2M
write_buffer                    = 2M
[mysqlhotcopy]
interactive-timeout
```

Anexo R – Fichero de configuración postfix/master.cf (MTA front-end)

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

```
 -o smtpd_sasl_auth_enable=yes
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       n       -       -       smtp
relay     unix  -       -       n       -       -       smtp
            -o smtp_fallback_relay=
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
retry     unix  -       -       n       -       -       error
discard   unix  -       -       n       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       -       -       -       lmtp
anvil     unix  -       -       -       -       1       anvil
scache    unix  -       -       -       -       1       scache
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
```

```
uucp      unix -      n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
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=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
scalemail-backend unix    -       n       n       -       2       pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user} ${extension}
mailman   unix -      n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
10025     inet  n     -       n       -       -       smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_client_restrictions=permit_mynetworks
  -o smtpd_recipient_restrictions=permit_mynetworks,check_relay_domains,reject
  -o mynetworks=127.0.0.1,192.168.5.5,192.168.5.12
```

Anexo S – Fichero de configuración postfix/main.cf (MTA front-end)

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/lib/postfix
```

```
data_directory = /var/lib/postfix

mail_owner = postfix

myhostname = lanzarote.tfc-uoc.dyndns.org

inet_interfaces = $myhostname

mydestination = $myhostname, localhost.$mydomain, localhost

local_recipient_maps = unix:passwd.byname $alias_maps

unknown_local_recipient_reject_code = 550

virtual_mailbox_domains = $virtual_mailbox_maps hash:/etc/postfix/vmaildomains

mynetworks = cidr:/etc/postfix/mynetworks.cidr

virtual_mailbox_maps= ldap:vuser

vuser_server_host = ldaps://lanzarote.tfc-uoc.dyndns.org:636

vuser_search_base = dc=tfc-uoc,dc=dyndns,dc=org

vuser_version = 3

vuser_bind = yes

vuser_bind_dn = cn=mtauser,ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org

vuser_bind_pw = 12345678Ab

vuser_query_filter = (&(mail=%u@%d)(!(mailHost=inactive))(objectClass=inetLocalMailRecipient))

vuser_result_attribute = uid

alias_maps = hash:/etc/aliases

virtual_alias_maps = ldap:valias

valias_server_host = ldaps://lanzarote.tfc-uoc.dyndns.org:636

valias_search_base = dc=tfc-uoc,dc=dyndns,dc=org

valias_version = 3

valias_bind = yes

valias_bind_dn = cn=mtauser,ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org

valias_query_filter = (&(mailRoutingAddress=%u@%d)(objectClass=inetLocalMailRecipient))

valias_bind_pw = 12345678Ab
```

```
valias_result_attribute = mailLocalAddress

alias_database = hash:/etc/aliases

transport_maps = ldap:vtransportmap hash:/etc/postfix/transport

vtransportmap_server_host = ldaps://lanzarote.tfc-uoc.dyndns.org:636

vtransportmap_search_base = dc=tfc-uoc,dc=dyndns,dc=org

vtransportmap_version = 3

vtransportmap_bind = yes

vtransportmap_bind_dn = cn=mtauser,ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org

vtransportmap_bind_pw = 12345678Ab

vtransportmap_query_filter = (&(mail=%s)(objectClass=inetLocalMailRecipient)(mailHost=*))

vtransportmap_result_attribute = mailHost

vtransportmap_result_format = smtp:[%s]

smtpd_banner = lanzarote.tfc-uoc.dyndns.org - ESMTP - Servicio de correo

debug_peer_level = 2

debugger_command =

        PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin

        ddd $daemon_directory/$process_name $process_id & sleep 5

sendmail_path = /usr/sbin/sendmail

newaliases_path = /usr/bin/newaliases

mailq_path = /usr/bin/mailq

setgid_group = postdrop

html_directory = /usr/share/doc/postfix/html

manpage_directory = /usr/share/man

sample_directory = /etc/postfix

readme_directory = /usr/share/doc/postfix

smtpd_sasl_auth_enable = yes

smtpd_sasl_security_options = noanonymous
```

```
broken_sasl_auth_clients = yes

disable_vrfy_command = yes

smtpd_helo_required = yes

smtpd_sender_login_maps = ldap:sendercheck

sendercheck_server_host = ldaps://lanzarote.tfc-uoc.dyndns.org:636

sendercheck_search_base = dc=tfc-uoc,dc=dyndns,dc=org

sendercheck_version = 3

sendercheck_bind = yes

sendercheck_bind_dn = cn=mtauser,ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org

sendercheck_bind_pw = 12345678Ab

sendercheck_query_filter = (&(mail=%s)(!(mailHost=inactive))(objectClass=inetLocalMailRecipient)
(objectClass=CourierMailAccount))

sendercheck_result_attribute = uid

sendercheck_result_format = %u@%D,%u

smtpd_recipient_restrictions =

 permit_mynetworks,

 reject_sender_login_mismatch,

 permit_sasl_authenticated,

 reject_unauth_destination

smtpd_use_tls = yes

smtpd_tls_key_file = /etc/ssl/postfix/lanzarote.tfc-uoc.dyndns.org.key

smtpd_tls_cert_file = /etc/ssl/postfix/lanzarote.tfc-uoc.dyndns.org.crt

smtpd_tls_CApath = /etc/ssl/certs

smtpd_tls_received_header = yes

smtpd_tls_session_cache_timeout = 3600s

tls_random_source = dev:/dev/urandom

smtpd_client_restrictions =
```

permit_mynetworks,

permit_sasl_authenticated,

reject_rhsbl_client blackhole.securitysage.com,

reject_rhsbl_sender blackhole.securitysage.com,

reject_rbl_client relays.ordb.org,

reject_rbl_client blackholes.easynet.nl,

reject_rbl_client cbl.abuseat.org,

reject_rbl_client proxies.blackholes.wirehub.net,

reject_rbl_client bl.spamcop.net,

reject_rbl_client sbl.spamhaus.org,

reject_rbl_client opm.blitzed.org,

reject_rbl_client dnsbl.njabl.org

maps_rbl_reject_code = 554

rbl_reply_maps = hash:/$config_directory/rbl_reply

default_process_limit=200

content_filter = smtp:mta-filter.tfc-uoc.dyndns.org

message_size_limit=52428800

maximal_queue_lifetime=2d

bounce_queue_lifetime=2d

Anexo T – Fichero de configuración etc/saslauthd.conf (MTA front-end)

ldap_servers: ldaps://lanzarote.tfc-uoc.dyndns.org:636

ldap_search_base: dc=tfc-uoc,dc=dyndns,dc=org

ldap_filter: (&(uid=%U)(mail=*))

ldap_auth_method: bind

ldap_bind_dn: cn=mtauser,ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org

ldap_bind_pw: 12345678Ab

Anexo U – Fichero de configuración postfix/sasl/smtpd.conf (MTA front-end)

```
pwcheck_method: saslauthd

mech_list: plain login
```

Anexo V – Fichero de configuración postfix/master.cf (MTA filter)

```
smtp      inet  n       -       n       -       -       smtpd
pickup    fifo  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
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
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       n       -       -       smtp
relay     unix  -       -       n       -       -       smtp
            -o smtp_fallback_relay=
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
retry     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
smtp-amavis unix -    -       n       -       20      smtp
  -o smtp_data_done_timeout=1200
  -o disable_dns_lookups=yes
  -o smtp_connect_timeout=1s
  -o smtp_helo_timeout=1s
10026     inet  n     -       n       -       -       smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_client_restrictions=
```

Anexo W – Fichero de configuración postfix/main.cf (MTA filter)

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
data_directory = /var/lib/postfix
mail_owner = postfix
myhostname = mta-filter.tfc-uoc.dyndns.org
inet_interfaces = all
inet_protocols = all
mydestination = $myhostname, localhost.$mydomain, localhost
local_recipient_maps = unix:passwd.byname $alias_maps
```

```
unknown_local_recipient_reject_code = 550

virtual_mailbox_domains = $virtual_mailbox_maps hash:/etc/postfix/vmaildomains

mynetworks = cidr:/etc/postfix/mynetworks.cidr

relayhost = lanzarote.tfc-uoc.dyndns.org:10025

alias_maps = hash:/etc/aliases

alias_database = hash:/etc/aliases

transport_maps = hash:/etc/postfix/transport

smtpd_banner = mta-filter.tfc-uoc.dyndns.org - ESMTP - Servicio de correo

debug_peer_level = 2

debugger_command =

        PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin

        ddd $daemon_directory/$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 = no

manpage_directory = /usr/share/man

sample_directory = /usr/share/doc/postfix-2.7.3/samples

readme_directory = /usr/share/doc/postfix-2.7.3/README_FILES

disable_vrfy_command = yes

smtpd_helo_required = yes

smtpd_recipient_restrictions =

 permit_mynetworks,

 reject

default_process_limit=200

content_filter = smtp-amavis:localhost:10025
```

```
message_size_limit=52428800

maximal_queue_lifetime=2d

bounce_queue_lifetime=2d

minimal_backoff_time= 2000s

maximal_backoff_time= 6000s
```

Anexo X – Fichero de configuración amavisd/amavisd.conf

```
use strict;

@mynetworks = qw( 127.0.0.1/8 [::1] [FE80::]/10 [FEC0::]/10 10.0.0.0/8 192.168.5.12 );

};

$policy_bank{'AM.PDP-SOCK'} = {

  protocol => 'AM.PDP',

};

@addr_extension_virus_maps      = ('virus');

@addr_extension_banned_maps     = ('banned');

@addr_extension_spam_maps       = ('spam');

@addr_extension_bad_header_maps = ('badh');

$path = '/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';

$MAXLEVELS = 14;

$MAXFILES = 1500;

$sa_spam_subject_tag = '[Possible SPAM content] - ';

$myhostname = 'mta-filter.tfc-uoc.dyndns.org';

$notify_method  = $forward_method;

$final_virus_destiny      = D_DISCARD;

$final_banned_destiny     = D_BOUNCE;

$final_spam_destiny       = D_DISCARD;

$final_bad_header_destiny = D_BOUNCE;
```

```
@keep_decoded_original_maps = (new_RE(
  qr'^(ASCII(?! cpio)|text|uuencoded|xxencoded|binhex)'i,
));
$banned_filename_re = new_RE(
  qr'^application/x-msdos-program$'i,
  qr'^application/hta$'i,
  qr'\.[^./]*[A-Za-z][^./]*\.\s*(exe|vbs|pif|scr|bat|cmd|com|cpl|dll)[.\s]*$'i,
);
    [qr'^(bulkmail|offers|cheapbenefits|earnmoney|foryou)@'i        => 5.0],
    [qr'^(greatcasino|investments|lose_weight_today|market\.alert)@'i=> 5.0],
    [qr'^(money2you|MyGreenCard|new\.tld\.registry|opt-out|opt-in)@'i=> 5.0],
    [qr'^(optin|saveonlsmoking2002k|specialoffer|specialoffers)@'i   => 5.0],
    [qr'^(stockalert|stopsnoring|wantsome|workathome|yesitsfree)@'i  => 5.0],
    [qr'^(your_friend|greatoffers)@'i                 => 5.0],
    [qr'^(inkjetplanet|marketopt|MakeMoney)\d*@'i                => 5.0],
   ),
    'nobody@cert.org'                     => -3.0,
    'cert-advisory@us-cert.gov'             => -3.0,
    'owner-alert@iss.net'                 => -3.0,
    'slashdot@slashdot.org'                 => -3.0,
    'securityfocus.com'                   => -3.0,
    'ntbugtraq@listserv.ntbugtraq.com'      => -3.0,
    'security-alerts@linuxsecurity.com'     => -3.0,
    'mailman-announce-admin@python.org'     => -3.0,
    'amavis-user-admin@lists.sourceforge.net'=> -3.0,
    'amavis-user-bounces@lists.sourceforge.net' => -3.0,
    'spamassassin.apache.org'               => -3.0,
```

```
    'notification-return@lists.sophos.com'   => -3.0,
    'owner-postfix-users@postfix.org'        => -3.0,
    'owner-postfix-announce@postfix.org'     => -3.0,
    'owner-sendmail-announce@lists.sendmail.org'   => -3.0,
    'sendmail-announce-request@lists.sendmail.org' => -3.0,
    'donotreply@sendmail.org'                => -3.0,
    'ca+envelope@sendmail.org'               => -3.0,
    'noreply@freshmeat.net'                  => -3.0,
    'owner-technews@postel.acm.org'          => -3.0,
    'ietf-123-owner@loki.ietf.org'           => -3.0,
    'cvs-commits-list-admin@gnome.org'       => -3.0,
    'rt-users-admin@lists.fsck.com'          => -3.0,
    'clp-request@comp.nus.edu.sg'            => -3.0,
    'surveys-errors@lists.nua.ie'            => -3.0,
    'emailnews@genomeweb.com'                => -5.0,
    'yahoo-dev-null@yahoo-inc.com'           => -3.0,
    'returns.groups.yahoo.com'               => -3.0,
    'clusternews@linuxnetworx.com'           => -3.0,
    lc('lvs-users-admin@LinuxVirtualServer.org')    => -3.0,
    lc('owner-textbreakingnews@CNNIMAIL12.CNN.COM') => -5.0,
    'sender@example.net'                     =>  3.0,
    '.example.net'                           =>  1.0,
  },
});
@decoders = (
  ['mail', \&do_mime_decode],
  ['asc',  \&do_ascii],
```

```
 ['uue',  \&do_ascii],
 ['hqx',  \&do_ascii],
 ['ync',  \&do_ascii],
 ['F',    \&do_uncompress, ['unfreeze','freeze -d','melt','fcat'] ],
 ['Z',    \&do_uncompress, ['uncompress','gzip -d','zcat'] ],
 ['gz',   \&do_uncompress,  'gzip -d'],
 ['gz',   \&do_gunzip],
 ['bz2',  \&do_uncompress,  'bzip2 -d'],
 ['lzo',  \&do_uncompress,  'lzop -d'],
 ['rpm',  \&do_uncompress, ['rpm2cpio.pl','rpm2cpio'] ],
 ['cpio', \&do_pax_cpio,   ['pax','gcpio','cpio'] ],
 ['tar',  \&do_pax_cpio,   ['pax','gcpio','cpio'] ],
 ['deb',  \&do_ar,          'ar'],
 ['zip',  \&do_unzip],
 ['7z',   \&do_7zip,       ['7zr','7za','7z'] ],
 ['rar',  \&do_unrar,      ['rar','unrar'] ],
 ['arj',  \&do_unarj,      ['arj','unarj'] ],
 ['arc',  \&do_arc,        ['nomarch','arc'] ],
 ['zoo',  \&do_zoo,         ['zoo','unzoo'] ],
 ['lha',  \&do_lha,         'lha'],
 ['cab',  \&do_cabextract,  'cabextract'],
 ['tnef', \&do_tnef_ext,    'tnef'],
 ['tnef', \&do_tnef],
 ['exe',  \&do_executable, ['rar','unrar'], 'lha', ['arj','unarj'] ],
);
@av_scanners = (
['ClamAV-clamd',
```

```
 \&ask_daemon, ["CONTSCAN {}\n", '127.0.0.1:3310'],
 qr/\bOK$/m, qr/\bFOUND$/m,
 qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
 ['KasperskyLab AVP - aveclient',
   ['/usr/local/kav/bin/aveclient','/usr/local/share/kav/bin/aveclient',
    '/opt/kav/5.5/kav4mailservers/bin/aveclient','aveclient'],
   '-p /var/run/aveserver -s {}/*',
   [0,3,6,8], qr/\b(INFECTED|SUSPICION|SUSPICIOUS)\b/m,
   qr/(?:INFECTED|WARNING|SUSPICION|SUSPICIOUS) (.+)/m,
 ],
 ['KasperskyLab AntiViral Toolkit Pro (AVP)', ['avp'],
   qr/infected: (.+)/m,
   sub {chdir('/opt/AVP') or die "Can't chdir to AVP: $!"},
   sub {chdir($TEMPBASE) or die "Can't chdir back to $TEMPBASE $!"},
 ],
 ['KasperskyLab AVPDaemonClient',
   [ '/opt/AVP/kavdaemon',       'kavdaemon',
     '/opt/AVP/AvpDaemonClient', 'AvpDaemonClient',
     '/opt/AVP/AvpTeamDream',    'AvpTeamDream',
     '/opt/AVP/avpdc', 'avpdc' ],
   "-f=$TEMPBASE {}", [0,8], [3,4,5,6], qr/infected: ([^\r\n]+)/m ],
 ['CentralCommand Vexira (new) vascan',
   ['vascan','/usr/lib/Vexira/vascan'],
   "-a s --timeout=60 --temp=$TEMPBASE -y $QUARANTINEDIR ".
   "--log=/var/log/vascan.log {}",
   [0,3], [1,2,5],
   qr/(?x)^\s* (?:virus|iworm|macro|mutant|sequence|trojan)\ found:\ ( [^\]\s']+ )\ \.\.\.\ /m ],
```

```
['Avira AntiVir', ['antivir','vexira'],
  '--allfiles -noboot -nombr -rs -s -z {}', [0], qr/ALERT:|VIRUS:/m,
  qr/(?x)^\s* (?: ALERT: \s* (?: \[ | [^']* ' ) |
      (?i) VIRUS:\ .*?\ virus\ '?) ( [^\]\s']+ )/m ],
['Command AntiVirus for Linux', 'csav',
  '-all -archive -packed {}', [50], [51,52,53],
  qr/Infection: (.+)/m ],
['Symantec CarrierScan via Symantec CommandLineScanner',
  'cscmdline', '-a scan -i 1 -v -s 127.0.0.1:7777 {}',
  qr/^Files Infected:\s+0$/m, qr/^Infected\b/m,
  qr/^(?:Info|Virus Name):\s+(.+)/m ],
['Symantec AntiVirus Scan Engine',
  'savsecls', '-server 127.0.0.1:7777 -mode scanrepair -details -verbose {}',
  [0], qr/^Infected\b/m,
  qr/^(?:Info|Virus Name):\s+(.+)/m ],
 ['F-Secure Antivirus for Linux servers',
  ['/opt/f-secure/fsav/bin/fsav', 'fsav'],
  '--virus-action1=report --archive=yes --auto=yes '.
  '--dumb=yes --list=no --mime=yes {}', [0], [3,4,6,8],
  qr/(?:infection|Infected|Suspected|Riskware): (.+)/m ],
  '-sec -nex {}', [0], [100],
  qr/was infected by virus (.+)/m ],
['CAI eTrust Antivirus', 'etrust-wrapper',
  '-arc -nex -spm h {}', [0], [101],
  qr/is infected by virus: (.+)/m ],
['MkS_Vir for Linux (beta)', ['mks32','mks'],
  '-s {}/*', [0], [1,2],
```

```
  qr/--[ \t]*(.+)/m ],
['MkS_Vir daemon', 'mksscan',
  '-s -q {}', [0], [1..7],
  qr/^... (\S+)/m ],
['ESET Software ESETS Command Line Interface',
  ['/usr/bin/esets_cli', 'esets_cli'],
  '--subdir {}', [0], [1,2,3],
  qr/:\s*action="(?!accepted)[^"]*"\n.*:\s*virus="([^"]*)"/m ],
['ESET NOD32 for Linux File servers',
  ['/opt/eset/nod32/sbin/nod32','nod32'],
  '--files -z --mail --sfx --rtp --adware --unsafe --pattern --heur '.
  '-w -a --action=1 -b {}',
  [0], [1,10], qr/^object=.*, virus="(.*?)",/m ],
['Norman Virus Control v5 / Linux', 'nvcc',
  '-c -l:0 -s -u -temp:$TEMPBASE {}', [0,10,11], [1,2,14],
  qr/(?i).* virus in .* -> \'(.+)\'/m ],
['Panda CommandLineSecure 9 for Linux',
  ['/opt/pavcl/usr/bin/pavcl','pavcl'],
  '-auto -aex -heu -cmp -nbr -nor -nos -eng -nob {}',
  qr/Number of files infected[ .]*: 0+(?!\d)/m,
  qr/Number of files infected[ .]*: 0*[1-9]/m,
  qr/Found virus :\s*(\S+)/m ],
['NAI McAfee AntiVirus (uvscan)', 'uvscan',
  '--secure -rv --mime --summary --noboot - {}', [0], [13],
  qr/(?x) Found (?:
      \ the\ (.+)\ (?:virus|trojan)  |
      \ (?:virus|trojan)\ or\ variant\ ([^ ]+)  |
```

```
      :\ (.+)\ NOT\ a\ virus)/m,
 ],
 ['VirusBuster', ['vbuster', 'vbengcl'],
   "{} -ss -i '*' -log=$MYHOME/vbuster.log", [0], [1],
   qr/: '(.*)' - Virus/m ],
 ['CyberSoft VFind', 'vfind',
   '--vexit {}/*', [0], [23], qr/##==>>>> VIRUS ID: CVDL (.+)/m,
 ],
 ['avast! Antivirus', ['/usr/bin/avastcmd','avastcmd'],
   '-a -i -n -t=A {}', [0], [1], qr/\binfected by:\s+([^ \t\n\[\]]+)/m ],
 ['Ikarus AntiVirus for Linux', 'ikarus',
   '{}', [0], [40], qr/Signature (.+) found/m ],
   '--action=ignore --no-list {}', qr/^Infected files\s*:\s*0+(?!\d)/m,
   qr/^(?:Infected files|Identified viruses|Suspect files)\s*:\s*0*[1-9]/m,
   qr/(?:suspected|infected)\s*:\s*(.*)(?:\033|$)/m ],
   '--arc --mail {}', qr/^Infected files *:0+(?!\d)/m,
   qr/^(?:Infected files|Identified viruses|Suspect files) *:0*[1-9]/m,
   qr/(?:suspected|infected): (.*)(?:\033|$)/m ],
 ['ArcaVir for Linux', ['arcacmd','arcacmd.static'],
   '-v 1 -summary 0 -s {}', [0], [1,2],
   qr/(?:VIR|WIR):[ \t]*(.+)/m ],
);
@av_scanners_backup = (
 ['F-PROT Antivirus for UNIX', ['fpscan'],
   [0,8,64],  [1,2,3, 4+1,4+2,4+3, 8+1,8+2,8+3, 12+1,12+2,12+3],
   qr/^\[Found\s+[^\]]*\]\s+<([^ \t(>]*)/m ],
 ['FRISK F-Prot Antivirus', ['f-prot','f-prot.sh'],
```

```
    qr/(?:Infection:|security risk named) (.+)|\s+contains\s+(.+)$/m ],
  ['Trend Micro FileScanner', ['/etc/iscan/vscan','vscan'],
    '-za -a {}', [0], qr/Found virus/m, qr/Found virus (.+) in/m ],
    ['/usr/local/drweb/drweb', '/opt/drweb/drweb', 'drweb'],
    '-path={} -al -go -ot -cn -upn -ok-',
    [0,32], [1,9,33], qr' infected (?:with|by)(?: virus)? (.*)$'m ],
   ['Kaspersky Antivirus v5.5',
     ['/opt/kaspersky/kav4fs/bin/kav4fs-kavscanner',
      '/opt/kav/5.5/kav4unix/bin/kavscanner',
      '/opt/kav/5.5/kav4mailservers/bin/kavscanner', 'kavscanner'],
     '-i0 -xn -xp -mn -R -ePASBME {}/*', [0,10,15], [5,20,21,25],
     qr/(?:INFECTED|WARNING|SUSPICION|SUSPICIOUS) (.*)/m,
   ],
);
```

Anexo Y – Fichero de configuración etc/freshclam.conf

```
UpdateLogFile /var/log/freshclam.log
LogSyslog yes
LogFacility LOG_MAIL
PidFile /var/run/freshclam.pid
AllowSupplementaryGroups yes
DatabaseMirror database.clamav.net
DatabaseMirror database.clamav.net
ScriptedUpdates yes
NotifyClamd /etc/clamd.d/scan.conf
```

Anexo Z – Fichero de configuración clamd.d/scan.conf

LogFile /var/log/clamd.scan

LogFileMaxSize 0

LogTime yes

LogSyslog yes

LogFacility LOG_MAIL

PidFile /var/run/clamd.scan/clamd.pid

LocalSocket /var/run/clamd.scan/clamd.sock

FixStaleSocket yes

TCPSocket 3310

TCPAddr 127.0.0.1

User root

Anexo AA – Fichero de configuración clamd.d/amavisd.conf

LogSyslog yes

LogFacility LOG_MAIL

PidFile /var/run/amavisd/clamd.pid

FixStaleSocket yes

User amavis

LocalSocket /var/spool/amavisd/clamd.sock

Anexo AB – Fichero de configuración openldap/ldap.conf (común)

TLS_REQCERT never

Anexo AC – Fichero de configuración openldap/slapd.conf (maestro)

include /etc/openldap/schema/core.schema

include /etc/openldap/schema/misc.schema

include /etc/openldap/schema/amavisd-new.schema

```
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/corba.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/samba.schema
include         /etc/openldap/schema/authldap.schema
include         /etc/openldap/schema/java.schema
pidfile         /var/run/openldap/slapd.pid
argsfile  /var/run/openldap/slapd.args
modulepath      /usr/lib64/openldap/openldap
moduleload      syncprov.la
moduleload      unique.la
moduleload      back_monitor.so
TLSCertificateFile      /etc/ssl/slapd/ldapmaster.tfc-uoc.dyndns.org.crt
TLSCertificateKeyFile   /etc/ssl/slapd/ldapmaster.tfc-uoc.dyndns.org.key
TLSCACertificatePath    /etc/ssl/certs/
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
access to *
        by anonymous auth
loglevel  sync stats
database        hdb
suffix          "dc=tfc-uoc,dc=dyndns,dc=org"
checkpoint      1024    5
cachesize       65536
idlcachesize    65536
```

```
rootdn          "cn=Directory Manager,dc=tfc-uoc,dc=dyndns,dc=org"
rootpw          {SSHA}VJ1dAYUVJASJHhviv255zRA4c7UL7AHa
directory /var/lib/openldap-data/tfc-uoc
index   objectClass,entryUUID,entryCSN,employeeNumber,mailHost,memberUid,mailRoutingAddress   eq
index   dc,o,ou,cn,mail,sn,givenName,uid    eq,pres,sub
index   uidNumber,gidNumber,loginShell,disableImap,disablePop3   eq,pres
sizelimit 1000
timelimit 60
limits
        dn.exact="cn=replicator,dc=tfc-uoc,dc=dyndns,dc=org"
        time.soft=unlimited
        time.hard=unlimited
        size.soft=unlimited
        size.hard=unlimited
include /etc/openldap/slapd.access.conf
overlay unique
unique_uri ldap:///?mail?sub?
unique_uri ldaps:///?mail?sub?
unique_uri ldap:///?uid?sub?
unique_uri ldaps:///?uid?sub?
overlay syncprov
syncprov-checkpoint     100 60
syncprov-sessionlog     100
database        config
rootpw          {SSHA}mAatH6MGv5DMyoDsx4M2YSB+pMmo9vF1
database        monitor
```

Anexo AD – Fichero de configuración openldap/slapd.access.conf (común)

```
access to *
        by peername.ip="127.0.0.1" read
        by dn.regex="cn=(.*),ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org" read
        by * break
```

Anexo AE – Fichero de configuración DB_CONFIG (común)

```
set_cachesize 0 268435456 1
set_lg_regionmax 262144
set_lg_bsize 2097152
```

Anexo AF – Fichero de configuración ldap/slapd.d/slapd.conf (réplica)

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/misc.schema
include         /etc/ldap/schema/amavisd-new.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/corba.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/openldap.schema
include         /etc/ldap/schema/samba.schema
include         /etc/ldap/schema/authldap.schema
include         /etc/ldap/schema/java.schema
pidfile         /var/run/slapd/slapd.pid
argsfile   /var/run/slapd/slapd.args
modulepath      /usr/lib/ldap
moduleload      syncprov.la
```

```
moduleload      back_monitor.so
moduleload      back_hdb.so
moduleload      back_bdb.so
TLSCertificateFile      /etc/ssl/slapd/lanzarote.tfc-uoc.dyndns.org.crt
TLSCertificateKeyFile   /etc/ssl/slapd/lanzarote.tfc-uoc.dyndns.org.key
TLSCACertificatePath    /etc/ssl/certs/
TLSVerifyClient         never
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
access to *
        by anonymous auth
loglevel  sync stats
database        hdb
suffix          "dc=tfc-uoc,dc=dyndns,dc=org"
checkpoint      1024    5
cachesize       65536
idlcachesize    65536
rootdn          "cn=Directory Manager,dc=tfc-uoc,dc=dyndns,dc=org"
rootpw          {SSHA}VJ1dAYUVJASJHhviv255zRA4c7UL7AHa
directory/var/lib/ldap/tfc-uoc/
index   objectClass,entryUUID,entryCSN,employeeNumber,mailHost,memberUid,mailRoutingAddress     eq
index   dc,o,ou,cn,mail,sn,givenName,uid     eq,pres,sub
index   uidNumber,gidNumber,loginShell,disableImap,disablePop3    eq,pres
sizelimit 1000
timelimit 60
include   /etc/ldap/slapd.d/slapd.access.conf
overlay   syncprov
```

```
syncrepl rid=001
        provider=ldaps://ldapmaster.tfc-uoc.dyndns.org:636
        type=refreshAndPersist
        searchbase="dc=tfc-uoc,dc=dyndns,dc=org"
        filter="(objectClass=*)"
        scope=sub
        schemachecking=on
        bindmethod=simple
        binddn="cn=replicator,ou=system-users,dc=tfc-uoc,dc=dyndns,dc=org"
        credentials=15u$eR041979
        retry="60 10 600 20"
        starttls=yes
database        config
rootpw          {SSHA}mAatH6MGv5DMyoDsx4M2YSB+pMmo9vF1
database        monitor
```

Anexo AG – Fichero de configuración perdition/perdition.imap4.conf

```
timeout         60
ssl_mode        none
imap_capability "IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
THREAD=REFERENCES SORT QUOTA IDLE"
map_library     /usr/lib/libperditiondb_ldap.so.0
map_library_opt 3:ldaps://lanzarote.tfc-uoc.dyndns.org:636/dc=tfc-uoc%2Cdc=dyndns%2Cdc=org?uid,mailhost?sub?
(uid=%25s)?!bindname=cn=mtauser%2Cou=system-users%2Cdc=tfc-uoc%2Cdc=dyndns%2Cdc=org,!x-
bindpw=12345678Ab
strip_domain    remote_login,servername_lookup
connection_logging
```

Anexo AH – Fichero de configuración perdition/perdition.imap4s.conf

timeout 60

ssl_mode none

imap_capability "IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE"

map_library /usr/lib/libperditiondb_ldap.so.0

map_library_opt 3:ldaps://lanzarote.tfc-uoc.dyndns.org:636/dc=tfc-uoc%2Cdc=dyndns%2Cdc=org?uid,mailhost?sub?(uid=%25s)?!bindname=cn=mtauser%2Cou=system-users%2Cdc=tfc-uoc%2Cdc=dyndns%2Cdc=org,!x-bindpw=12345678Ab

strip_domain remote_login,servername_lookup

connection_logging

root@LANZAROTE:~# cat /etc/perdition/perdition.imap4s.conf | egrep -v "^#|^$|^;"

timeout 60

ssl_mode ssl_all

ssl_cert_file /etc/ssl/perdition/lanzarote.tfc-uoc.dyndns.org.crt

ssl_key_file /etc/ssl/perdition/lanzarote.tfc-uoc.dyndns.org.key

ssl_ca_path /etc/ssl/certs

ssl_no_cert_verify

ssl_no_cn_verify

ssl_cert_accept_self_signed

ssl_cert_accept_expired

ssl_cert_accept_not_yet_valid

imap_capability "IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE"

map_library /usr/lib/libperditiondb_ldap.so.0

map_library_opt 3:ldaps://lanzarote.tfc-uoc.dyndns.org:636/dc=tfc-uoc%2Cdc=dyndns%2Cdc=org?uid,mailhost?sub?(uid=%25s)?!bindname=cn=mtauser%2Cou=system-users%2Cdc=tfc-uoc%2Cdc=dyndns%2Cdc=org,!x-bindpw=12345678Ab

strip_domain remote_login,servername_lookup

connection_logging

AnexoAI – Fichero de configuración perdition.pop3.conf

timeout 60

ssl_mode none

pop_capability "TOP STLS USER LOGIN-DELAY 10 PIPELINING UIDL"

map_library /usr/lib/libperditiondb_ldap.so.0

map_library_opt 3:ldaps://lanzarote.tfc-uoc.dyndns.org:636/dc=tfc-uoc%2Cdc=dyndns%2Cdc=org?uid,mailhost?sub?(uid=%25s)?!bindname=cn=mtauser%2Cou=system-users%2Cdc=tfc-uoc%2Cdc=dyndns%2Cdc=org,!x-bindpw=12345678Ab

strip_domain remote_login,servername_lookup

connection_logging

Anexo AJ – Fichero de configuración perdition.pop3s.conf

timeout 60

ssl_mode ssl_all

ssl_cert_file /etc/ssl/perdition/lanzarote.tfc-uoc.dyndns.org.crt

ssl_key_file /etc/ssl/perdition/lanzarote.tfc-uoc.dyndns.org.key

ssl_ca_path /etc/ssl/certs

ssl_no_cert_verify

ssl_no_cn_verify

ssl_cert_accept_self_signed

ssl_cert_accept_expired

ssl_cert_accept_not_yet_valid

pop_capability "TOP STLS USER LOGIN-DELAY 10 PIPELINING UIDL"

map_library /usr/lib/libperditiondb_ldap.so.0

map_library_opt 3:ldaps://lanzarote.tfc-uoc.dyndns.org:636/dc=tfc-uoc%2Cdc=dyndns%2Cdc=org?uid,mailhost?sub?

(uid=%25s)?!bindname=cn=mtauser%2Cou=system-users%2Cdc=tfc-uoc%2Cdc=dyndns%2Cdc=org,!x-bindpw=12345678Ab

strip_domain remote_login,servername_lookup

connection_logging