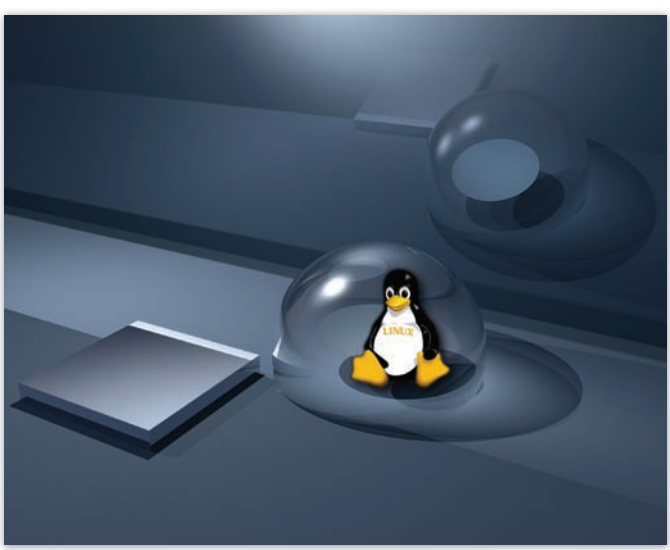
Linux en el instituto, segunda parte

Antonio Gómez

En la anterior entrega, reestructuramos la red local de nuestro centro educativo centralizándola en un equipo configurado como servidor a varios niveles. En esta segunda parte, crearemos un servicio experimental, pero funcional, de correo electrónico interno y estableceremos un sistema web disponible de manera individual para cada miembro de la comunidad educativa que demuestre necesitarlo.



En nuestro anterior artículo, habíamos empezado a relatar la experiencia llevada a cabo en el IES Eduardo Valencia, de Calzada de Calatrava, orientada a instalar un ordenador con Ubuntu Server 9.04, que racionalizara la (raquítica) conexión a Internet de que dispone (no llega a 3 Mb), ofreciera un filtro a través de *SQUID* que protegiera a nuestros alumnos menores de edad del acceso a contenidos inapropiados, e implementara un sistema de carpetas de red para alumnos, profesores y Departamentos Didácticos con una organización de permisos de lectura, escritura y ejecución muy bien delimitados, utilizando *SAMBA*. A lo largo de esta segunda parte, incidiremos en la instalación y configuración de *APACHE2* para poder ofrecer a cada miembro de nuestra comunidad educativa que demuestre necesitarlo, su propio sitio web, adecuadamente preparado y protegido contra malos usos, y en los pasos necesarios para empezar a poner en marcha un servicio de correo electrónico disponible para profesores y Departamentos Didácticos, con *POSTFIX, DOVECOT* y *SQUIRRELMAIL*. Por último, ampliaremos el interfaz *WEBMIN* que centró parte del anterior artículo a la herramienta *USERMIN* que granjeará un acceso limitado a algunos profesores a determinadas funciones del servidor (cambio de claves internas, consulta de correo,...).

Repasando un poco lo ya hecho

Recordemos cual era la estructura de red que deseábamos: el centro se conecta a Internet a través de un router estándar que alimenta a cuatro subredes con un origen común:

- Aula Althia: sala con dieciséis ordenadores con arranque dual Windows y Molinux, parte de un proyecto de la JCCM de hace un par de años, para mejorar la informatización de los colegios e institutos.
- Aula de informática: sala con dieciocho ordenadores con arranque dual Windows y Ubuntu.
- Departamentos Didácticos: desde un switch, se cableó a lo largo de todo el centro el acceso a Internet del ordenador de cada Departamento. Unos veinte ordenadores más, contando los tres de la biblioteca del instituto.

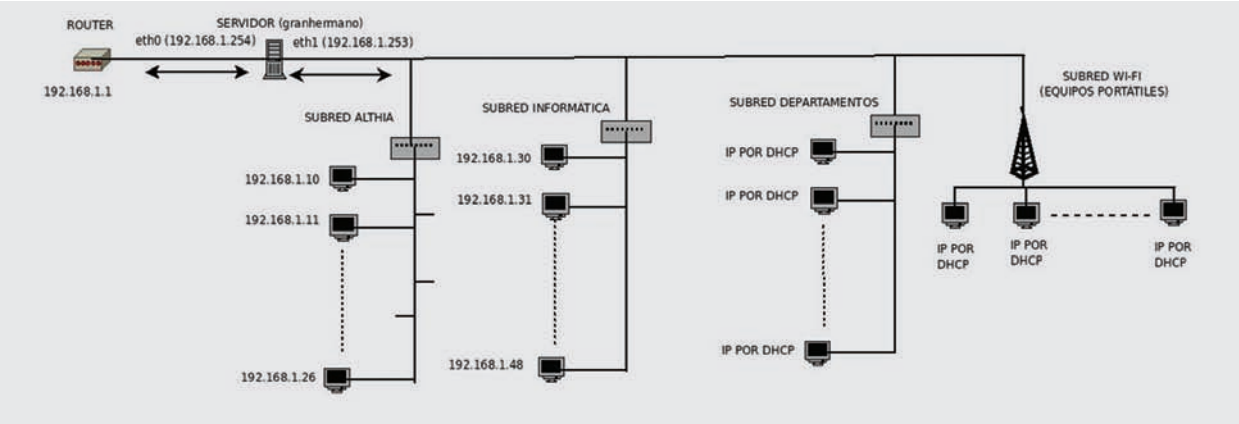


Figura 1. En la primera parte del artículo, reorganizábamos de esta manera las subredes del IES

- Red Wi-Fi: desde hace dos años, la Junta de Comunidades dotó también de los recursos necesarios para garantizar el acceso wi-fi a cualquier ordenador desde cualquier punto del instituto. A la sazón, tenemos instalada la red correspondiente de puntos de acceso por todo el edificio.

Lo que hicimos en el número anterior fue introducir nuestro servidor, al que llamamos, en un arranque de humor, *granhermano*, a la cabeza de este conglomerado, utilizando dos tarjetas de red, *eth0* (conexión al router, IP local 192.168.1.254) y *eth1* (conexión a la red LAN, IP local 192.168.1.253), tal y como se puede ver en la Figura 1.

Al final del artículo, dejábamos la estructura de red completamente operativa, funcionando granhermano como un proxy transparente, accesible desde equipos externos por canales SSH o a través del interfaz web WEBMIN, para garantizar nuestro acceso al equipo incluso en fracciones horarias en las que el aula en la que está instalado está ocupada por algún grupo de alumnos, y disponiendo de un sistema de usuarios y grupos con un sistema de permisos de lectura, escritura y ejecución (notación octal) a través de SAMBA, que granjeará el libre intercambio (dentro del ámbito de dichos permisos), de archivos y carpetas entre distintos equipos de alumnos y profesores, independientemente del sistema operativo en el que estamos trabajando. Procedamos ahora con la instalación y configuración de nuestros servidores web y de correo.

Nuestro propio servidor web con APACHE2

En el actual estado de las cosas, estamos preparados para configurar un sistema medianamente estable que permita a cada Departamento, profesor o grupo de alumnos disponer de su propia web de cara a la realización de distintas actividades de enseñanza-aprendizaje. Partiendo de la configuración básica, vamos a explorar distintas posibilidades de *APACHE2* en un entorno multiusuario, incluyendo la protección de contenidos restringidos a determinados miembros de la comunidad educativa y la combinación *APACHE+SAMBA* que permite la gestión de sitios web basados en CMS como *Joomla!*, desde equipos que en el instituto pueden funcionar independientemente desde Windows, Molinux o Ubuntu.

Instalación básica de APACHE2 y paquetes complementarios

Apache2 como paquete viene instalado casi de manera obligada con Ubuntu Server. De todos modos, *aptitude* nos ayudará a "bajarnos" cualquier componente que echemos de menos. Por ejemplo, Joomla! está cada vez más presente en las webs educativas de nuestra comunidad. Joomla! necesita que el servidor entienda el lenguaje PHP (mínimo versión 4) y MySQL (recomiendo la versión 5). Además, sería muy conveniente una herramienta como *PHPMyAdmin* para gestionar las bases de datos en MySQL que utilizaremos por cada sitio web de este tipo que queramos alojar:

```
# aptitude install mysql-server php5
libapache2-mod-php5 php5-gd php5-dom
php5-pgsql php5-mysql phpmyadmin
```

Al instalar *PHPMYADMIN*, que es un simple interfaz web para poder gestionar más cómodamente las bases de datos MySQL que estén funcionando en *granhermano*, se nos pedirá (como es lógico) una contraseña para un usuario con opciones de *root.* Todos los recursos web a los que acudimos mientras investigábamos y recopilábamos información para una correcta instalación desaconsejan *expresamente* trabajar por sistema con un usuario *root* en estas bases de datos, por razones de seguridad, así que crearemos un usuario aparte con todos estos privilegios para empezar a trabajar con *PHPMYADMIN*, y después procuraremos seguir una política bien definida de crear un

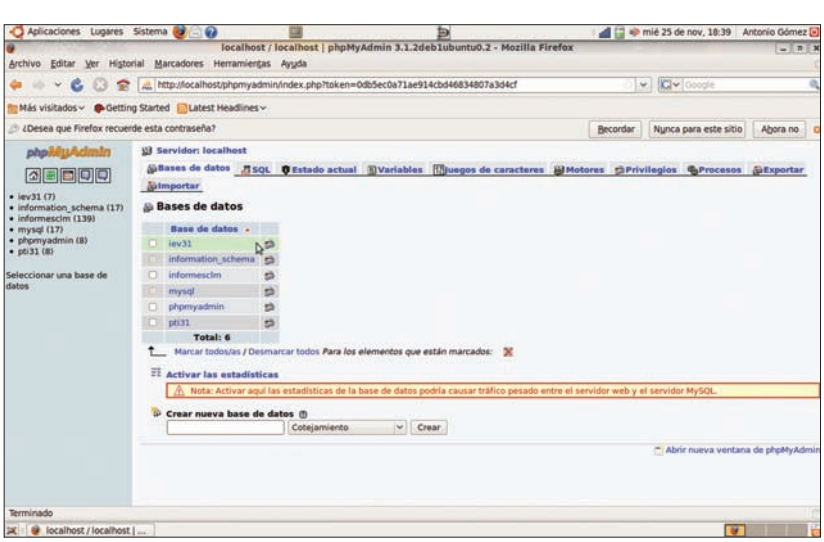


Figura 2. PHPMyAdmin acaba siendo una herramienta imprescindible en la configuración de sitios web de tipo CMS

usuario con todas las atribuciones diferenciado para cada base de datos que precisemos utilizar (un usuario MySQL para nuestra página principal en *Joomla!*, otro para páginas secundarias que otros profesores quieran tener en sus carpetas *home* (véase el apartado siguiente sobre *directorios virtuales*), otro para instalar un wiki (nuestra *CALZALDEAPEDIA*, aún en fase beta)...

Esta interesante (y al final imprescindible) herramienta es también manejable desde WEBMIN.

Por defecto, la dirección en la que alojar nuestros sitios web será */var/www/*.

En su estado original, si en nuestro explorador tecleamos la dirección *http://192.168.1.254* o simplemente *http://granhermano*, accederemos a la típica página de ¡Funciona!, que será rápidamente sustituida en cuanto introduzcamos nuestra propia carpeta. Recordemos que estas direcciones sólo servirían dentro de nuestra red local. Si queremos acceder desde nuestro domicilio, por ejemplo, tendríamos que teclear en la barra de direcciones la IP pública de nuestro servidor.

Directorios virtuales

Pero podemos mejorar nuestra situación. No olvidemos que una comunidad educativa está compuesta por muchos grupos, subgrupos, grupúsculos o simplemente personas individuales que pueden encontrar de utilidad disponer de su propio sitio web dentro del servidor. Es por eso que hemos encontrado tan útil *APACHE2* en combinación (o no) con *WEBMIN*: es sencillísimo utilizar directorios virtuales. Pero como para ello habría que montar un servidor DNS, que no era objeto de este artículo, nos limitaremos a crear una web para un departamento, por ejemplo, Tecnología:

```
# sudo mkdir /var/www/tecnologia
# sudo chmod -R 777 /var/www/
tecnologia
```

Hemos dispuesto un espacio web en *http://granhermano/tecnologia*, y hemos concedido (al menos temporalmente) todos los permisos de lectura y escritura para facilitar que este departamento pueda crear su espacio Joomla! o similar sin ninguna cortapisa. Responsabilidad posterior del administrador será remodelar dichos permisos una vez este espacio web haya sido instalado y testeado de manera definitiva. Este sistema presenta el pequeño problema de que es imprescindible la colaboración del administrador de la red en la creación de la web del Departamento, al menos en sus primeros pasos. A continuación, proponemos otro método que dotaría de mayor autonomía al correspondiente Departamento.

Otro modo muy interesante (aunque algo más peligroso) de disponer de una web para cada usuario dentro del servidor sería la utilización de enlaces duros o blandos (según elección) a los directorios en *home,* sabiendo que cada Departamento tiene acceso a dicha carpeta en forma de carpeta de red. Por ejemplo, en el Departamento de Lengua Castellana y Literatura, están trabajando actualmente en su propia pequeña web sobre Literatura Universal con varios alumnos de Bachillerato. Para darles mayor autonomía, este grupo crea dicha web en su carpeta */home/lengua* (accesible como unidad de red desde WINDOWS XP).

Entramos en *granhermano* como superusuario, y nos limitamos a teclear:

```
cd /var/www
ln -s /home/lengua lengua
```

Listado 1. Archivo default de configuración del servidor web general

```
<VirtualHost *:80>
        ServerAdmin administrador@eduardovalencia.no-ip.org
        DocumentRoot /var/www
             <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>
</VirtualHost>
```

Listado 2. Contenido del archivo .htaccess que restringe el acceso web

```
AuthName "No, no, no... si no eres profesor del centro, no pasas... "
AuthType Basic
AuthUserFile /etc/usuariosapache
Require valid-user
```

Listado 3. El archivo /etc/apache2/sites-enabled/000-default modificado para restringir contenidos

```
<VirtualHost *:80>
        ServerAdmin administrador@eduardovalencia.no-ip.org
        DocumentRoot /var/www
             <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>
         <Directory /var/www/sensible/>
         AllowOverride AuthConfig
         </Directory>
</VirtualHost>
```

Listado 4. Instalación de los paquetes necesarios para el servidor de correo desde la shell

```
# sudo aptitude install postfix
# sudo aptitude install dovecot-imapd dovecot-pop3d
# sudo aptitude install squirrelmail
# sudo ln -s /usr/share/squirrelmail /var/www/correo
```

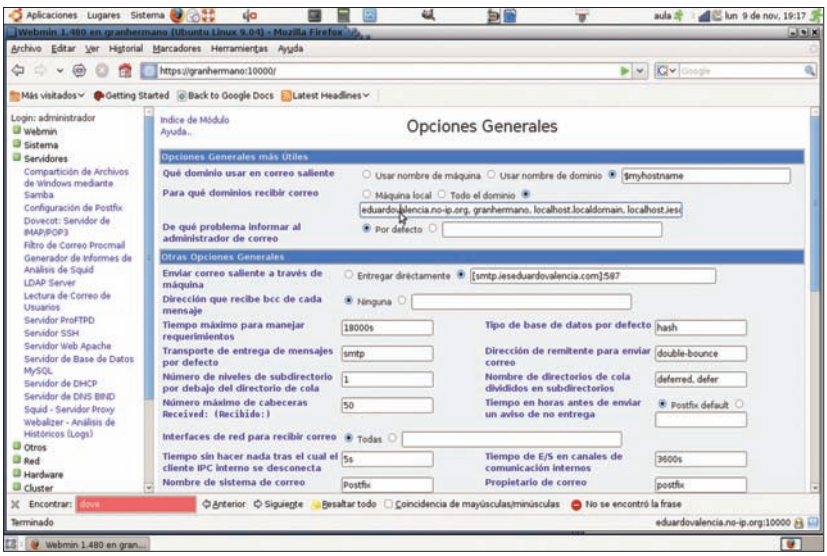


Figura 3. Configurando las opciones generales de POSTFIX

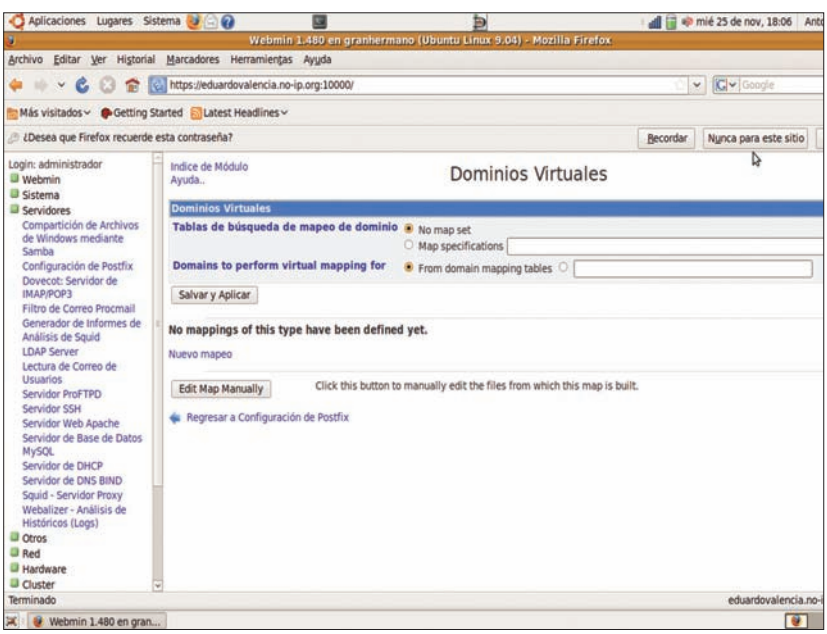


Figura 4. Postfix incorpora la posibilidad de trabajar con usuarios virtuales

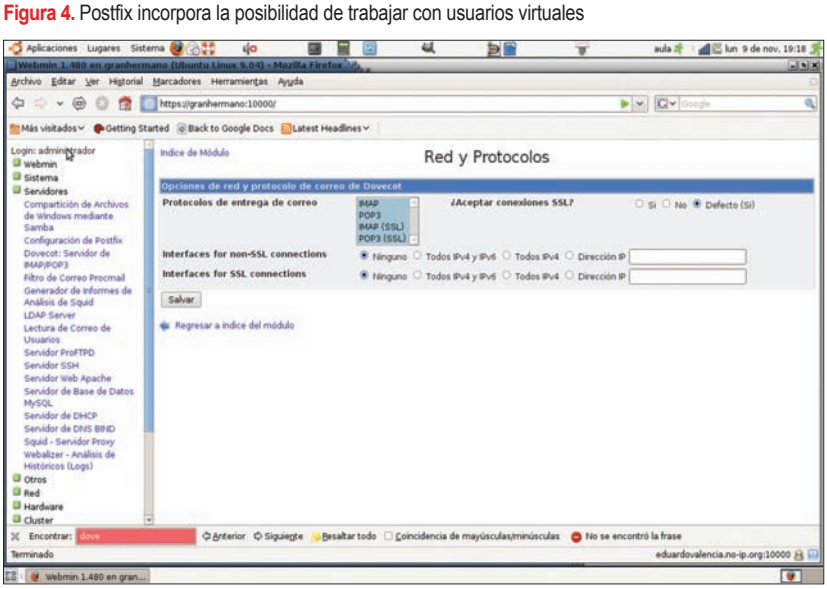


Figura 5. Seleccionando todos los protocolos disponibles para DOVECOT

Hemos generado un enlace blando dentro de nuestra web general al directorio */home/lengua*, de modo que todos los cambios que este grupo realice (sea desde Windows o desde Linux) en dicha carpeta, serán accesibles vía web, a través del puerto 80, en la dirección *http://granhermano/lengua* o *http://IPPUBLICA/lengua* si accedemos desde fuera de la red local.

Este método es bastante más peligroso porque estamos enlazando desde una carpeta accesible sólo para el usuario *www-data* a una carpeta de usuario dentro de */home/lengua*, que para más inri, está siendo modificada desde varios equipos por alumnos que pueden estar trabajando con Molinux, Ubuntu, y por qué no decirlo, con W....

¡Uf!. ¡Casi mencionamos a *aquél-que-no-debe-ser-nombrado*! Puede tacharse a este redactor de fanático incorregible (podría ser, no lo niega, aunque lo duda), pero en este caso, sigue la misma política que la empresa objeto de esta pequeña nota de humor: ignorar sistemáticamente al antagonista. ¿Opina el lector que esta pequeña salida no venía al caso en este artículo? ¡Podría ser! ¡Sigamos!

Decíamos que estamos creando un potencial problema tanto de incompatibilidad de los permisos de cada uno de los equipos que están participando en este proyecto, como de seguridad general, al proporcionar al usuario malicioso un posible "camino" a nuestro servidor...

A todo esto, el modo más inteligente de resolver este problema sería utilizar el complemento *a2enmod*:

```
# a2enmod userdir
```

que permitiría a cada usuario crear su propia página web en su carpeta */home*, creando, eso sí, una carpeta denominada *public_html*.

De este modo, el usuario *lengua* (en nuestro ejemplo), crearía su web en */home/lengua/public_html*, que sería accesible en la dirección *http://IPPUBLICA/~lengua*.

La virgulilla (~) es un carácter incómodo para la mayoría de los usuarios (tecla Alt Gr+4), por eso puede crearse (si no está ya creado) un archivo denominado *alias* en la dirección */etc/apache2/conf.d/alias*, con la relación de direcciones que deseamos asignar a cada usuario:

```
alias /lengua/ /home/lengua/public_
html
```

Un detalle muy interesante para comentar, a pesar de la simplicidad que buscamos en un

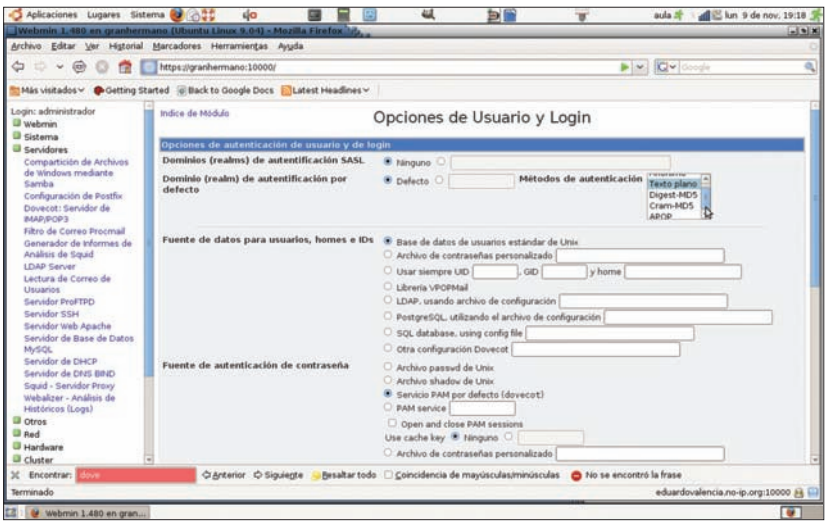


Figura 6. Seleccionando PAM como opción de acceso para DOVECOT

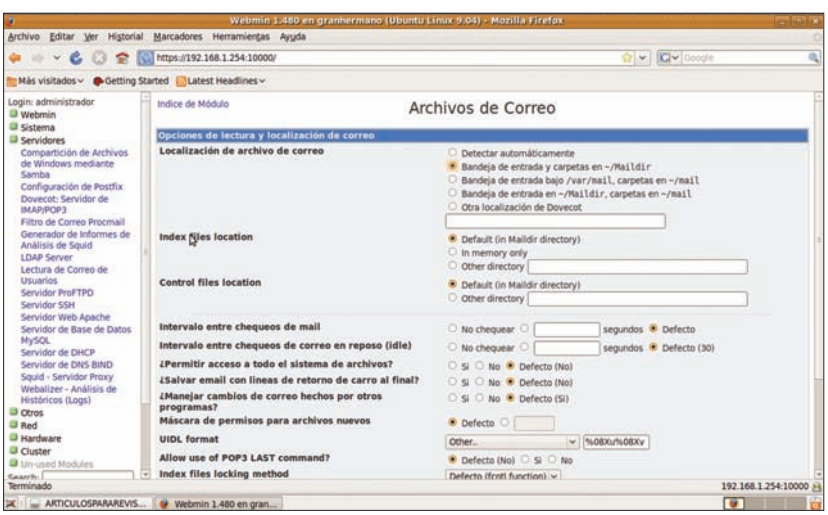


Figura 7. Seleccionamos maildir como forma de almacenado de archivos

texto orientado al usuario novel, es el de posibilitar que el explorador web pueda acceder o no a la lista de carpetas del directorio web al que ha accedido, en caso de que no especifique un archivo *.html o *.php concreto, y no exista *index*. En el archivo de configuración del servidor APACHE2 que corresponda (en nuestro ejemplo, */etc/apache2/sites-available/default*, aunque esto depende de cómo hayamos configurado dicho servidor, y si hemos dispuesto o no varios servidores virtuales), podemos encontrarnos con una línea de opciones que incluye las posibilidades *Indexes* y *FollowSymLinks,* entre otras. Dichas opciones, si están presentes, activan, en el caso de *Index*, el acceso libre a dichas carpetas, y en el caso de *FollowSymLinks*, la posibilidad de seguir los enlaces a carpetas fuera de */var/www* (ya hemos mencionado esta posibilidad para dar más autonomía a las posibles web de cada Departamento Didáctico). Por seguridad, es conveniente borrar la opción *Index,* aunque necesitaremos conservar el acceso a carpetas enlazadas (ver Listado 1).

Restringiendo contenidos web a usuarios autorizados

Si, como parece, nuestro experimento lleva el camino de convertirse en un elemento permanente dentro de los recursos TIC (Tecnologías de la Información y de la Comunicación, en la jerga educativa actual), es evidente que deberemos aumentar la seguridad de *APACHE2*, al menos en lo relativo al acceso a algunos directorios.

Supongamos que hemos incluido en */var/www/* una carpeta que recoge un conjunto de archivos para uso interno de los Departamentos Didácticos del Centro, y a los que no deseamos dar acceso público. El objetivo es permitir al profesor con permiso para ello poder acceder desde su casa, por ejemplo, a dichas carpetas.

Supongamos que tenemos una carpeta en */var/www/sensible/*.

El primer paso será crear un archivo que contenga los usuarios con acceso autorizado a esta dirección; supongamos que queremos dar acceso a *profesor* con la contraseña *docencia*:

```
# htpasswd -c /etc/usuariosapache
profesor
```

Se nos pedirá la contraseña (dos veces). Este comando crea un archivo en */etc/* llamado *usuariosapache*, e introduce el nombre y la clave especificados. Si queremos repetir este paso en otras ocasiones, no será necesaria la opción *-c*. A continuación, nos situaremos en la carpeta a restringir (*/var/www/sensible*), y crearemos un archivo *.htaccess*, con el siguiente contenido (ver Listado 2). Ya sólo nos queda incluir la referencia a dicha restricción en el archivo de configuración del servidor (*/etc/apache2/sites-enabled/000-default*). Dicha modificación se reflejaría en el Listado 3.

¡Y listo! Sólo resta reiniciar el servidor web:

```
# /etc/init.d/apache2 restart
```

Podrá comprobarse, acto seguido, que el avezado usuario de nuestro sitio web tendrá libre acceso a todos los contenidos, excepto a *sensible*. Una ancha sonrisa cruzará en este momento la cara del profesor responsable de estos contenidos, siempre celoso de la privacidad en lo referente a datos de carácter público dentro del centro (aunque, seamos sinceros, nunca hay nada remotamente comprometedor; ¡ni siquiera interesante!, en estas carpetas...).

Nuestro propio servidor de correo interno

Una vez hemos decidido qué usuarios tendrán acceso directo, con su propia carpeta *home*, a nuestro flamante servidor, estamos en condiciones de dotarles de un sistema interno de correo, que podría incluso llegar a externalizarse fácilmente, utilizando servicios de DNS dinámicas, como *dyndns* o *no-ip*.

Figura 8. Entrando en nuestro buzón de correo a través de SQUIRRELMAIL

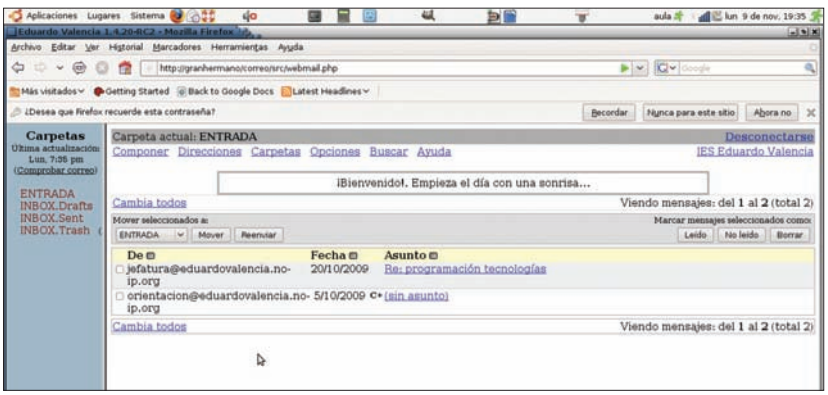


Figura 9. Apariencia del buzón de correo del usuario

Para ello, vamos a disponer de tres herramientas complementarias.

Servidor de correo SMTP *POSTFIX*: es un MTA (*Mail Transfer Agent*), encargado de recoger y enviar los mensajes de texto con archivos adjuntos que conforman un correo electrónico desde el servidor a Internet.

Servidor *DOVECOT*: es un servidor IMAP (*Internet Message Access Protocol)* que gestionará los mensajes entrantes y salientes entre todos los usuarios con acceso a *granhermano*.

Interfaz web *SQUIRRELMAIL*: instalaremos y configuraremos esta herramienta web para facilitar el acceso de todos los usuarios a su buzón de correo electrónico.

Como siempre, incluiremos el listado de instalación de todos los paquetes implicados, independientemente de que vengan incluidos en *Ubuntu Server 9.04* (véase Listado 4).

En las últimas versiones, *Ubuntu* incluye Squirrelmail dentro de sus repositorios.

Un último paso incluye la generación de un enlace blando desde la carpeta donde Squirrelmail actúa a una carpeta dentro de nuestra página web, que llamaremos *correo.*

Por si alguien lo había olvidado, o no lo hemos mencionado suficiente número de veces, somos usuarios de Linux muy limitados, así que de nuevo recurriremos a la configuración vía nuestro amadísimo *WEBMIN*.

Instalación y configuración de POSTFIX

Postfix puede funcionar desde el mismo momento de su instalación. Según lo que queramos hacer, sobre todo de cara al acceso desde fuera de nuestra red, es interesante jugar con las opciones generales: qué dominios utilizar en correo saliente, para qué dominios recibir correo... Eso sí, no hay que olvidar, que si queremos utilizar este sistema con acceso externo, deberemos asegurarnos de tener abierto el puerto 25, tanto en nuestro router, como desde el *SQUID*.

Así, por ejemplo, en *WEBMIN->Servidores->Configuración de Postfix->Opciones Generales*, especificaremos para qué dominios recibir correo (granhermano para funcionamiento en local, eduardovalencia.no-ip.org para correos exteriores), y qué dominio utilizar en el correo saliente (especificado en la variable $hostname, que en el apartado de Opciones Generales en el que nos encontramos, se correspondería con el Nombre de máquina de internet de este sistema de correo).

POSTFIX incluye la interesantísima opción de crear direcciones de correo virtual (*WEBMIN->Configuración de Postfix->Dominios Virtuales*). Esta opción permitiría, si reuniéramos los suficientes conocimientos, crear un usuario virtual de correo (no serían auténticos usuarios dentro de granhermano) por cada uno de los alumnos y profesores que conforman nuestra comunidad educativa. Esta herramienta trabajaría en conjunto con una base de datos MySQL que trabajaría en combinación con Postfix, de acuerdo a unas tablas denominadas de mapeo de dominio. Estas tablas incluirían datos tan simples como el nombre y el curso de nuestros alumnos (importadas desde cualquiera de las bases de datos en que constan), quizás su número de pasaporte escolar o de matrícula para utilizar como índice, de modo que ya desde principio de curso cada uno de nuestros chicos contaría con una dirección de correo sin necesidad de utilizar servicios de corte gratuito, sean propios del entorno doméstico del alumno, sean creados específicamente en el marco de la actividad que sea que estén llevando a cabo con un profesor, con la pérdida de tiempo que suelen conllevar.

Pero, como diría Michael Ende, esa es otra historia, y será contada en otra ocasión (¿han leído La historia interminable?, ¡muy recomendable!).

Instalación y configuración de DOVECOT

Al instalar *DOVECOT*, hemos considerado que pueden utilizarse los protocolos IMAP o POP3, pero en realidad lo más normal es que utilicemos el IMAP. De todos modos, para asegurar las cosas, como usuarios novatos que somos, priorizaremos el asegurar que funcione sobre la seguridad propiamente dicha (puedo oír como rechinan los dientes de los usuarios avezados, pero repito que estamos experimentando y aprendiendo). Así que configuraremos *DOVECOT* para que funcione con ambos protocolos, incluyendo la encriptación SSL (aunque no vamos a utilizarla hoy), y nos aseguraremos, en las opciones de login de usuario, de que el modo de acceso que utilizará *DOVECOT* es el que venía por defecto, el servicio PAM (también podríamos elegir el archivo *shadow* de contraseñas de usuario, pero sobre esta opción aún no hemos hecho suficientes pruebas).

Al objeto de aclarar esta última aseveración, intentemos reenfocar algunos conceptos:

- Un servicio de correo electrónico siempre tiene dos partes: el servidor MTA y el servidor interno IMAP/POP.
- El MTA, *Mail Transfer Agent*, se encarga de transferir los archivos necesarios a otras máquinas en el exterior. De ello se encarga el anteriormente mencionado *POSTFIX*, que trabaja con el protocolo SMTP, *Service Mail Transfer Protocol*. Este servidor sale al exterior a través del puerto 25, que deberemos tener abierto en nuestro router y en *SQUID* (ver anteriores apartados).
- El servidor IMAP/POP, que puede trabajar con ambos protocolos, es el encargado de asignar, dentro de la máquina, cada correo al usuario correspondiente. Necesitaremos tener abierto el apartado 143.
- Para configurar adecuadamente el servidor *DOVECOT* debemos tener muy claro qué usuarios van a tener acceso al servicio de correo, y qué sistema de identificación vamos a utilizar. El archivo de

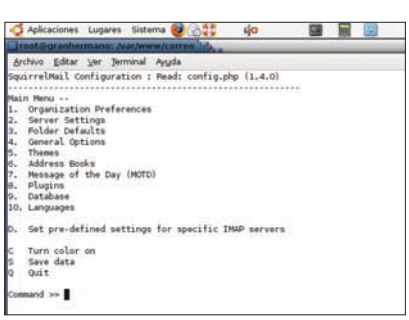


Figura 10. Opciones de configuración de SQUIRRELMAIL desde consola

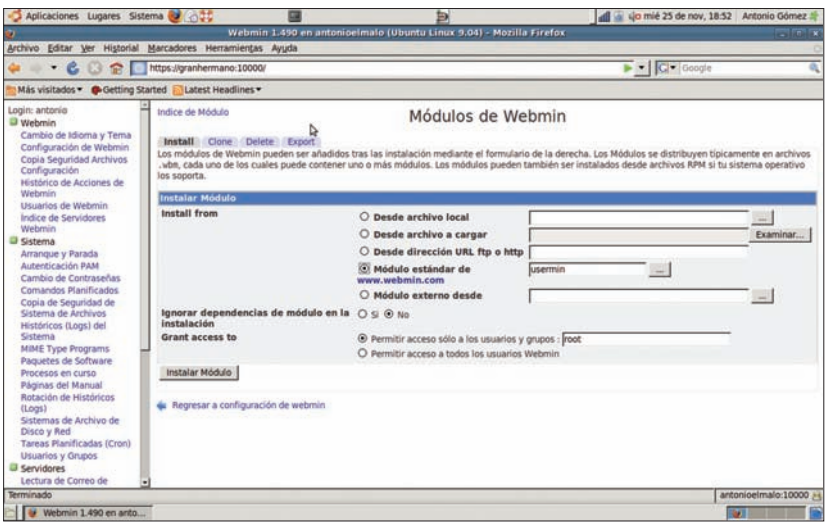


Figura 11. Desde el apartado de Configuración, podemos instalar módulos específicos de WEBMIN

configuración correspondiente está en */etc/dovecot/dovecot.conf*. Es un archivo que viene, por defecto, lo suficientemente comentado como para que el usuario algo más experto pueda pararse a analizarlo con más profundidad, al objeto de retocar las características de funcionamiento que desee. En *granhermano* nos hemos limitado a configurarlo a través de *WEBMIN*.

- DOVECOT tiene dos sistemas de ordenación y almacenamiento de los mensajes: Maildir y Mailbox. Mailbox guarda todos los mensajes en un solo archivo de carácter creciente, situado en /var/spool/mail/usuario. Maildir, por su parte, crea una carpeta mail en la home de cada usuario, donde guarda los mensajes en archivos individuales, permitiendo a su vez que varios procesos puedan acceder a estas carpetas. Nosotros nos decantamos por este último sistema.

Squirrelmail

En realidad, no hay gran cosa que hacer con Squirrelmail una vez está instalado. Para saber si el sistema funciona, sólo hay que acceder, desde el navegador, a la dirección (en nuestra red interna) *http://granhermano/correo* e introducir el nombre de usuario y la clave de cualquiera de los Departamentos Didácticos que hemos introducido tal y como hemos ido explicando en los apartados anteriores. La estructura del buzón de correo que se ofrece al usuario es lo bastante sencilla como para no asustar a cualquier compañero que haya escrito un e-mail alguna vez a cualquier dirección.

Si todo funciona correctamente, (de nuevo podemos sentir el amenazante aliento de Murphy tras nosotros), podemos animarnos a tratar de configurar las opciones que nos ofrece *SQUIRRELMAIL*, eso sí, obligadamente desde la consola: `# sudo squirrelmail-configure` o, si no funciona (dependiendo de la versión de *SQUIRRELMAIL* que pudiera hallarse previamente instalada):

```
#  sudo su
# /var/www/correo/configure
```

Las opciones van desde la gestión de posibles plugins, a la selección de temas y plantillas, administración de agendas, e incluso la posibilidad de saludar al usuario con un simpático Message of the Day.

Las opciones de paso obligado son:

- *Organization Preferences*: nombre del centro, dirección web, configuración del logo a utilizar (si queremos personalizar y sustituir a la ardilla símbolo de *SQUIRRELMAIL*)
- *Server Settings*:
  - *Domain: granhermano* para uso en local. En nuestro caso, hemos seleccionado nuestro dominio gratuito, *eduardovalencia.no-ip.org*
  - Sendmail or SMTP: POSTFIX es un servidor SMTP
  - Update IMAP Settings: nos aseguraremos de que SQUIRRELMAIL sabe que trabajamos con DOVECOT en el puerto 143, y que nuestro método de conexión en DOVECOT es el uso de PAM (login)
  - Update SMTP Settings: se indicará si POSTFIX está preparado para trabajar con encriptación TLS, y si exige autenticación.
- *Languages*: podemos seleccionar el lenguaje español, pero es posible que esto no funcione a la primera; habría que reconfigurar el archivo locales que contiene los lenguajes que soporta nuestro granhermano. Desde la shell, podemos probar con la opción: `# dpkg-reconfigure locales` (partiendo de que esté el lenguaje español, es_ES, ya instalado en nuestro equipo, aunque esto suele ser lo más normal).

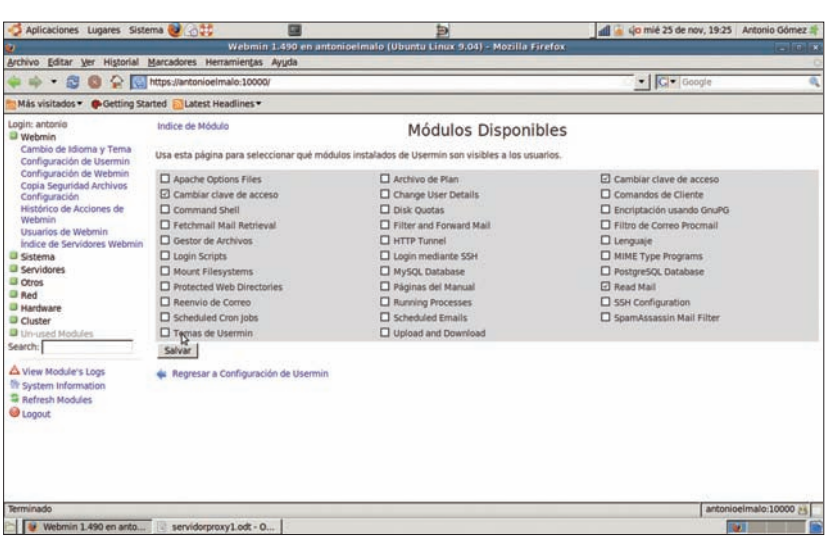


Figura 12. Podemos seleccionar qué funciones serán accesibles desde USERMIN

Concediendo más autonomía a nuestros usuarios: instalando *USERMIN*

USERMIN es un módulo particular de webmin que trabaja a través del puerto 20000 (nuevamente deberemos asegurarnos de tener abierto este puerto, tanto desde SQUID como en nuestro router), y que, configurado a través de WEBMIN, concede a los usuarios que desee el administrador acceso a determinados módulos de webmin. Esta posibilidad, que al principio puede parecer un tanto rebuscada

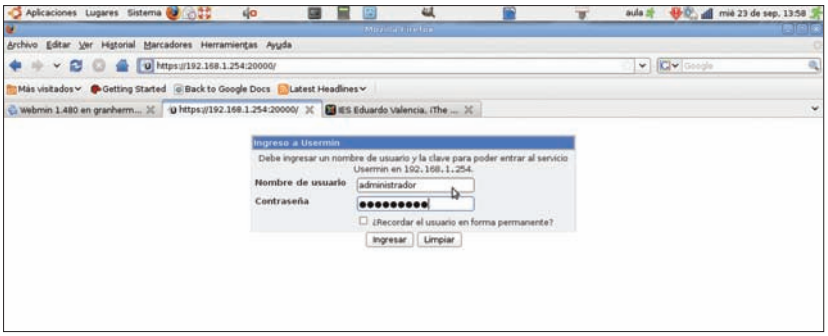


Figura 13. Accediendo a USERMIN como usuario ADMINISTRADOR

para la simplicidad de la que tanto hemos alardeado a lo largo de todos estos párrafos, deviene ciertamente atractiva cuando nos enfrentamos a estas consideraciones:

En nuestro sistema de correo, así como en las contraseñas *SAMBA* para compartir unidades de red, hemos tenido que crear nosotros, como administradores, las contraseñas, para después pasárselas a cada usuario. Cuando nos encontramos (como es el caso de un instituto) con un nutrido grupo de personas, dichas password acaban perdiendo bastante de su privacidad (el administrador se las pasa al Jefe del Departamento Didáctico, éste a cada uno de los profesores, en ocasiones hay que compartir información con la Orientadora...).

Los profesores, muchas veces, son aún peor que los alumnos a la hora de recordar palabras o combinaciones alfanuméricas que no les resulten familiares, hasta el punto de que se arriesgan a utilizar siempre una misma, familiar, y sencillísima palabra. El que esto escribe ha llegado a escuchar, de labios de una compañera, "siempre utilizo esta palabra para todo, hasta para mis transferencias bancarias", sin reparar en que le estaba confiando el propio estado de sus cuentas... Sencillamente deprimente, cuando uno va a ser el responsable de que todo marche.

¡Decidido!, *USERMIN* es ciertamente adecuado para nosotros. A través de esta herramienta, configuraremos un acceso a determinados módulos de *WEBMIN* a todo el profesorado (concretamente, el acceso al buzón de correo y la posibilidad de cambiar la contraseña).

Descargando e instalando *USERMIN*

Hay dos modos de instalar *USERMIN*: directamente a través de *WEBMIN* o descargándolo e instalándolo por consola (en la dirección *http://webmin.com*). Nosotros lo haremos a través de *WEBMIN*.

Será preciso reiniciar la aplicación para que aparezca la nueva opción, *Usermin->Configuración de Usermin*. Desde allí podremos seleccionar los usuarios con acceso a esta herramienta (en un principio, todos), o seleccionar (*Usermin->Módulos disponibles)*, qué módulos serán accesibles para los usuarios con permiso (en la Figura 12, sólo lectura de correo y cambio de claves).

Accediendo a *USERMIN*

El acceso a *USERMIN* será el mismo que el de *WEBMIN*, sólo que utilizando el puerto 20000: *https://TUIPPUBLICA:20000*.

Una vez hemos accedido a la página web, y nos hemos identificado correctamente, sólo habrá que entrar en los módulos que nos interesen (en la Figura 14, las opciones son mail, Change language and theme, Others y Login).

Conclusión

El hecho de centralizar la red informática de un centro educativo en un equipo principal tiene muchas ventajas, que hemos ido enumerando a lo largo de las dos partes que integran este artículo. Hemos resumido lo mejor que hemos podido los pasos que dimos para lograr nuestro objetivo, obviando los múltiples errores y pruebas subsiguientes. Está bastante claro que no hemos incluido absolutamente todas las especificaciones técnicas y protocolos de instalación y configuración que deben seguirse, puesto que lo que tendría el lector en sus manos sería un libro, no un simple artículo. Pero creemos que la lectura de éste puede animar a otros profesionales en nuestra situación a intentar ésta o parecidas experiencias en sus respectivos colegios o institutos.

En cualquier caso, queremos aseverar que el software libre, sea desde la perspectiva del administrador de una red, la del educador que puede utilizar Linux en sus actividades de enseñanza-aprendizaje sin miedo a romper los términos de ninguna licencia comercial, o la del simple usuario que desea romper los límites que le constreñían hasta hace pocos años, el software libre, decimos, ha llegado a la educación para quedarse. En Castilla la Mancha, aumentan año a año las iniciativas que vertebran actividades de aprendizaje de todo tipo en torno a Molinux y Ubuntu, principalmente, y que integran una oferta de calidad creciente y de innegable influencia sobre la formación de los ciudadanos del futuro.

No debe olvidarse que una experiencia como ésta nunca puede desarrollarse de forma unipersonal. Sea activa o pasivamente, siempre necesitaremos la colaboración de otros compañeros docentes, sea como testers o como colaboradores directos. Sirvan estas líneas para agradecerles su colaboración, muy concretamente a D. Félix J. Villanueva, que a lo largo de más de dos cursos, ha realizado tareas en ambas vertientes, siendo un pilar imprescindible para erigir a nuestro pequeño /granhermano/, sin perder nunca el ánimo ni la sonrisa.

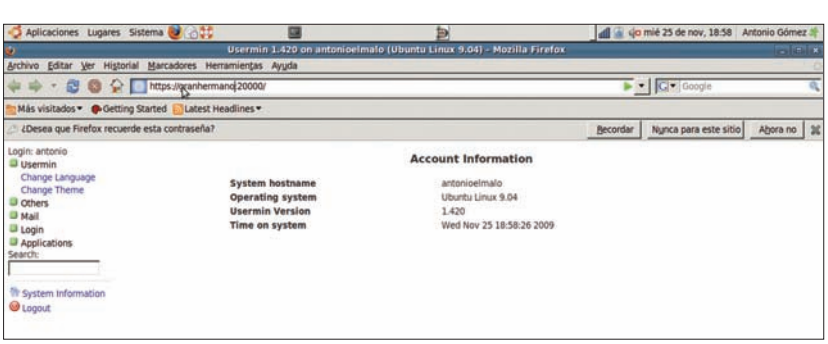


Figura 14. Opciones permitidas en USERMIN

Sobre el autor

Ingeniero Técnico Industrial de formación, Antonio Gómez es profesor de Tecnologías en el IES Eduardo Valencia, en Calzada de Calatrava (Ciudad Real), desde el año 2004, donde desempeña el cargo de Responsable de Equipos Informáticos del centro. Anteriormente ha sido también asesor TIC en el Centro de Profesores de Puertollano (Ciudad Real), con el que sigue desarrollando diversos proyectos de innovación y formación relacionados con el uso del Software Libre en educación.