Software Libre y Educación:

servicios de red, gestores de contenidos y seguridad

Administración Avanzada

José Ángel Bernal, Fernando Gordillo, Hugo Santander y Paco Villegas

13 de mayo de 2005

Índice general

Capítulo 1

Copias de seguridad

> "La idea de hacer una copia de seguridad es hacer copia de tantos datos como sean posibles de tu sistema, pero con excepciones. No es lógico incluir determinados datos ya que perderás tiempo y espacio en el soporte para nada."
>
> *Securing and Optimizing Linux: The Ultimate solution*

1.1. Visión general

Para tener un servidor seguro y confiable es necesario realizar copias de seguridad de forma regular. Los fallos son indeterminados en el tiempo y pueden ocurrir en cualquier momento, pudiendo ser fallos de tipo lógico (borrado accidental de ficheros, errores al procesar shell scripts, ...) o físico (fallo de componentes del ordenador, sobretensiones en el suministro eléctrico, ...). Además, estos fallos pueden producirse de forma fortuita o ser la consecuencia directa de un ataque al servidor por parte de un agente externo. La forma más segura de hacer copias de seguridad es tener los datos almacenados en otro servidor distinto del que se hace la copia o, mejor aún, en un soporte de almacenamiento externo.

A continuación se mostrarán distintos métodos para realizar copias de seguridad usando las utilidades que están por defecto en la mayoría de sistemas linux: `tar`, `dump`, `cpio` y `dd`. Sin embargo, no se entrará en profundidad en su uso, limitándonos a dejar claros los conceptos básicos de las copias de seguridad aplicados a estas herramientas.

También están disponibles herramientas en modo texto como AMANDA, que se utilizarán para hacer más amigable la gestión de copias de seguridad y restauraciones.

La idea de hacer una copia de seguridad es realizar un volcado de la mayor parte del sistema para una posterior restauración de la situación original, todo esto en el menor tiempo posible. Es también conveniente que se realice esta copia en el menor espacio posible, evitando copiar archivos que no sean útiles para la recuperación del sistema.

1.2. Políticas de copias de seguridad

Tan importante como realizar la copia de seguridad es definir una política de copias de seguridad. Cuando se decide hacer copia de seguridad de los archivos del sistema debe adoptarse un esquema de copia de seguridad o *política de copia de seguridad*. No debe caerse en la tentación de "copiarlo todo, por si acaso" y es necesario hacer un estudio previo valorando la importancia de los datos. Existen muchas estrategias para realizar copias de seguridad y la elección de una determinada, depende de las políticas de copia de seguridad adoptadas. Se busca un equilibrio entre el uso de recursos y la disponibilidad de los datos.

Para implementar una política de seguridad, lo primero que se define son los datos de los cuales va a realizarse la copia. Podrán ser archivos sueltos, directorios o sistemas de archivos completos. El esquema propuesto parte de una copia completa del sistema o *backup* total, que será la primera

copia de seguridad que se haga. A partir de esta copia, el resto se realizará de forma incremental, guardando únicamente los archivos que hayan cambiado desde la copia de seguridad inicial[1].

Esta política, a pesar de su simpleza, aporta un ahorro de medios de almacenamiento. Sería más fácil almacenar todos los datos haciendo copias de seguridad completas diarias, pero:

- ¿podemos permitirnos ese gasto de medios de almacenamiento?
- ¿disponemos del sistema el suficiente tiempo para realizar estas copias de seguridad?
- y lo más importante ¿es necesario copiar los mismos datos a diario sin tener la certeza de que hayan cambiado?

Así, supongamos que el sistema al cual se realiza la copia de seguridad es un servidor web. No parece lógico hacer copias de todas las páginas todos los días cuando solo cambian unas pocas páginas que ocupan unos pocos kilobytes. Incluso puede que únicamente se cambien un día de la semana.

Sin embargo, tampoco se puede restringir excesivamente el uso de medios ya que las sucesivas escrituras en el mismo pueden deteriorarlo y producir errores al intentar recuperar los datos. Del mismo modo, no parece conveniente el utilizar siempre el mismo medio físico para almacenar todas las copias. ¿Qué pasaría si este medio se pierde o deteriora? Se perderían todos los datos almacenados y todas las copias de seguridad que contenía el medio.

Con todas estas premisas se llega a la conclusión que hay que buscar el equilibrio entre los datos que se van a guardar, los medios que se van a utilizar y el coste de los mismos. La siguiente política que se plantea intenta equilibrar estos aspectos sin que prime ninguno, pero no debe utilizarse como estándar de copias de seguridad, es simplemente una primera aproximación. Cada sistema tiene sus particularidades y cada administrador debe crear una política de seguridad a medida para sus sistemas.

Supondremos que se dispone de una unidad de cinta para realizar las copias de seguridad, la cual se corresponde con el dispositivo `/dev/st0`. Se utilizarán 6 cintas, etiquetadas CINTA1 a CINTA6, así se realizará la copia de seguridad cada día en soportes distintos. El proceso comienza el viernes haciendo una copia completa y etiquetando esta cinta como CINTA1. La siguiente copia de seguridad se realizará el lunes sobre la CINTA2 y se hará lo mismo hasta el jueves con el resto de cintas. Así, el viernes se ha conseguido una copia completa en CINTA1 y copias incrementales (una por día) en el resto de cintas. Utilizaremos la CINTA6 para hacer nuevamente una copia completa del sistema. La nueva semana empezaría reutilizando las cintas CINTA2 hasta CINTA5, ya que los datos que almacenan se encuentran en la copia completa de CINTA6. La siguiente copia completa se hará en CINTA1 reutilizándola de nuevo.

A pesar de la simplicidad del esquema anterior, el objetivo de la copia de seguridad se cumple de forma satisfactoria. Se puede realizar una primera modificación a la planificación si es necesario que los datos se almacenen por más de 1 semana, guardando las cintas con copias completas por un periodo superior en lugar de reutilizarlas.

Es importante tener claro durante qué periodo de tiempo van a ser válidos los datos ya que esto influirá en el número de soportes que deben guardarse, lo que repercute en el dinero que se invierte en hacer las copias de seguridad. Así, si se realizan las copias de seguridad de un servidor web, no es necesario almacenar copias de la web por más de 1-2 semanas.

Se ha introducido otro concepto importante en las copias de seguridad, el etiquetado del soporte físico donde se guardan las copias. De nada sirve el llevar a cabo una política de seguridad si luego no es posible identificar dónde está la copia de seguridad correspondiente a un determinado día. El soporte donde se realice una copia de seguridad debe estar correctamente etiquetado, conteniendo la fecha en que se ha realizado la copia, así como el nombre de la política de seguridad de la cual forma parte.

[1] Se copian sólo los datos que cambian con respecto a la copia completa. Estas copias parciales se denominan diferenciales cuando se copian los ficheros que han cambiado respecto la copia anterior (ya sea completa o parcial) o incrementales cuando se copian los datos que han cambiado respecto de la última copia completa.

1.3. Dispositivos de almacenamiento

Hasta ahora se ha hablado de cintas como soporte de almacenamiento de las copias de seguridad. Pueden considerarse como el dispositivo de almacenamiento de copias de seguridad por excelencia, existiendo multitud de fabricantes y formatos. Otro dispositivo que está utilizándose cada vez más para la realización de copias de seguridad son los discos, debido a que la relación coste/capacidad es cada vez más pequeña.

La diversidad de soportes para la realización de copias de seguridad puede representar un problema. Puede darse el caso que dispongamos de un dispositivo ultramoderno que sea muy rápido y con una gran capacidad, pero que no sea accesible desde cualquier sistema. Así, si el sistema que alberga el dispositivo deja de estar operativo no será posible recuperar los datos. El dispositivo de almacenamiento que se elija debe ser lo más estándar posible, de forma que en caso de desastre sea facilmente accesible desde cualquier otro ordenador.

En lo referente a las cintas, han sufrido una evolución considerable desde las clásicas cintas de 9 pistas (aquellas con un elemento circular donde se enrollaba la cinta) a las cintas DAT de 4mm. Es por ello que no se entrará en detalle al no estar a disposición de todo el mundo un sistema de almacenamiento basado en cinta. En los ejemplos se utilizará un dispositivo genérico sin entrar en detalles.

Otro dispositivo que no debe olvidarse es el CDROM, que a pesar de su capacidad limitada de 700Mb es importante tener en cuenta por el bajo coste que representa el soporte. Está claro que mejor opción aún es el DVD como soporte para copias. La evolución del mercado ha producido un abaratamiento de los costes tanto de las unidades grabadoras como del soporte DVD que hace que sea ya una opción a tener en cuenta más interesante que el anterior.

La utilización de un disco duro como dispositivo de almacenamiento de las copias de seguridad puede que sea el método más seguro y barato. La capacidad de los discos cada vez es más grande y su precio no es excesivo. Además, puede instalarse el disco duro en cualquier ordenador y acceder así al mismo sin problemas.

El uso del disco duro puede hacerse desde una perspectiva local o remota:

- Copias locales. Se instala el disco duro en el mismo ordenador del que se quiere realizar una copia de seguridad. De este modo las copias estarán accesibles en todo momento, aunque esto presenta varios inconvenientes. ¿Qué pasa si roban el ordenador? Perderíamos al mismo tiempo los datos originales así como todas las copias que se hayan realizado.

- Copias remotas. Un ordenador dedicado a almacenar las copias de seguridad del resto. Los requerimientos de hardware de este ordenador serán básicos, ya que se encargará únicamente de proporcionar espacio en disco al resto de ordenadores. En este caso las copias de seguridad se realizarán a través de la red.

En ambos casos es necesario identificar de forma clara y precisa la localización de las copias de seguridad. Una opción es tener un directorio con la identificación de cada máquina y dentro del mismo los ficheros que contienen las copias de seguridad, teniendo éstas nombres que hagan referencia tanto a la fecha en que se realizó la copia como a los datos que se copiaron y si la copia era completa o incremental.

1.4. Utilidades de archivado

1.4.1. Utilidad tar

La utilidad del sistema `tar` es un programa de archivado, diseñado para almacenar y extraer ficheros desde un archivo (conocido como `tarfile`). Es decir, una estructura de archivos y directorios se guarda en un solo fichero, con la posibilidad de recuperarla posteriormente. Dicho `tarfile` puede estar alojado en una unidad de cinta o en el propio disco duro del servidor como un fichero más.

Supongamos que queremos hacer una copia de seguridad de los ficheros con información sobre usuarios y claves (`/etc/passwd` y `/etc/shadow`).

```
[hugo@fedora backup]$ tar -cvf backup-password.tar /etc/passwd /etc/shadow
tar: Eliminando la / inicial de los nombres
etc/passwd
tar: /etc/shadow: No se puede open: Permiso denegado
tar: Salida con error demorada desde errores anteriores
```

El error aparecido al intentar hacer una copia de seguridad del archivo `/etc/shadow` es debido a que se ha ejecutado la utilidad `tar` con un usuario normal del sistema (hay que recordar que el fichero `/etc/shadow` sólo es visible por el usuario root).

Cuando se realice copia de seguridad de los archivos es recomendable mantener los datos referentes a dueños de los archivos y permisos de acceso. Por esto es conveniente realizar estas operaciones como `root` o verificar que el usuario que realiza la llamada a la utilidad `tar` tiene permiso de acceso a los ficheros de los que va a hacer copia de seguridad.

```
[root@fedora tmp]# tar -cvf backup-password.tar /etc/passwd /etc/shadow
tar: Eliminando la / inicial de los nombres
etc/passwd
etc/shadow
```

De esta forma, en el fichero `backup-password.tar` estarán almacenados los dos ficheros anteriores. Almacena los nombres con un camino (*path*) relativo, al quitarle la / inicial. Lo hace automáticamente para que luego se puedan restaurar los ficheros en un lugar diferente si así se desea, sin tener que machacar los originales.

Para restaurar dichos ficheros, se utilizará el comando `tar -xvf backup-password.tar`.

1.4.2. Utilidad dump/restore

A pesar de ser bastante antigua, la utilidad `dump` es muy utilizada en el mundo Unix y realiza el volcado de sistemas de ficheros completos. Por ejemplo, si queremos realizar una copia de seguridad con `dump` de los siguientes sistemas de ficheros, será necesario realizar una llamada a `dump` por cada uno de ellos.

```
/
/home
/usr
/var
```

También permite realizar las copias de los sistemas de ficheros entre máquinas remotas (`rdump/rrestore`). Como utilidad complementaria está `restore`, que será la encargada de realizar las recuperaciones de las copias realizadas con `dump`.

Una de las principales ventajas de la pareja de utilidades `dump/restore` es que son compatibles entre los distintos sabores de Linux y Unix. Además, durante la realización de la copia de un sistema de archivos a cinta, si detecta que se va a acabar la cinta, solicitará otra para continuar con el proceso.

Operaciones con dump/restore

La sintaxis general de la utilidad `dump` es:

```
dump opciones argumentos sistema_ficheros
```

Esta sintaxis, similar a la de otros comandos y utilidades, no se verifica en el resto de sistemas operativos Unix que no sean Linux. En el resto de Unix las opciones y argumentos irán agrupados y deberán coincidir en orden y número.

Por ejemplo, para hacer una copia de seguridad de la partición que contiene `/boot/`

```
[root@fedora root]# dump -f /tmp/dumpfile /boot/
DUMP: Date of this level 0 dump: Thu Dec 25 18:07:22 2003
DUMP: Dumping /dev/sda1 (/boot) to /tmp/dumpfile
DUMP: Added inode 8 to exclude list (journal inode)
DUMP: Added inode 7 to exclude list (resize inode)
DUMP: Label: /boot
DUMP: mapping (Pass I) [regular files]
DUMP: mapping (Pass II) [directories]
DUMP: estimated 5422 tape blocks.
DUMP: Volume 1 started with block 1 at: Thu Dec 25 18:07:23 2003
DUMP: dumping (Pass III) [directories]
DUMP: dumping (Pass IV) [regular files]
DUMP: Closing /tmp/dumpfile
DUMP: Volume 1 completed at: Thu Dec 25 18:07:24 2003
DUMP: Volume 1 5410 tape blocks (5.28MB)
DUMP: Volume 1 took 0:00:01
DUMP: Volume 1 transfer rate: 5410 kB/s
DUMP: 5410 tape blocks (5.28MB) on 1 volume(s)
DUMP: finished in 1 seconds, throughput 5410 kBytes/sec
DUMP: Date of this level 0 dump: Thu Dec 25 18:07:22 2003
DUMP: Date this dump completed: Thu Dec 25 18:07:24 2003
DUMP: Average transfer rate: 5410 kB/s
DUMP: DUMP IS DONE
```

Las opciones más utilizadas son las que se muestran en la siguiente tabla:

Opción	Acción realizada	Argumento
0-9	Nivel de la copia de seguridad	NO
u	Actualiza `/etc/dumpdates` al finalizar la copia	NO
f	Indica una cinta diferente de la usada por defecto	SI
b	Tamaño de bloque	SI
c	Indica que la cinta destino es un cartucho	NO
W	Ignora todas las opciones excepto el nivel de la copia	NO
a	Se escribirá hasta el final de la cinta en lugar de calcular el espacio	NO

La copia de seguridad puede realizarse tanto en un dispositivo de cinta (local o remoto) como en un fichero. Cuando la copia se realice a un dispositivo o fichero remoto será necesario indicarle también el nombre del servidor destino.

```
dump -f backuphost:/dev/rmt/0mn
```

El nombre del dispositivo de cinta remoto será el que tenga en el servidor remoto. Será necesario también que el servidor remoto permita el acceso por `rsh` sin necesidad de clave. Esto representa un agujero de seguridad bastante importante, por lo que se recomienda estudiar la conveniencia o no de usar este método para hacer copias remotas.

Para realizar la restauración de las copias realizadas con `dump` se utiliza la utilidad complementaria `restore`. La restauración puede realizarse de forma interactiva o no interactiva.

Restauración interactiva: Este tipo de restauraciones se utilizarán cuando sólo queremos restaurar ficheros sueltos. Será necesario utilizar la opción `-i` para realizar restauraciones de este tipo. Retomando el ejemplo anterior, donde realizamos una copia de seguridad del sistema de archivos `/boot`

```
[root@fedora root]# restore -if /tmp/dumpfile
restore > ls
.:
```

```
System.map              initrd-2.4.18-14.img    module-info-2.4.18-14
System.map-2.4.18-14    kernel.h                os2_d.b
boot.b                  lost+found/             vmlinux-2.4.18-14
chain.b                 message                 vmlinuz
config-2.4.18-14        message.ja              vmlinuz-2.4.18-14
grub/                   module-info
```

Dentro de este modo interactivo existen varios comandos:

```
restore > help
Available commands are:
ls [arg] - list directory
cd arg - change directory
pwd - print current directory
add [arg] - add 'arg' to list of files to be extracted
delete [arg] - delete 'arg' from list of files to be extracted
extract - extract requested files
setmodes - set modes of requested directories
quit - immediately exit program
what - list dump header information
verbose - toggle verbose flag (useful with ``ls'')
prompt - toggle the prompt display
help or '?' - print this list
If no 'arg' is supplied, the current directory is used
```

Restauración no interactiva: En este caso se restaurarán todos los ficheros

Como ya se ha comentado anteriormente, dentro de un mismo dispositivo se pueden tener varias copias de seguridad. Para acceder a una en concreto es necesario moverse de forma secuencial por la cinta. La utilidad que permite desplazarse por el dispositivo de cinta es `mt`. Esta utilidad tiene numerosas opciones y nos centraremos en las más utilizadas para el uso conjunto con `dump/restore`:

- Rebobinar la cinta

  ```
  mt -f tapedev rewind
  ```

- Moverse por la cinta

  ```
  mt -t tapedev fsf count
  ```

Así pues, en el caso que se disponga de una cinta con varias copias de seguridad realizadas con `dump`, si se quiere restaurar la que se encuentra en la segunda posición:

```
mt -f tapedev rewind
mt -t tapedev fsf 1
```

1.5. Sincronización de sistemas de ficheros

La utilidad `rsync` es una pequeña utilidad que nos permite realizar transferencias incrementales de ficheros, de esta forma sólo se copian las diferencias que se han producido entre los datos origen y destino. Estos datos pueden ser enviados comprimidos, y mediante `ssh` si queremos que viajen encriptados. Es condición indispensable que `rsync` se encuentre instalado en las dos máquinas que están involucradas en la transferencia de ficheros.

A modo de resumen, `rsync` basa su funcionamiento en los siguientes conceptos:

Diferencias. Únicamente se transfieren los ficheros que han cambiado en lugar de todos los ficheros y, de los que hayan cambiado, sólo las diferencias lo que hace que la transferencia sea mucho más rápida (conveniente en caso de tener enlaces de red lentos) a diferencia de `ftp` o `scp` que enviaría el archivo completo incluso si sólo cambia 1 byte.

Compresión. Las pequeñas partes de los ficheros que han cambiado se comprimen en el momento, con lo cual el tamaño de los datos a mandar es aún menor.

Encriptación. Es posible que los datos que han cambiado se envíen por la red a través de un canal seguro proporcionado con `ssh`, con lo cual evitamos que cualquier persona pueda capturarlos.

1.5.1. Trabajando con rsync

Básicamente, el funcionamiento es similar a las utilidades de copia remota `rcp` o `scp`. Ofrece grandes ventajas a la hora de realizar copias de seguridad o espejos de determinadas partes del sistema de ficheros de un servidor, especialmente en el caso de servidores web.

La utilidad `rsync` puede funcionar también en modo "`daemon`": a la escucha en un determinado puerto. Esta opción suele utilizarse para la distribución de ficheros en equipos de desarrollo de software. En nuestro caso nos centraremos en la ejecución de `rsync` en modo cliente ya que sacaremos más provecho.

La shell remota que utiliza `rsync` por defecto es `rsh`. En caso de querer cambiar a `ssh` (es lo más conveniente por los motivos de seguridad indicados) es necesario utilizar la opción `-e` en la llamada a `rsync` o establecer la variable de entorno `RSYNC_RSH` a `ssh`.

La mejor forma de comprender el funcionamiento de `rsync` es viendo el resultado de la ejecución de unos ejemplos. Utilizaremos un servidor web y se realizará una copia del directorio `/var/www/html` en `/home/hugo`:

```
[hugo@fedora www]$ rsync -av html /home/hugo/
building file list ... done
html/
html/usage/
html/usage/ctry_usage_200311.png
html/usage/daily_usage_200311.png
html/usage/hourly_usage_200311.png
html/usage/index.html
html/usage/msfree.png
html/usage/usage.png
html/usage/usage_200311.html
html/usage/webalizer.png
wrote 50357 bytes read 148 bytes 33670.00 bytes/sec
total size is 49757 speedup is 0.99
```

La opción `-v` (*verbose*) es conveniente utilizarla ya que informará de la evolución del proceso.

El comando anterior sería equivalente a:

```
cp -a html home/hugo/
```

Sin embargo el uso de `rsync` es mucho más eficiente por lo comentado previamente. El ejemplo anterior suponía que tanto el directorio fuente como el directorio destino estaban localizados localmente. En caso que se encuentren en distintas máquinas el formato general es:

```
rsync -a -e ssh fuente/ usuario@maquinaremota:/ruta/a/destino/
```

En este caso se supondrá que el directorio destino se encuentra en la máquina `maquinaremota`.

Consideremos que se está desarrollando el contenido del servidor web en nuestro ordenador personal con Linux (`hugo.midominio.org`). Una vez conformes con las modificaciones hechas a las páginas web es necesario pasarlas al servidor web para que las vea todo el mundo (`www.micentro.org`).

```
rsync -av -e ssh /home/hugo/html/ www.micentro.org:/home/httpd/html/
```

- Aunque realmente no estaría dentro de los conceptos referidos a la utilidad `rsync`, merece la pena detenernos un momento en ver las diferencias existentes entre poner `directorio/` o `directorio` (se ha utilizado de las dos formas en distintos ejemplos) ya que el resultado puede diferir en algunos casos. Normalmente estamos acostumbrados a que los comandos no prestan especial atención a las barras de *path*. Por ejemplo, si `a` y `b` son dos directorios, los siguientes comandos serían equivalentes:

  ```
  cp -a a b
  cp -a a/ b/
  ```

  Sin embargo en el caso de `rsync` estas barras al final de una ruta sí son importantes, pero únicamente en el caso del directorio fuente. De esta forma, si el directorio `a` contiene a su vez un subdirectorio llamado `temp` se obtienen los siguientes resultados:

  ```
  rsync -a a b ⟼ b/a/temp
  rsync -a a/ b ⟼ b/temp
  ```

  Como puede verse, el resultado no es el mismo, así que debe tenerse en cuenta este aspecto para poner o no la barra de *path* al final del directorio origen.

Otra opción muy interesante a la hora de realizar copias con la utilidad `rsync` es `--delete`. Continuemos con el ejemplo anterior y supongamos que un fichero que estaba en el directorio `html` ha sido borrado porque ya no era necesario. La copia existente en el directorio `html` del servidor destino debería ser igual que la del directorio del que tomó los datos. Esto se consigue borrando el fichero del servidor de destino mediante:

```
rsync -av --delete -e ssh /home/hugo/html/ www.micentro.org:/home/httpd/html
    /
receiving file list ... done
deleting html/index.html
html/
wrote 16 bytes  read 395 bytes  91.33 bytes/sec
total size is 94287  speedup is 229.41
```

Como puede verse, hay una referencia al fichero `index.html` que se ha borrado al haber sido borrado previamente del origen. Como con cualquier operación que implique borrado de ficheros se recomienda utilizar con cuidado esta opción, asegurándonos que realmente es eso lo que se desea.

Otra posibilidad que ofrece `rsync` a la hora de realizar transferencias selectivas de ficheros es la opción `--exclude` y `--exlude-from`. Con la primera de las opciones, se excluirán de la copia los ficheros que verifiquen el patrón, mientras que con la segunda opción los ficheros a excluir se obtendrán de un fichero auxiliar.

```
rsync -av --exclude '*.bak' /home/hugo/html/ www.centro.org:/home/httpd/html
    /
rsync -av --exclude-from excluir.txt /home/hugo/html/ www.micentro.org:/home
    /httpd/html/
```

1.5.2. Copias de seguridad con rsync

Ahora que ya se ha trabajado un poco con `rsync` se aplicará a la realización de copias de seguridad. Como ya se vió, `rsync` proporciona un mecanismo cómodo para realizar copias de seguridad tanto en local[2] como en una máquina remota.

[2]En este caso, lo recomendable es que se realice en un sistema de archivos y disco independiente

Usando `rsync` junto a la utilidad `cron` se puede planificar una copia de seguridad para que se realice todos los días.

```
00 22 * * * rsync -a --delete -e ssh fuente/ usuario@maquinaremota:/path/to/destino/
```

De esta forma, todos los días a las 22:00 se realizaría una copia de seguridad del directorio en cuestión, teniendo en cuenta que únicamente viajarán por la red los cambios existentes.

Sin embargo, si se produce el borrado accidental de un fichero y se realiza la copia de seguridad, este fichero se borrará en el directorio destino, con lo que sería imposible su recuperación. Surge así la necesidad de avanzar un poco más, como ya se ha hecho anteriormente con otras utilidades, a la hora de definir el esquema de copias de seguridad.

No debe olvidarse que es recomendable hacer una copia completa al menos una vez a la semana y el resto de días realizar copias incrementales.

1.6. Copias de seguridad en CDROM

Al comienzo de este capítulo se indicó que, debido al bajo precio tanto del dispositivo de grabación como del soporte, se está extendiendo el uso del CDROM para la realización de las copias de seguridad en determinados casos.

En este caso no se utilizarán las utilidades vistas hasta ahora, será necesario hacer uso de una utilidad diseñada específicamente para realizar escritura sobre soporte CDROM.

Se asumirá que el sistema operativo ha reconocido de forma correcta el dispositivo. A partir de este punto es necesario un software capaz de utilizar la unidad para escribir datos. Por un lado una utilidad para crear las imágenes ISO (`mkisofs`) y por otro la utilidad para realizar el proceso de grabación.

El proceso a seguir en la realización de las copias de seguridad será crear una imagen con los datos que se desea copiar y posteriormente grabar esta imagen en el CDROM.

Supongamos que vamos a hacer la copia de seguridad del directorio `/home`:

```
[hugo@fedora hugo]$ ls -l /home
total 8
drwx------ 20 hugo hugo 4096 dic 27 09:33 hugo
drwx------ 2 pepito pepito 4096 nov 8 11:21 pepito
[hugo@fedora home]$ mkisofs -R -l -o /mnt/imagen.iso /home/
mkisofs: Permission denied. Unable to open directory /home/pepito
mkisofs: Permission denied. Unable to open disc image file
```

Nuevamente aparece un problema de permisos ya que el usuario `hugo` está intentando acceder a un directorio `/home/pepito` en el que no tiene permiso de acceso. Lo mismo pasa con el fichero que va a almacenar la imagen ISO. Para evitar este tipo de problemas se realizarán las copias utilizando el usuario `root`.

```
[root@fedora root]# mkisofs -R -l -o /mnt/imagen.iso /home
54.56% done, estimate finish Sat Dec 27 09:40:51 2003
Total translation table size: 0
Total rockridge attributes bytes: 63340
Total directory bytes: 313344
Path table size(bytes): 2314
Max brk space used 5c544
9168 extents written (17 Mb)
```

No es necesario entrar en detalle de todas las opciones que puede utilizar `mkisofs`, únicamente van a describirse las que puedan ser más útiles[3]:

[3]Respecto a la columna **Opción** hay que aclarar que aunque en la documentación aparecen las opciones `-m` y `-x` como distintas, son equivalentes y se puede utilizar una u otra indistintamente

Opción	Acción realizada
`-f`	Sigue los enlaces simbólicos cuando se genera el sistema de ficheros
`-l`	Permite nombres de ficheros de 31 caracteres
`-L`	Permite nombres de ficheros que empiecen por .
`-m patrón`	Excluye los nombres de ficheros que concuerden con el parámetro
`--exclude-list fichero`	Excluye los nombres de ficheros que concuerden con los patrones de fichero
`-o fichero`	Nombre del fichero donde se va a almacenar la imagen ISO
`-R`	Se registra información sobre permisos y dueños de los archivos
`-v`	Muestra información detallada sobre la creación de la imagen ISO
`-x ruta`	Excluye los ficheros que coinciden con la ruta especificada

Se puede afinar un poco más la copia de seguridad y excluir ficheros o directorios que no quieran incluirse en las copias de seguridad:

```
# mkisofs -R -l -x *~ -x /home/*/.openoffice -o /mnt/imagen.iso /home
59.10% done, estimate finish Sat Dec 27 09:55:32 2003
Total translation table size: 0
Total rockridge attributes bytes: 53335
Total directory bytes: 260096
Path table size(bytes): 1938
Max brk space used 4e000
8464 extents written (16 Mb)
```

Antes de grabar la imagen a CDROM es recomendable comprobar su contenido:

```
# mount /mnt/imagen.iso -r -t iso9660 -o loop /mnt/home
# ls -l /mnt/home/
total 14
drwx------ 20 hugo hugo 8192 dic 27 09:39 hugo
drwx------ 2 pepito pepito 2048 nov 8 11:21 pepito
dr-xr-xr-x 18 root root 4096 dic 27 09:40 rr_moved
```

Una vez montada la imagen con la opción `-o loop` es posible operar sobre ella como cualquier sistema de archivos. Se podrá añadir, borrar o realizar modificaciones sobre los ficheros y, una vez desmontado, estas modificaciones se mantendrán en el archivo de imagen ISO.

En este punto ya se dispone de una imagen creada y lista para almacenar en CDROM. Entra en juego ahora la utilidad de cdrom para realizar la grabación de los datos.

k3b

Si bien, el modo comando permite trabajar de forma eficiente y eficaz, las utilidades gráficas de creación de imágenes ISO y de grabación nos pueden facilitar enormemente la vida a la hora de hacer lo comentado. Existen varias de funcionalidad similar pero nos pararemos sólo en una de las mejores y más usadas, se trata de `k3b`[4]. K3b, lo mismo que xcdroast, es un *front-end* para los programas de grabación de siempre (`cdrecord, cdrdao, mkisofs y cdparanoia`) pero incorpora además las utilidades `dvd+rw-tools` y `growisofs` para hacer copias de DVD. Su interfaz gráfica es muy amigable e intuitiva y se tienen a mano todas las herramientas de grabación.

[4]

- La página oficial del programa es `http://www.k3b.org`. Para instalarla

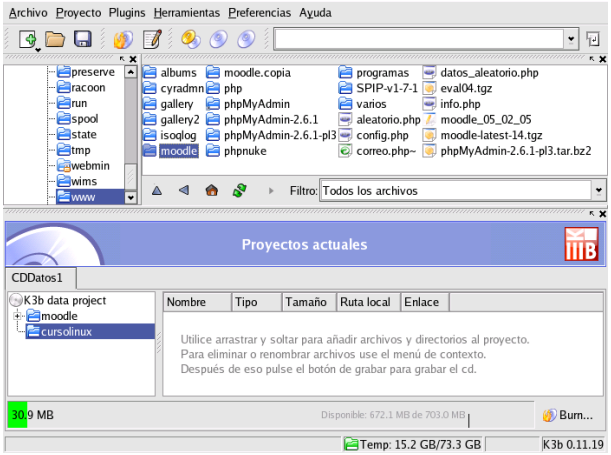
  ```
  #apt-get install k3b
  ```

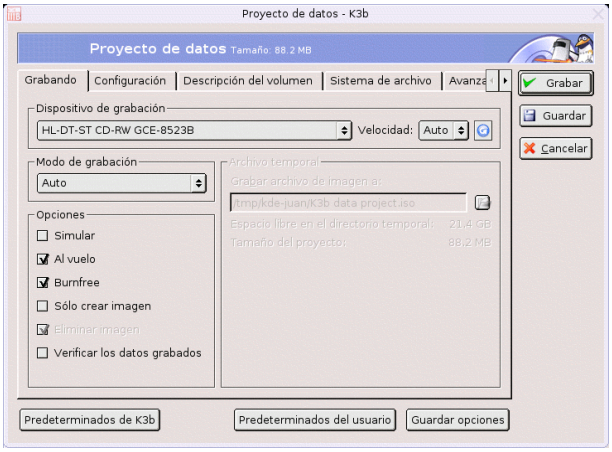
- Partiremos de que está instalada y configurada y sólo ejemplificaremos los aspectos que nos interesan respecto a copias de seguridad.

Figura 1.1: Inicio de k3b

Con ella podemos tanto crear la imagen `iso` de la zona de disco que deseemos como finalizar el proceso de grabación.

Ejecutemos k3b y seleccionemos **Archivo→Nuevo Proyecto → Nuevo proyecto de CD de Datos**[5]. Arrastremos las carpetas y ficheros que deseemos al panel del proyecto. Cuando hayamos elegido las que deseamos[6] pulsaremos sobre **Burn..** En la ventana ***Proyecto de datos*** accedemos a las pestañas de opciones de grabación: podemos copiar al vuelo, sólo crear imagen, iniciar multisesión, poner nombre al Cd, etc. Cuando esté todo a nuestro gusto, optaremos por [**Grabar**]. Si en ese momento no deseamos hacer la grabación podemos guardar el proyecto **Archivo→Guardar como...** darle nombre y grabarlo más tarde.





1.7. Solución integrada de copias de seguridad: AMANDA

Uno de los problemas con que se encuentran a menudo los administradores de grandes y pequeñas redes es la realización de copias de seguridad. Hacer que cada usuario haga copia de seguridad de sus propios archivos parece una solución obvia, pero es impracticable. Además, equipar a cada estación de trabajo y servidor de su propio hardware de copia de seguridad es muy caro.

[5] O DVD de datos.

[6] Si pulsamos con el botón derecho del ratón sobre un fichero, un menú emergente nos permitirá renombrar, borrar, crear carpeta, etc.

Podría enfocarse la solución a este problema desde un punto de vista centralizado, donde un único servidor, el servidor de *backup*, controla un proceso de copia por la red. Con este punto de vista, una vez configurado un cliente, no es necesaria la intervención del administrador y podría constituirse como solución válida.

AMANDA (*Advanced Maryland Automated Network Disk Archiver*) es una utilidad de dominio público desarrollada por la Universidad de Maryland que toma esta aproximación centralizada. AMANDA permite establecer un único servidor maestro para gestionar las copias de seguridad de múltiples nodos en una única unidad de cinta. Utiliza las utilidades `dump` y `tar`, pudiendo realizar las copias de seguridad de clientes Unix con distintas versiones de Sistema Operativo. Las versiones más recientes pueden también hacer copias de clientes Windows mediante SAMBA.

La idea surgió por la problemática existente con la introducción de los soportes de cinta de alta capacidad. En el caso de organizaciones con muchos servidores, no es rentable tener una unidad de cinta conectada a cada servidor para realizar las copias de seguridad. Con este sistema únicamente el servidor maestro tiene conectadas las unidades de cinta.

Aunque inicialmente se diseñó para trabajar con unidades de cinta, se realizarán unas modificaciones en la configuración para utilizar el disco duro como soporte final de las copias de seguridad. El precio que actualmente tienen los discos, así como la proliferación de los discos externos con conexión USB hace que se puedan considerar un serio aspirante a medio de almacenamiento de copia de seguridad.

El sistema de copias de seguridad que proporciona AMANDA permite hacer copias en un único soporte de varios ordenadores. Este sistema gestiona copias incrementales y completas, aunque normalmente sólo se hacen copias completas de pocos ordenadores en cada sesión de copias de seguridad.

1.7.1. Características de AMANDA

AMANDA está diseñado para manejar un gran número de clientes y datos, siendo aún así facil de instalar y configurar. Es fácilmente escalable, así que pequeñas configuraciones, de incluso un único nodo, son posibles. Su funcionamiento está sustentado por una serie de comandos que se encargan de diversas tareas relativas a la copia de seguridad. Las posibilidades de AMANDA son extraordinariamente amplias, limitándonos aquí a dar unos conceptos básicos que nos permitan dar los primeros pasos en su uso.

Trabaja sobre un protocolo propio encima de TCP y UDP. Cada cliente escribirá en la salida estándar, siendo AMANDA el encargado de recoger y transmitir dicha información al servidor maestro. Esto permitirá insertar compresión y encriptación así como la gestión de un catálogo con las imágenes creadas para su uso en la restauración. El cliente de red existente en el servidor de *backup* de AMANDA, contacta con los servidores AMANDA que se ejecutan en los clientes de los que se va a hacer copia de seguridad para iniciar la transferencia de datos. Para la restauración de los datos, AMANDA ejecuta varios servicios en el servidor de *backup* y un programa cliente (en el ordenador cliente del cual se quiere restaurar).

Múltiples clientes entran en el proceso de copia en paralelo al copiar por la red los datos a uno o varios discos, configurados en el servidor maestro para almacenar las imágenes de las copias. Posteriormente, el proceso de copia sobre el dispositivo de cinta toma como origen estos discos. AMANDA puede ejecutarse directamente sobre cinta sin utilizar este almacenamiento intermedio, pero se logrará un rendimiento peor.

Al utilizar software estándar para generar las imágenes, sólo las herramientas Unix como `mt`, `dd` y `gunzip` son necesarias para restaurar una copia desde cinta, si AMANDA no está disponible.

AMANDA utiliza una secuencia de cintas para las copias. Las cintas están numeradas con etiquetas que son leídas por los servidores. Así, AMANDA gestiona las cintas que son necesarias utilizar en cada sesión, evitando escribir en una cinta que no corresponda.

Este sistema realiza las copias basándose en el espacio en disco reservado por AMANDA en el servidor de cintas y que almacenará las copias hechas por la red. De esta manera, las copias de los servidores clientes se volcarán a disco mientras la unidad de cinta trabaja.

Una vez configurado, AMANDA necesita muy poca intervención por parte del administrador. Normalmente existirá una línea en el `cron` del sistema, que será el encargado de lanzar el proceso de copia. Los clientes que estén colgados o no estén disponibles en el momento de la copia son marcados e ignorados.

Cada mañana el administrador del sistema recibirá un informe con los detalles del proceso de copia de seguridad realizado durante la noche. Las primeras líneas son las más importantes, ya que indicarán si el proceso finalizó correctamente y se escribieron los archivos en la cinta correcta o si hubo algún fallo (pudo haberse realizado bien el proceso de volcado a disco pero fallar la copia a cinta). En el caso de fallo en el dispositivo de cinta, el sistema pasa a un estado degradado, donde las copias de seguridad se siguen realizando, pero únicamente a disco.

A continuación veremos una configuración básica de AMANDA que nos permita empezar a realizar copias de seguridad.

1.7.2. Instalación de AMANDA

La instalación de los distintos paquetes, así como de las dependencias que éstos presenten se realizará por el procedimiento habitual:

```
apt-get install amanda-common
apt-get install amanda-server
apt-get install amanda-client
```

La infraestructura que se describe a continuación se basa en un sistema Guadalinex que ejerce al mismo tiempo de servidor de cintas y de cliente de backup. No debe presentar dificultad ampliar este esquema mediante la configuración de nuevos clientes al sistema, según lo indicado en el apartado correspondiente.

1.7.3. Configuración de clientes

Los clientes de AMANDA ejecutan un servicio llamado `amandad`. Normalmente se ejecutará desde `inetd` o `xinetd`.

En Fedora, al trabajar con `xinetd` es necesario crear el fichero `/etc/xinetd.d/amanda`:

```
# default: off
# description: The client for the Amanda backup system.\
#              This must be on for systems being backed up\
#              by Amanda.
service amanda
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = backup
        group                   = backup
        server                  = /usr/lib/amanda/amandad
        disable                 = no
}
```

Por supuesto, dependiendo de la instalación de AMANDA, puede ser necesario cambiar la ruta donde se encuentra el programa servidor.

Es recomendable modificar también el fichero `/etc/services` para que refleje el nuevo servicio, en caso de no estar definido:

```
amanda          10080/tcp         # amanda backup services
amanda          10080/udp         # amanda backup services
```

También es necesario comprobar que haya una cuenta de sistema para AMANDA. Normalmente, el nombre de usuario de esta cuenta será `amanda`, aunque en el caso de Guadalinex la cuenta que se crea en la instalación y que se utilizará es `backup`. Si se va a utilizar otra cuenta distinta de `backup` pueden producirse problemas referentes a permisos con los ficheros y directorios que utiliza AMANDA. El directorio `$HOME` de este usuario deberá contener un fichero de autenticación llamado `.amandahost,` que en realidad es un enlace simbólico al fichero `/etc/amandahost`. Contendrá el nombre del servidor de *backup* y el usuario con el que este servidor accederá al servicio que tenemos ejecutándose en el cliente de *backup*. Proporciona un control de acceso sin el cual AMANDA no podrá realizar la copia de seguridad. Teniendo en cuenta que el servidor tiene como nombre de host `guadalinex` y que el usuario que se utiliza es `backup`, el contenido de este fichero será:

```
guadalinex backup
```

Una vez configurado el cliente con las indicaciones que acabamos de dar, es preciso reiniciar `inetd` o `xinetd` para que los cambios tomen efecto. Este proceso es necesario repetirlo en cada uno de los clientes que se desee salvaguardar con AMANDA.

1.7.4. Configuración del servidor de cintas

Lo primero que hay que decidir, una vez instalado AMANDA, es qué máquina será el servidor de cintas. Necesitará tener acceso directo al dispositivo de cintas y un espacio en disco lo suficientemente grande para almacenar las imágenes. En el caso que nos ocupa no se accederá a ningún dispositivo de cintas ya que éstas se simularán sobre el espacio en disco.

La máquina que ejerza de servidor de *backup* no es necesario que ejecute ningún servicio para realizar las operaciones de copia de seguridad. Únicamente necesita ejecutar servicios para la gestión de restauraciones iniciadas desde los clientes. Al igual que en el caso de los clientes, estos servicios se gestionarán desde `inetd` o `xinetd`. En el caso de `xinetd` son necesarios los ficheros `/etc/xinetd.d/amandaidx`:

```
# default: off
#
# description: Part of the Amanda server package
service amandaidx
{
        socket_type             = stream
        protocol                = tcp
        wait                    = no
        user                    = backup
        group                   = backup
        server                  = /usr/lib/amanda/amindexd
        disable                 = no
}
```

Y el fichero `/etc/xinetd.d/amidxtape`:

```
# default: off
#
# description: Part of the amanda server package
#
service amidxtape
{
        socket_type             = stream
        protocol                = tcp
        wait                    = no
        user                    = backup
        group                   = backup
        server                  = /usr/lib/amanda/amidxtaped
```

```
        disable                 = no
}
```

Las correspondientes entradas en `/etc/services` serán:

```
amandaidx       10082/tcp               # amanda backup services
amidxtape       10083/tcp               # amanda backup services
```

La configuración para gestionar las copias de seguridad se define en `amanda.conf`. Este fichero se encuentra localizado en un subdirectorio que indica el nombre de la copia de seguridad dentro de `/etc/amanda`. Por ejemplo, si se define una política de copias de seguridad que se llama `Daily`, el fichero de configuración debería estar en `/etc/amanda/Daily/amanda.conf`. Este subdirectorio debe tener permisos de escritura para el usuario `backup`.

Algunos de los parámetros de configuración de este fichero son:

`dumpuser` Especifica el nombre de usuario con el que se ejecutarán las operaciones de copia de seguridad.

`dumpcycle` Define el tiempo que AMANDA toma para realizar un *backup* completo del sistema.

`runspercycle` Es el número de veces que `amdump` se ejecuta en cada ciclo.

`tapecycle` Es el número de cintas que van a ser usuadas en un único ciclo de carga. Este número suele ser mayor que `runspercycle` por si hay cintas dañadas.

`runtapes` Es el número de cintas que se usan en cada ejecución de `amdump`. Normalmente es 1 si no hay cargador de cintas.

`tapedev` Es el dispositivo de cinta sin rebobinado, por ejemplo `/dev/nst0` o `/dev/nht0`.

`tapetype` Es el tipo de dispositivo de cinta.

`labelstr` Establece la etiqueta para las cintas.

`holdingdisk` Establece información sobre el espacio en disco reservado para las copias de seguridad.

La parte más complicada de la configuración es establecer el ciclo de copia. Los parámetros de esta categoría interaccionan para definir el número de cintas requeridas para cada ciclo y el número de cintas disponibles en total. Los parámetros `dumpcycle`, `runspercycle` y `tapecycle` se definen de forma que se hace una copia de cada sistema de ficheros al menos una vez por `dumpcycle` y el número de cintas en `tapecycle` debe ser más grande que `runspercycle * runtapes`. Al estar establecido `runtapes` a 1, si no tenemos un cargador de cintas, el valor de `tapecycle` dependerá únicamente de `runspercycle`.

Otros ficheros que podemos encontrar dentro de este directorio `/etc/amanda/Daily` son[7]:

`disklist` Es un fichero que puede editarse, contiene la combinación de servidor/disco para las copias de seguridad con el formato `hostname diskdev dumptype [spindle [interface]]`

`tapelist` No es editable, contiene el nombre, estado y fecha de último uso para todas las cintas de la configuración.

`tapelist.amlabel` No editable, contiene el estado original de las cintas cuando fueron etiquetadas.

[7] Algunos de estos ficheros no estarán disponibles hasta que no se haya realizado la configuración completa o se haya realizado algún backup. En caso de no encontrarlos en el sistema completar el proceso de configuración y volver a comprobarlos.

`tapelist.yesterday` No editable, contiene el nombre, estado y fecha de último uso (desde la última ejecución de AMANDA) para todas las cintas definidas en la configuración.

Los ficheros `tapelist.*` son gestionados por las utilidades `amdump` y `amlabel` y se crearán conforme se utilice AMANDA. No deben editarse de forma manual.

El fichero de configuración que se muestra a continuación facilitará bastante la comprensión de los conceptos anteriores. También hay que tener en cuenta que AMANDA está diseñado para realizar copias de seguridad sobre dispositivos de cinta. Se efectuarán unas modificaciones en la definición de los dispositivos de cinta que proporciona AMANDA por defecto para utilizar el disco duro local. Así no será necesario comprar ningún dispositivo de cinta y el uso del sistema se basará en escritura sobre cintas virtuales que están definidas sobre espacio en disco.

El fichero `/etc/amanda/Daily/amanda.conf` quedaría como sigue:

```
#
org "Daily"                # Nombre descriptivo para los mensajes
mailto "amanda"            # lista de mails que reciben los logs
dumpuser "backup"          # usuario propietario de los backups
inparallel 1               # procesos en paralelo
netusage  10               # ancho de banda máximo
dumpcycle 14 days          # numero de dias de un ciclo completo
tapecycle 14               # numero total de cintas
runtapes  1                #
tpchanger "chg-multi"      # script controlador de cintas
changerfile "/etc/amanda/Daily/changer.conf" # configuración de las cintas
tapetype HARD-DISK                 # tipo de almacenamiento
labelstr "^HISS[0-9][0-9]*$"       # expresion regular de la etiqueta de las
    cintas
infofile "/var/lib/amanda/Daily/curinfo"    # fichero de datos
logfile  "/var/log/amanda/Daily/log"        # fichero de log
indexdir "/var/lib/amanda/Daily/index"  # fichero de indice
# definición del almacenamiento
define tapetype HARD-DISK {
        comment "Esto es un disco duro, no una cinta"
        length 4000 mbytes  # 4 GB de espacio
}
# definición de volcado de datos completo
define dumptype hard-disk-dump {
        comment "Backup en disco en lugar de cinta - usando dump"
        holdingdisk no
        index yes
        options compress-fast, index, exclude-list "/etc/amanda/exclude.gtar
            "
        priority high
}
# definición de volcado de datos con 'tar'
define dumptype hard-disk-tar {
        program "GNUTAR"
        hard-disk-dump
        comment "Backup en disco en lugar de cinta - usando tar"
}
```

En la configuración anterior hemos hecho referencia al fichero `/etc/amanda/Daily/changer.conf`, encargado de la configuración de las cintas. En la configuración que nos atañe, definirá la localización del espacio en disco correspondiente a cada cinta virtual.

```
multieject 0
gravity 0
needeject 0
```

```
ejectdelay 0
statefile /var/lib/amanda/Daily/changer-status
firstslot 1
lastslot 14
slot 1 file:/backups/tape01
slot 2 file:/backups/tape02
slot 3 file:/backups/tape03
slot 4 file:/backups/tape04
slot 5 file:/backups/tape05
slot 6 file:/backups/tape06
slot 7 file:/backups/tape07
slot 8 file:/backups/tape08
slot 9 file:/backups/tape09
slot 10 file:/backups/tape10
slot 11 file:/backups/tape11
slot 12 file:/backups/tape12
slot 13 file:/backups/tape13
slot 14 file:/backups/tape14
```

Se define cada cinta virtual como un directorio dentro de `/backups/`, siendo el número de cintas de las que disponemos 14. A efectos prácticos AMANDA no notará la diferencia.

Ya estaría configurado AMANDA, pero no hay que olvidarse de crear los directorios en los que se mapean las cintas virtuales. Lo primero será crear los directorios que simularán las cintas.

```
root@guadalinex:~# mkdir /backups
root@guadalinex:~# mkdir -p /backups/tape01/data
root@guadalinex:~# mkdir -p /backups/tape02/data
[...]
root@guadalinex:~# mkdir -p /backups/tape14/data
root@guadalinex:~# chown -R backup:backup /backups
```

Cuando se crea un conjunto o *pool* de cintas es necesario etiquetarlas para que AMANDA pueda referenciarlas de forma unívoca. Las cintas se etiquetan con el comando `amlabel` y la etiqueta deberá seguir la expresión regular definida en `amanda.conf`. Todas las cintas definidas en `tapecycle` deben ser etiquetadas con objeto de estar disponibles en la fase de testeo. El comando `amlabel` graba cada cinta etiquetada en `tapelist` de forma que los otros programas de AMANDA pueden identificarlas. Es necesario crear el fichero vacío `/etc/amanda/Daily/tapelist` mediante el comando `touch` y posteriormente ejecutar `amlabel` para etiquetar cada una de las cintas:

```
-bash-2.05b$ /usr/sbin/amlabel Daily HISS01 slot 1
backup@guadalinex:/etc/amanda/Daily$ /usr/sbin/amlabel Daily HISS01 slot 1
labeling tape in slot 1 (file:/backups/tape01):
rewinding, reading label, not an amanda tape
rewinding, writing label HISS01, checking label, done.
-bash-2.05b$ /usr/sbin/amlabel Daily HISS02 slot 2
[...]
-bash-2.05b$ /usr/sbin/amlabel Daily HISS14 slot 14
```

Por último, se definen los clientes con los ficheros de los que se va a realizar la copia de seguridad en `/etc/amanda/Daily/disklist`. En este ejemplo únicamente definimos un cliente:

```
# El nombre de la máquina debe ser el que aparezca en el DNS o /etc/hosts
guadalinex.midominio.org     /home/hugo/CICA/ed05     hard-disk-tar
```

1.7.5. Salvaguarda de datos con AMANDA

Ya parece que está preparado el sistema para realizar copias de seguridad, pero es conveniente realizar un chequeo previo con `amcheck`. No hay que preocuparse si la salida no es exactamente igual a la que se muestra a continuación. Lo realmente importante es que no aparezca ningún mensaje de error[8].

```
backup@guadalinex:/etc/amanda/Daily$ /usr/sbin/amcheck Daily
Amanda Tape Server Host Check
-----------------------------------
ERROR: log dir /var/log/amanda/Daily: not writable
amcheck-server: slot 14: date X        label HISS14 (new tape)
NOTE: skipping tape-writable test
Tape HISS14 label ok
NOTE: info dir /var/lib/amanda/Daily/curinfo: does not exist
NOTE: it will be created on the next run
NOTE: index dir /var/lib/amanda/Daily/index/guadalinex.midominio.org: does
    not exist
Server check took 1.164 seconds
Amanda Backup Client Hosts Check
--------------------------------
ERROR: guadalinex.midominio.org: [Can't open exclude file '/etc/amanda/
    exclude.gtar': No such file or directory]
Client check: 1 host checked in 0.382 seconds, 1 problem found
(brought to you by Amanda 2.4.4p3)
```

El error aparecido sobre permisos del directorio que almacena los logs es facilmente solucionable. Se crea el directorio en cuestión y se le asigna como dueño al usuario `backup` y al grupo `backup`. El segundo error hace referencia al fichero `/etc/amanda/exclude.gtar`, que no ha sido creado aún. Basta con ejecutar `touch /etc/amanda/exclude.gtar` para crearlo.

Una vez realizadas estas modificaciones se ejecuta de nuevo `amcheck` para comprobar que no aparecen más errores.

```
backup@guadalinex:/etc/amanda/Daily$ /usr/sbin/amcheck Daily
Amanda Tape Server Host Check
-----------------------------------
amcheck-server: slot 14: date X        label HISS14 (new tape)
NOTE: skipping tape-writable test
Tape HISS14 label ok
NOTE: info dir /var/lib/amanda/Daily/curinfo: does not exist
NOTE: it will be created on the next run
NOTE: index dir /var/lib/amanda/Daily/index/guadalinex.midominio.org: does
    not exist
Server check took 0.858 seconds
Amanda Backup Client Hosts Check
--------------------------------
Client check: 1 host checked in 10.272 seconds, 0 problems found
(brought to you by Amanda 2.4.4p3)
```

Al no existir errores puede ejecutarse la primera copia de seguridad. Para eso se utiliza el comando `amdump`. Es necesario indicarle el esquema de copia de seguridad que se desea ejecutar.

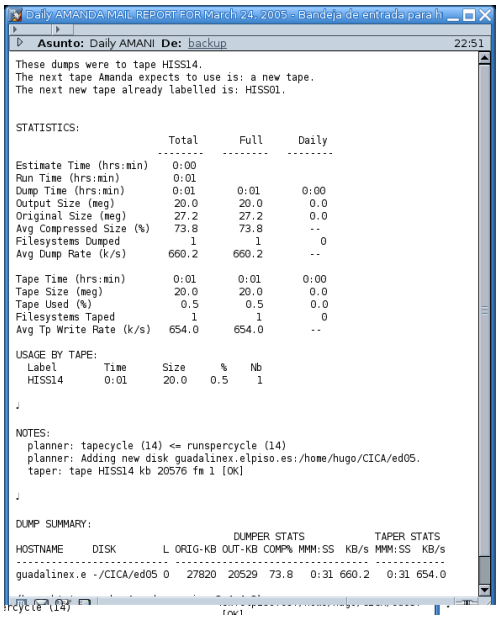
```
backup@guadalinex:/etc/amanda/Daily$ /usr/sbin/amdump Daily
```

Hasta ahora la ejecución de todos los comandos de AMANDA se ha realizado con el usuario `backup`. Esto es importante y no debe olvidarse a la hora de ejecutar estos comandos desde cualquier script auxiliar que se utilice.

[8] Mirando las páginas del manual se comprueba que `amcheck` puede mandar este informe por correo en lugar de mostrarlo por pantalla.

En la configuración que se definió en `amanda.conf` se indicó el destinatario de los informes que genera AMANDA al finalizar una copia de seguridad.

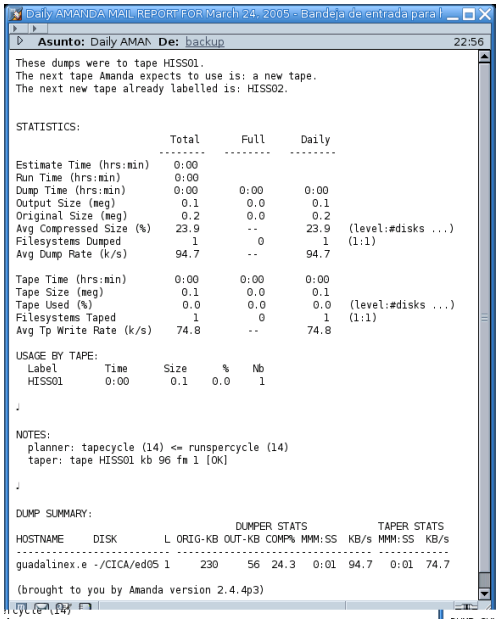
Figura 1.2: Informe de copia de seguridad sin errores de AMANDA



```
Daily AMANDA MAIL REPORT FOR March 24, 2005 - Bandeja de entrada para h
Asunto: Daily AMANI De: backup                                    22:51

These dumps were to tape HISS14.
The next tape Amanda expects to use is: a new tape.
The next new tape already labelled is: HISS01.


STATISTICS:
                          Total       Full      Daily
                        --------   --------   --------
Estimate Time (hrs:min)    0:00
Run Time (hrs:min)         0:01
Dump Time (hrs:min)        0:01       0:01       0:00
Output Size (meg)          20.0       20.0        0.0
Original Size (meg)        27.2       27.2        0.0
Avg Compressed Size (%)    73.8       73.8         --
Filesystems Dumped            1          1          0
Avg Dump Rate (k/s)       660.2      660.2         --

Tape Time (hrs:min)        0:01       0:01       0:00
Tape Size (meg)            20.0       20.0        0.0
Tape Used (%)               0.5        0.5        0.0
Filesystems Taped             1          1          0
Avg Tp Write Rate (k/s)   654.0      654.0         --

USAGE BY TAPE:
  Label        Time      Size      %    Nb
  HISS14       0:01      20.0    0.5     1


NOTES:
  planner: tapecycle (14) <= runspercycle (14)
  planner: Adding new disk guadalinex.elpiso.es:/home/hugo/CICA/ed05.
  taper: tape HISS14 kb 20576 fm 1 [OK]


DUMP SUMMARY:
                                       DUMPER STATS            TAPER STATS
HOSTNAME     DISK        L ORIG-KB OUT-KB COMP% MMM:SS  KB/s MMM:SS  KB/s
-------------------------- ---------------------------------- ------------
guadalinex.e -/CICA/ed05 0   27820  20529  73.8   0:31 660.2   0:31 654.0
```

El informe de esta primera copia de seguridad es bastante completo y permite conocer todos los aspectos del proceso. Si a continuación se lanza de nuevo la copia de seguridad el informe obtenido es distinto.

Figura 1.3: Informe de copia de seguridad de AMANDA



```
Daily AMANDA MAIL REPORT FOR March 24, 2005 - Bandeja de entrada para l
Asunto: Daily AMAN De: backup                                     22:56

These dumps were to tape HISS01.
The next tape Amanda expects to use is: a new tape.
The next new tape already labelled is: HISS02.


STATISTICS:
                          Total       Full      Daily
                        --------   --------   --------
Estimate Time (hrs:min)    0:00
Run Time (hrs:min)         0:00
Dump Time (hrs:min)        0:00       0:00       0:00
Output Size (meg)           0.1        0.0        0.1
Original Size (meg)         0.2        0.0        0.2
Avg Compressed Size (%)    23.9         --       23.9   (level:#disks ...)
Filesystems Dumped            1          0          1   (1:1)
Avg Dump Rate (k/s)        94.7         --       94.7

Tape Time (hrs:min)        0:00       0:00       0:00
Tape Size (meg)             0.1        0.0        0.1
Tape Used (%)               0.0        0.0        0.0   (level:#disks ...)
Filesystems Taped             1          0          1   (1:1)
Avg Tp Write Rate (k/s)    74.8         --       74.8

USAGE BY TAPE:
  Label        Time      Size      %    Nb
  HISS01       0:00       0.1    0.0     1


NOTES:
  planner: tapecycle (14) <= runspercycle (14)
  taper: tape HISS01 kb 96 fm 1 [OK]


DUMP SUMMARY:
                                       DUMPER STATS            TAPER STATS
HOSTNAME     DISK        L ORIG-KB OUT-KB COMP% MMM:SS  KB/s MMM:SS  KB/s
-------------------------- ---------------------------------- ------------
guadalinex.e -/CICA/ed05 1     230     56  24.3   0:01  94.7   0:01  74.7

(brought to you by Amanda version 2.4.4p3)
```

Puede comprobarse que en este caso se ha cambiado de cinta y que el volumen de datos copiados ha sido menor. Efectivamente, el esquema definido está funcionando tal como se desea y se produce el cambio de cinta en esta segunda copia, en la que unicamente se copian los datos que han sido modificados.

Ya puede añadirse la línea anterior al cron del sistema para que se ejecute la copia de seguridad a la hora que establezcamos, preferentemente por la noche, para no interferir con otros procesos.

1.7.6. Recuperación de datos con AMANDA

Según los informes anteriores, se ha realizado la primera copia de seguridad con éxito. Sin embargo, todos los sistemas de copia de seguridad tienen que ser comprobados de forma periódica en lo referente a la restauración.

AMANDA proporciona el comando `amrecover` para la restauración de los datos de una salvaguarda. Al ejecutar `amrecover` se obtiene una sesión interactiva en la que especificando una fecha, un servidor y un disco podemos caminar por los archivos disponibles para restaurar. A diferencia de los anteriores, este comando debe ser ejecutado con el usuario `root` para poder acceder a cualquier archivo del sistema. Será necesario entonces modificar el fichero `.amandahosts` para permitir que el usuario `root` pueda acceder a los datos de AMANDA.

```
backup@guadalinex:~$ more /etc/amandahosts
guadalinex backup
localhost root
```

Con esta configuración del fichero `/etc/amandahosts` se puede iniciar la ejecución del comando `amrecover`:

```
root@guadalinex:~# /usr/sbin/amrecover Daily
AMRECOVER Version 2.4.4p3. Contacting server on localhost ...
220 guadalinex AMANDA index server (2.4.4p3) ready.
200 Access OK
Setting restore date to today (2005-03-25)
200 Working date set to 2005-03-25.
200 Config set to Daily.
501 Host guadalinex is not in your disklist.
Trying host guadalinex ...
501 Host guadalinex is not in your disklist.
Trying host guadalinex.elpiso.es ...
200 Dump host set to guadalinex.midominio.org.
Trying disk / ...
Trying disk rootfs ...
Can't determine disk and mount point from $CWD '/root'
amrecover> setdisk /home/hugo/CICA
501 Disk guadalinex.midominio.org:/home/hugo/CICA is not in your disklist.
amrecover> setdisk /home/hugo/CICA/ed05
200 Disk set to /home/hugo/CICA/ed05.
amrecover> history
200- Dump history for config "Daily" host "guadalinex.midominio.org" disk "/
    home/hugo/CICA/ed05"
201- 2005-03-24 0 HISS14 1
201- 2005-03-24 1 HISS01 1
201- 2005-03-24 1 HISS02 1
200 Dump history for config "Daily" host "guadalinex.midominio.org" disk "/
    home/hugo/CICA/ed05"
amrecover> cd /home/hugo/CICA/ed05/tema5
/home/hugo/CICA/ed05/tema5
amrecover> ls
2005-03-24 .
```

```
2005-03-24 Daily/
2005-03-24 entrega5.lyx
2005-03-24 entrega5.lyx~
2005-03-24 images/
2005-03-24 paquetes_amanda.txt
amrecover> add entrega5.lyx
Added /tema5/entrega5.lyx
amrecover> add paquetes_amanda.txt
Added /tema5/paquetes_amanda.txt
amrecover> list
TAPE HISS14 LEVEL 0 DATE 2005-03-24
        /tema5/paquetes_amanda.txt
        /tema5/entrega5.lyx
amrecover> lpwd
/root
amrecover> lcd /tmp
amrecover> settape file:/backups/tape14
Using tape "file:/backups/tape14" from server localhost.
amrecover> extract
Extracting files using tape drive file:/backups/tape14 on host localhost.
The following tapes are needed: HISS14
Restoring files into directory /tmp
Continue [?/Y/n]? Y
Extracting files using tape drive file:/backups/tape14 on host localhost.
Load tape HISS14 now
Continue [?/Y/n/s/t]? Y
./tema5/entrega5.lyx
tar: ./tema5/entrega5.lyx: implausibly old time stamp 1970-01-01 01:00:00
./tema5/paquetes_amanda.txt
tar: ./tema5/paquetes_amanda.txt: implausibly old time stamp 1970-01-01
    01:00:00
amrecover>
```

Ya se habrían recuperado los archivos `entrega5.lyx` y `paquetes_amanda.txt` en `/tmp/tema5`. No parece que sea difícil ¿verdad? De todas formas se van a repasar más detenidamente los pasos seguidos en la recuperación.

Una vez en la consola interactiva de `amrecover` el primer comando que se utiliza es:

```
amrecover> setdisk /home/hugo/CICA
501 Disk guadalinex.elpiso.es:/home/hugo/CICA is not in your disklist.
amrecover> setdisk /home/hugo/CICA/ed05
```

El comando `setdisk` especifica el disco que vamos a considerar para navegar por los archivos salvados. El error `501` que se produce es debido a que en la copia de seguridad se ha guardado `/home/hugo/CICA/ed05` por lo que no encuentra la ruta `/home/hugo/CICA`. A continuación se muestra el histórico de copias de seguridad para ese directorio:

```
amrecover> history
```

Ya se puede navegar por las imágenes almacenadas con objeto de recuperar los archivos. Los archivos a recuperar se guardan en una lista hasta que demos la orden de recuperar.

```
amrecover> cd /home/hugo/MisDocumentos
amrecover> add entrega1.lyx
amrecover> add mailscanner.lyx
```

Para ver el contenido de la lista que se está creando con los archivos a recuperar:

```
amrecover> list
```

Antes de recuperar los archivos deseados es necesario definir en qué lugar se van a recuperar. Primero se comprueba en qué directorio se recuperan por defecto, para posteriormente cambiarlo a `/tmp`. Los ficheros se recuperarán con los mismos permisos y dueño que tenían originalmente, ésta es la razón por la que hay que ejecutar `amrecover` desde el usuario `root`.

```
amrecover> lpwd
amrecover> lcd /tmp
```

A continuación se define dónde está montada la cinta que contiene las imágenes que se van a utilizar.

```
amrecover> settape file:/backups/tape14
```

Y por último se da la orden de recuperar los archivos.

```
amrecover> extract
```

El error que aparece referente a la fecha es debido a un bug en la utilidad `tar`. Los ficheros recuperados pueden verificarse en la localización que se indicó `/tmp/tema5`.

La utilidad `amrecover` ofrece más opciones de las que se han utilizado en el ejemplo anterior.

```
amrecover> help
valid commands are:
add path1 ...      - add to extraction list (shell wildcards)
addx path1 ...     - add to extraction list (regular expressions)
cd directory       - change cwd on virtual file system (shell wildcards)
cdx directory      - change cwd on virtual file system (regular expressions)
clear              - clear extraction list
delete path1 ...   - delete from extraction list (shell wildcards)
deletex path1 ...  - delete from extraction list (regular expressions)
extract            - extract selected files from tapes
exit
help
history            - show dump history of disk
list [filename]    - show extraction list, optionally writing to file
lcd directory      - change cwd on local file system
ls                 - list directory on virtual file system
lpwd               - show cwd on local file system
mode               - show the method used to extract SMB shares
pwd                - show cwd on virtual file system
quit
listdisk [diskdevice] - list disks
setdate {YYYY-MM-DD|--MM-DD|---DD} - set date of look
setdisk diskname [mountpoint] - select disk on dump host
sethost host       - select dump host
settape [host:][device|default] - select tape server and/or device
setmode smb|tar    - select the method used to extract SMB shares
```

Como puede verse, la potencia de AMANDA a la hora de realizar copias de seguridad viene acompañada de la misma potencia en lo referente a recuperaciones. A pesar de todo no se han descrito todas las posibilidades de AMANDA, limitándose este apartado a las nociones básicas que permiten poner en marcha un sistema de backup/recuperación lo suficientemente estable como para dar tranquilidad al administrador de sistemas.

Capítulo 2

Logs del sistema

"Se debe confiar, pero también verificar"

2.1. Archivos de bitácora

Tan importante como establecer unos mecanismos de seguridad adecuados, es vigilar el sistema. El proceso de vigilar cómo se comporta el sistema se denomina *auditar*.

Los sistemas UNIX en general y Linux en particular, mantienen una serie de archivos de bitácora o logs de sistema que ayudan al administrador del mismo en las funciones de auditoría. Los archivos de log son bloques importantes para construir sistemas seguros, ya que muestran el pasado del sistema así como ayudan a la localización de errores intermitentes o ataques maliciosos.

Sin embargo, los archivos de log tienen un punto negativo muy importante: se encuentran situados en el propio sistema. De esta forma si se pierde el acceso al sistema por error grave, se perderá el acceso a estos archivos, con lo que pierden toda su utilidad.

Para solucionar esto, se pueden llevar los archivos de log a otro sistema, no siendo necesario que tenga la misma potencia que el sistema principal. Este sistema secundario tiene una única función, la de almacenar los archivos de bitácora, por lo que los requerimientos de software y hardware serán mínimos. Es importante también restringir al máximo el acceso a este sistema secundario para evitar que se pierdan los archivos de bitácora, ya sea de forma accidental o provocada.

Otra opción, muy recomendable, es tener en cuenta los archivos de bitácora en las políticas de copia de seguridad. De esta forma podremos recuperar siempre los archivos que hayan sido eliminados y acceder de esta forma a la historia del sistema.

2.2. Archivos de log existentes en el sistema

Por defecto, los archivos de bitácora se encuentran en el directorio `/var/log` del sistema de archivos de Linux. Veamos qué tiene ese directorio en el sistema que estamos utilizando[1]:

```
-rw-r-----   1 root    root       540 2005-03-25 09:14 acpid
drwxrwx---   4 backup  backup    4096 2005-03-24 21:49 amanda
drwxr-xr-x   2 root    root      4096 2005-02-15 18:34 apache
-rw-r-----   1 root    adm      25410 2005-03-25 17:09 auth.log
-rw-rw-r--   1 root    utmp         0 2005-03-20 06:28 btmp
drwxr-xr-x   2 root    root      4096 2005-03-25 16:30 cups
-rw-r-----   1 root    adm     607991 2005-03-25 17:09 debug
-rw-r--r--   1 root    root     10034 2005-03-25 09:14 dmesg
-rw-r--r--   1 root    root       118 2005-01-02 23:29 fontconfig.log
```

[1] Hay que tener en cuenta que este listado puede tener más o menos archivos, dependiendo de las aplicaciones que estén instaladas y que utilicen este directorio para almacenar sus logs.

```
drwxr-xr-x  2 root    root     4096 2005-03-25 09:15 gdm
-rw-r-----  1 root    adm     76839 2005-03-25 09:15 kern.log
-rw-rw-r--  1 root    utmp   584876 2005-03-25 09:17 lastlog
-rw-r-----  1 root    adm       308 2005-03-25 00:40 lpr.log
-rw-r-----  1 root    adm         0 2005-03-20 06:47 mail.err
-rw-r-----  1 root    adm     41539 2005-03-25 17:00 mail.info
-rw-r-----  1 root    adm     42397 2005-03-25 17:00 mail.log
-rw-r-----  1 root    adm         0 2005-03-20 06:47 mail.warn
-rw-r-----  1 root    adm     97629 2005-03-25 17:00 messages
drwxr-xr-x  4 nagios  nagios  4096 2005-03-24 00:00 nagios
drwxr-xr-x  2 root    root    4096 2004-05-03 16:27 news
drwxr-xr-x  2 root    root    4096 2005-03-25 09:18 ntpstats
drwxr-x---  2 root    adm     4096 2005-03-20 06:28 samba
-rw-r--r--  1 root    root       0 2005-03-20 06:28 scrollkeeper.log
drwxr-x---  2 proxy   proxy   4096 2005-02-15 14:18 squid
-rw-r-----  1 root    adm    808262 2005-03-25 17:09 syslog
-rw-r-----  1 root    adm     22824 2005-03-25 17:00 user.log
-rw-r--r--  1 root    root       0 2004-09-22 16:26 uucp.log
-rw-rw-r--  1 root    utmp   57600 2005-03-25 09:31 wtmp
-rw-rw-r--  1 root    utmp  108288 2005-03-20 06:07 wtmp.1
-rw-r--r--  1 root    root   61691 2005-03-25 16:21 XFree86.0.log
```

Los subdirectorios que se encuentran dentro de `/var/log` van a almacenar archivos de bitácora específicos de otras aplicaciones. Tal es el caso de los directorios `/var/log/apache` y `/var/log/samba` que almacenarán, respectivamente, los archivos de bitácora del servidor web apache y de la utilidad de compartición de ficheros samba.

A continuación se describe brevemente el objetivo de algunos de los archivos de log que se encuentran en un sistema Linux.

`/var/log/cron.log` Mensajes que aparecen relativos al funcionamiento del `cron`.

`/var/log/daemon.log` Mensajes que aparecen relativos al funcionamiento de los demonios del sistema.

`/var/log/dmesg` Mensajes que aparecen durante el arranque del sistema.

`/var/log/mail.*` Mensajes relativos al demonio de correo, en distintos ficheros según su severidad.

`/var/log/messages` Mensajes genéricos del sistema incluyendo los generados en el arranque.

`/var/log/lastlog` Información de últimos accesos de los distintos usuarios al sistema.

`/var/log/utmp` Información acerca de quiénes están usando el sistema actualmente. Puede haber más usuarios de los que muestre este fichero, ya que no todos los programas utilizan utmp como registro de sesiones.

`/var/log/wtmp` Información acerca de los inicios y finales de sesión

`/var/log/XFree86.0.log` Mensajes relativos a las X.

Como puede verse, se almacena información de cualquier evento que pueda producirse en el sistema, lo cual permite tener una visión hacia atrás en el tiempo en el caso que se produzca un error. Es posible conocer qué pasó antes de producirse el error, lo que ayuda a averiguar las causas del mismo.

La mayoría de los ficheros que se acaban de describir están en formato texto y son visibles desde cualquier editor. Sin embargo, hay uno de los ficheros de log del sistema que requiere del uso de un comando externo para su visualización. El fichero es `/var/log/lastlog` y la utilidad que se necesita para extraer la información contenida en él es `lastlog`. Esta utilidad formatea e

imprime el contenido del fichero `/var/log/lastlog` de forma más legible para el usuario que lo ejecuta.

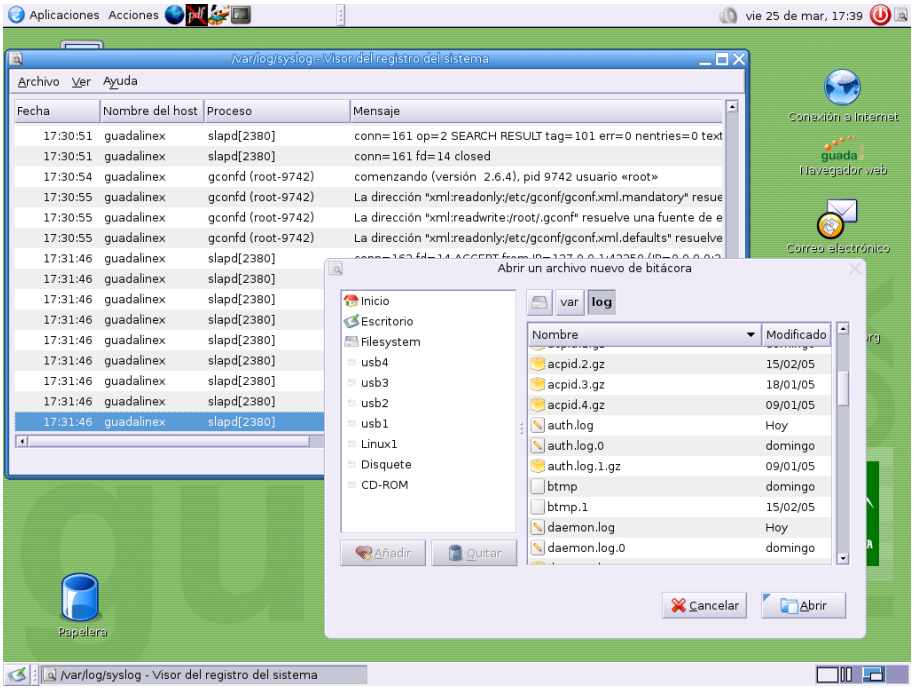
```
root@guadalinex:~# lastlog
Nombre           Puerto    De               Último
root             :20                        sáb mar 19 13:24:44 +0100 2005
daemon                                      **Nunca ha entrado**
bin                                         **Nunca ha entrado**
sys                                         **Nunca ha entrado**
sync                                        **Nunca ha entrado**
games                                       **Nunca ha entrado**
man                                         **Nunca ha entrado**
lp                                          **Nunca ha entrado**
mail                                        **Nunca ha entrado**
...
...
hugo             :0                         vie mar 25 09:17:36 +0100 2005
telnetd                                     **Nunca ha entrado**
legolas          pts/4     192.168.0.13     mar feb 15 21:19:53 +0100 2005
smmta                                       **Nunca ha entrado**
smmsp                                       **Nunca ha entrado**
postfix                                     **Nunca ha entrado**
nagios                                      **Nunca ha entrado**
amanda                                      **Nunca ha entrado**
jose.fernandez   pts/6     guadalinex       dom ene 30 20:09:53 +0100 2005
hugo.santander                              **Nunca ha entrado**
```

Otro comando que también se utiliza para ver los últimos accesos al sistema es `last`. Esta utilidad busca en el fichero `/var/log/wtmp` y muestra una lista de los usuarios conectados al sistema desde que el fichero fue creado.

```
root@guadalinex:~# last
hugo     pts/2        :0.0             Fri Mar 25 09:31   still logged in
hugo     pts/1        :0.0             Fri Mar 25 09:30   still logged in
hugo     pts/0        :0.0             Fri Mar 25 09:30   still logged in
hugo     :0                            Fri Mar 25 09:17   still logged in
reboot   system boot  2.6.5            Fri Mar 25 09:14          (08:15)
hugo     pts/2        :0.0             Thu Mar 24 13:34 - 00:39  (11:05)
hugo     pts/1        :0.0             Thu Mar 24 13:19 - 00:39  (11:20)
hugo     pts/0        :0.0             Thu Mar 24 13:19 - down   (11:20)
hugo     :0                            Thu Mar 24 13:14 - down   (11:25)
reboot   system boot  2.6.5            Thu Mar 24 11:10          (13:30)
hugo     pts/2        :0.0             Wed Mar 23 22:53 - down   (01:10)
hugo     pts/1        :0.0             Wed Mar 23 22:37 - down   (01:25)
hugo     pts/0        :0.0             Wed Mar 23 22:37 - down   (01:26)
hugo     :0                            Wed Mar 23 22:33 - down   (01:29)
reboot   system boot  2.6.5            Wed Mar 23 22:31          (01:32)
hugo     pts/1        :0.0             Sun Mar 20 14:29 - down   (00:19)
hugo     pts/0        :0.0             Sun Mar 20 14:17 - down   (00:30)
hugo     :0                            Sun Mar 20 14:15 - down   (00:33)
reboot   system boot  2.6.5            Sun Mar 20 14:11          (00:36)
wtmp begins Sun Mar 20 07:03:08 2005
```

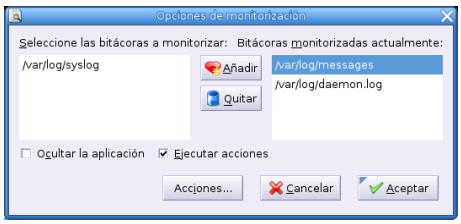
En Guadalinex existe una utilidad gráfica, fácilmente configurable, que visualiza los ficheros de log. Se encuentra en el menú **Aplicaciones→Configuración→Sistema→Bitácora del Sistema**. Se corresponde con la utilidad `gnome-system-log` y es necesario ejecutarla como usuario `root`.

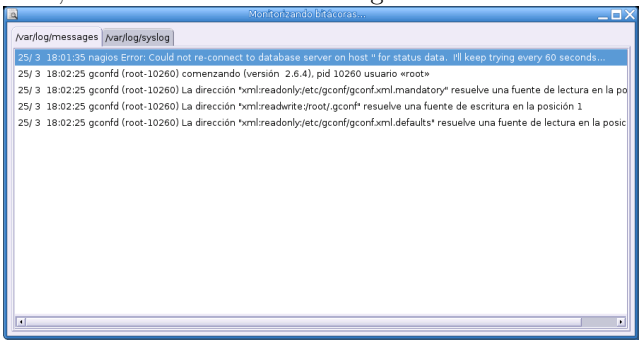
Figura 2.1: Guadalinex, Bitácora del Sistema



Es posible usar esta utilidad para supervisar los archivos de log del sistema previamente seleccionados, usando para ello la opción **Monitor**. Esta opción permite visualizar de forma simultánea varios ficheros de log.

Figura 2.2: Guadalinex, Monitorizar ficheros de log

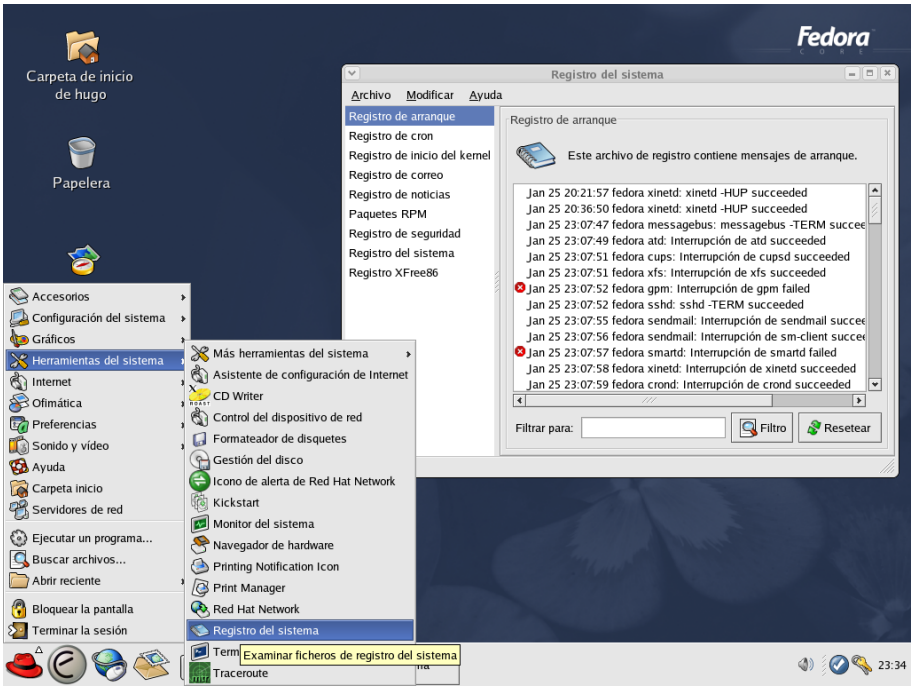




En el caso de Fedora, para facilitar la visión de algunos de estos ficheros, el sistema proporciona una utilidad gráfica denominada "Registro del Sistema"[2]

[2]Se corresponde con la utilidad Log Viewer versión 0.9.3

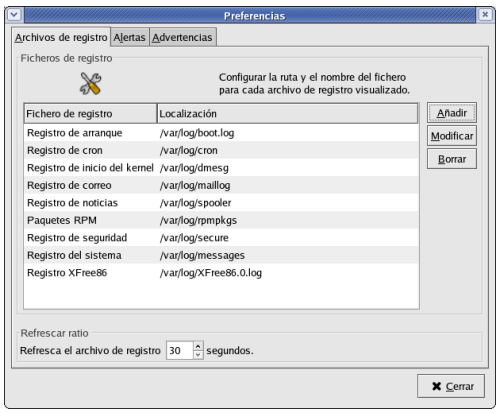
Figura 2.3: Fedora, Registro del sistema



Anteriormente, se vió el listado de algunos de los archivos de log que pueden encontrarse en el sistema. Hay que notar que la mayoría de ellos tenían establecido como dueño y grupo a `root`. Esto significa que únicamente `root` puede ver el contenido de estos ficheros. Lo mismo ocurre con los que pertenecen a otros usuarios, pudiendo visualizar su contenido los propios dueños o `root`. Esta aplicación para ver los archivos de logs se rige también por estos permisos, por lo que será necesario ejecutarla como `root`.

Si se pulsa sobre la opción **Modificar→Preferencias** pueden verse los archivos de log que tiene definidos por defecto:

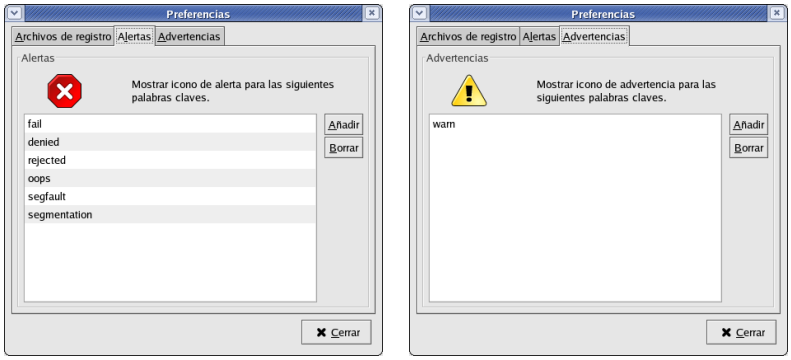
Figura 2.4: Fedora, Archivos de log por defecto



A esta lista se pueden añadir más archivos de log, así como definir en qué circunstancias se va a visualizar un indicador gráfico al lado de las líneas de log, que indicará alguna circunstancia

especial o de error.

Figura 2.5: Fedora, Alarmas y Advertencias

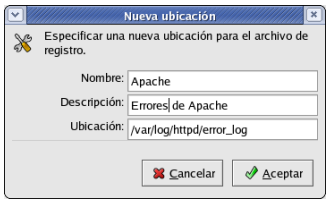


(a) Alarmas (b) Advertencias

En el caso de las alertas, las palabras que se han elegido para indicarnos esta circunstancia son: *fail*, *denied*, *rejected*, *oops*, *default*, *segmentation*. En el caso de las advertencias se tiene *warm*. Esto es configurable a según las necesidades para cada uno de los archivos de log.

La funcionalidad de esta utilidad no acaba aquí, es posible añadir nuevos archivos de log para visualizar.

Figura 2.6: Fedora, Configuración de nuevos archivos de log



En este caso, se ha elegido el archivo de log del servidor web apache que almacena las incidencias del servidor web `/var/log/httpd/error_log`.

2.3. Bitácora del sistema: syslog

La utilidad `syslogd` proporciona soporte al sistema de log de sistema así como del *kernel*. Soporta el almacenamiento de logs tanto de forma local como remota. El soporte para los logs del *kernel* lo proporciona la utilidad `klogd`.

Esta utilidad corre como un servicio que se ejecuta en el inicio del sistema. Es usado por distintas aplicaciones y otros servicios para guardar información sobre los distintos eventos que pueden ocurrir en el sistema. Por ejemplo, cuando el demonio de `cron` está intentando ejecutar un trabajo, manda una petición de "*logging*" a `syslogd`, que a su vez está configurado para enviar la entrada de información al archivo de log correspondiente `/var/log/cron`.

```
Mar 25 20:48:42 guadalinex crontab[4539]: (root) LIST (root)
Mar 25 20:48:46 guadalinex crontab[4540]: (root) BEGIN EDIT (root)
```

```
Mar 25 20:48:52 guadalinex crontab[4540]: (root) REPLACE (root)
Mar 25 20:48:52 guadalinex crontab[4540]: (root) END EDIT (root)
```

Cada de uno de los mensajes que se guardan en los archivos de log contienen al menos un campo con la hora y el nombre del *host*. Dependiendo de las características del programa de log y cómo sea de configurable esta información será más o menos completa, acorde a nuestras necesidades.

`Syslogd` puede mantener múltiples ficheros de log para distintas aplicaciones y servicios. La configuración del demonio `syslogd` se encuentra en `/etc/syslogd.conf`. Es en este fichero donde se le indica a `syslogd` la localización de los archivos de log dependiendo del grado de severidad del mensaje que ha provocado la aplicación de la cual se pretende registrar información.

```
#  /etc/syslog.conf     Configuration file for syslogd.
#
#                       For more information see syslog.conf(5)
#                       manpage.
#
# First some standard logfiles.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
cron.*                          /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log
uucp.*                          /var/log/uucp.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err
# Logging for INN news system
#
news.crit                       /var/log/news/news.crit
news.err                        /var/log/news/news.err
news.notice                     -/var/log/news/news.notice
#
# Some 'catch-all' logfiles.
#
*.=debug;\
        auth,authpriv.none;\
        news.none;mail.none     -/var/log/debug
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail,news.none          -/var/log/messages
#
# Emergencies are sent to everybody logged in.
#
*.emerg                         *
#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
#daemon,mail.*;\
```

```
#        news.=crit;news.=err;news.=notice;\
#        *.=debug;*.=info;\
#        *.=notice;*.=warn        /dev/tty8
# The named pipe /dev/xconsole is for the 'xconsole' utility.  To use it,
# you must invoke 'xconsole' with the '-file' option:
#
#    $ xconsole -file /dev/xconsole [...]
#
# NOTE: adjust the list below, or you'll go crazy if you have a reasonably
#      busy site..
#
daemon.*;mail.*;\
        news.crit;news.err;news.notice;\
        *.=debug;*.=info;\
        *.=notice;*.=warn        |/dev/xconsole
```

Las entradas de este fichero de configuración se encuentran divididas en dos columnas: qué registrar y dónde registrarlo.

2.3.1. ¿Qué podemos registrar en los ficheros de log?

La primera columna tendrá el formato:

```
servicio.severidad
```

La porción `servicio` de la entrada del fichero `syslogd.conf` especificará el tipo de proceso o servicio al que se aplica la norma.

Cuadro 2.1: Tipos de procesos disponibles en `/etc/syslogd.conf`

Tipo	Descripción
`*`	Todos los tipos posibles de procesos
`auth`	Mensajes relacionados con la autorización
`authpriv`	Mensajes relacionados con la autorización privada
`cron`	Mensajes desde los demonios cron y at
`daemon`	Mensajes de los demonios del sistema no especificados en esta tabla
`kern`	Mensajes del núcleo
`local0-local7`	Mensajes enviados a un terminal específico
`lpr`	Mensajes del demonio de impresión
`mail`	Mensajes del servidor de correo
`news`	Mensajes del servidor de noticias
`syslog`	Mensajes del demonio `syslogd`
`user`	Mensajes generales

Con `severidad` se indica qué información quiere guardase, teniendo en cuenta las limitaciones existentes de espacio en disco.

Cuadro 2.2: Niveles de severidad

Nivel	Descripción
`none`	Nada de este tipo de elemento
`emerg`	Mensajes que pueden estar relacionados con un mal funcionamiento o fallo
`alert`	Mensajes de alerta del sistema
`crit`	Mensajes relacionados con cuestiones críticas
`err`	Mensajes de error
`warning`	Mensajes que contienen advertencias
`notice`	Mensajes que contienen noticias que da el programa
`info`	Mensajes de información general
`debug`	Mensajes de depuración
`*`	Todos los niveles para este tipo de elemento

Pueden utilizarse comodines (`*`) tanto en los servicios como en las prioridades para indicar que concuerda con cualquiera. Existe también la partícula `none` como severidad que indica que no se guarde información sobre el evento en particular. Ésta última tiene sentido si se utiliza de forma conjunta con comodines

```
*.info
mail.none
```

Con la configuración anterior se indica que se guarde la información de severidad `info` para todas las aplicaciones excepto para el servicio `mail`.

Otra opción es especificar un subconjunto de servicios separados y una severidad:

```
mail,uucp,news.info
```

También pueden agruparse múltiples reglas juntas para que realicen la misma acción, utilizando el siguiente formato:

```
mail.info;cron.warning
```

Hay que tener en cuenta un aspecto importante en lo referente a la severidad. Cuando se configura una acción para una severidad, se configura para esa severidad y para las que son más altas. Existe sin embargo una funcionalidad que permite decirle al demonio `syslogd` que registre únicamente el nivel de severidad que se puso en la lista[3]. Esta funcionalidad se activa colocando el signo `=` delante de la severidad.

```
mail.=warning
```

En este caso se está indicando que únicamente registre los mensajes con severidad `warning`.

También puede indicarse que no incluya una severidad concreta, colocando el signo `!` delante de ésta.

```
mail.warning; mail.!err
```

Ahora se registrarán los mensajes de severidad `warning` y superiores, excepto los de severidad `err`.

2.3.2. Acciones en respuesta a eventos.

Una vez se ha establecido la información sobre los servicios que se van a registrar, es necesario indicar a syslogd dónde tiene que colocar esa información. En la segunda columna de `/etc/syslog.conf` se indica el destino de la información.

Normalmente lo que aparece aquí es la ruta al archivo en el que se guardarán los mensajes con una determinada severidad que vaya generando el servicio.

En el fichero de configuración mostrado al principio aparece la siguiente entrada:

[3]Es una característica adicional incluida en las distribuciones basadas o con origen en RedHat

```
cron.*                                          /var/log/cron
```

Esta línea indica al sistema operativo que almacene cualquier mensaje proveniente de la aplicación `cron` en el fichero `/var/log/cron`. El `*` se refiere a la severidad del mensaje, optando por almacenar todos los mensajes, independientemente de su severidad, en el fichero `/var/log/cron`. Puede especificar también distintas localizaciones dependiendo de la severidad:

```
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err
```

En este caso, los mensajes de error serán almacenados en `/var/log/mail.err`, los mensajes de advertencia en `/var/log/mail.warn` y los mensajes con carácter informativo en `/var/log/-mail.info`.

Tras registrar la información que genera un servicio, se sincroniza el archivo donde se están guardando los mensajes. Esto es debido a que la información no siempre se guarda de forma inmediata en el sistema de archivos, sino que ésta se encuentra inicialmente en memoria. Si el trasvase de información es elevado, la constante sincronización puede afectar al rendimiento del sistema. Para anular esta sincronización se añade un signo `-` delante de la ruta.

Dentro de las acciones a realizar con la información que estamos registrando está el enviarla, mediante una tubería, a otro programa o script para un posterior procesamiento. Simplemente tendremos que añadir el símbolo `|` antes de la ruta al programa o script.

```
|/usr/local/bin/procesarlogs.sh
```

Como se indicó al comienzo de esta sección, existe la posibilidad de centralizar los logs del sistema en una máquina remota. El requisito que debe cumplir el servidor remoto es que tenga el demonio `syslogd` ejecutándose.

```
@maquinaremota
```

Por último, la información de log no tiene por qué enviarse a un fichero, puede enviarse directamente a la pantalla o la consola de administración (`/dev/tty3` y `/dev/console` respectivamente). Otra opción es enviar la información de log que se genera por correo a los usuarios que definamos, únicamente tenemos que poner la lista de usuarios separados por comas.

2.4. Gestión de los logs

2.4.1. Registro de nuestros scripts

Acabamos de ver cómo el sistema almacena los eventos que se van produciendo en distintas localizaciones. Así, cualquier fallo o error en el sistema queda reflejado para su posterior estudio. Sería interesante disponer de esta misma funcionalidad en cualquiera de los scripts que creemos para ayudar en la administración del sistema. Conoceríamos en todo momento si la ejecución de los mismos ha sido correcta o no. Para realizar esta función está `logger` (`/usr/bin/logger`), es una interfaz de línea de comando con syslog.

```
logger [-isd] [-f fichero] [-p severidad] [-t tag] [-
u socket] [mensaje ...]
```

Con `logger` podemos escribir los mensajes de nuestros scripts a la localización estándar de los logs, siendo gestionado por el demonio `syslogd`.

Cuadro 2.3: Opciones de la utilidad `logger`

Opción	Descripción
`-i`	Registra el pid del proceso en cada línea
`-s`	Registra el mensaje en la salida de error estándar
`-d`	Utiliza un datagrama en lugar de una conexión stream con el socket
`-f fichero`	Registra el mensaje en el fichero especificado
`-p severidad`	Registra el mensaje con la severidad especificada
`-t tag`	Marca cada línea con la etiqueta específica
`-u socket`	Escribe en un socket
`--`	Finaliza la lista de opciones para poder empezar el mensaje con -
`mensaje`	Escribe el mensaje en el log

La prioridad indicada con la opción `-p` puede ser especificada numéricamente o con la pareja `servicio.severidad`. Si no se especifica el valor por defecto es `user.notice`. Por ejemplo para registrar los mensajes del servicio `local3` con la severidad `info`:

```
logger -p local3.info
```

En caso de que no especifiquemos mensaje y tampoco proporcionemos la opción `-f`, se registrará la entrada estándar.

La salida de `logger` será `0` si hay éxito ó `>0` en caso de error.

Consideraciones previas que hay que tener en cuenta antes de empezar a utilizar `logger`:

- Es necesario que el fichero de log exista antes de enviar un mensaje al mismo a través de `logger`.
- Es necesario crear una entrada en `/etc/syslog.conf` que refleje la existencia del fichero de log que `logger` va a mantener.

2.4.2. Rotación de los logs

Los distintos ficheros de log con la información de registro de aplicaciones y sistema van a almacenar una gran cantidad de datos. Es necesario implementar un mecanismo que permita borrar los datos de registro antiguos así como facilitar la búsqueda de información en los mismos. En el caso de no tener esto en cuenta se podrá comprobar cómo el sistema se llena cada vez más con ficheros de log, los cuales serán cada vez más grandes.

Los sistemas actuales cuentan con la utilidad `logrotate`. Esta utilidad se encarga de realizar la rotación de los ficheros de registro, renombrando el archivo y creando uno nuevo que pasa a ser el fichero de log activo.

Esta utilidad se configura de forma general a través del fichero `/etc/logrotate.conf`. Este fichero suele tener por defecto una configuración similar a la siguiente:

```
# Mirar "man logrotate" para más detalles
# Rota los ficheros de log de forma semanal
weekly
# Guarda 4 copias de los ficheros de logs
rotate 4
# Crea un fichero nuevo (vacio) de log después de rotar los antiguos
create
# Los ficheros de log que se guardan serán comprimidos
compress
# Los paquetes de las aplicaciones dejan la información sobre la rotación de
    logs en este directorio
include /etc/logrotate.d
# También se define aquí el comportamiento de logs específicos
```

```
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}
/var/log/btmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}
# La rotación del resto de logs específicos del sistema se define a partir
    de aquí
```

Contendrá la configuración global para todo el sistema de rotación de logs. Para configurar la rotación de forma particular también tenemos cada uno de los ficheros de `/etc/logrotate.d`.

2.5. Análisis de logs con logwatch

El análisis de los logs de sistema por parte del administrador es un trabajo rutinario y pesado. Son muchos los ficheros que hay que mirar y algunos de ellos pueden generar miles de líneas de información cada día, siendo necesario analizarlos a diario en busca de posibles fallos en el sistema o intentos de acceso no permitidos al mismo.

Una utilidad que puede ayudar en este trabajo es **Logwatch**[4]. Tiene como función principal analizar los archivos de log del sistema, así como crear informes sobre el estado del mismo. Analizará las entradas en los ficheros de log del sistema por el periodo de tiempo definido y realizará un informe sobre determinadas áreas con el nivel de detalle especificado.

```
logwatch [opciones]
```

Las opciones con que puede llamarse a esta utilidad son:

Opción	Acción realizada
`--detail`	Indica el nivel de detalle del informe (`high`, `med` y `low`)
`--logfile`	Fuerza a logwatch a utilizar únicamente el grupo de ficheros de registro indicado. De esta forma sólo se procesará información de los servicios que escriban en estos ficheros de registro
`--service`	Fuerza a logwatch a procesar únicamente los servicios indicados en este parámetro. Procesará todos los ficheros de registro que utiliza este servicio.
`--print`	Muestra el resultado del análisis por la salida estándar.
`--mailto`	Dirección a la que va a enviar el informe de análisis de ficheros de registro.
`--archives`	Esta opción indica a logwatch qué ficheros de registro archivados (normalmente con extensión gz) puede analizar, junto con los ficheros de registro actuales.
`--range`	Rango en el que se va a realizar el análisis (Today, Yesterday y All)
`--debug`	Nivel de debug que se va a aplicar durante el análisis. Únicamente utilizado para detectar errores durante el análisis.
`--save`	Nombre de fichero donde se va a guardar el resultado del análisis de los ficheros de registro.
`--usage` y `--help`	Muestra información de uso de logwatch.

[4]Esta aplicación normalmente está instalada en las distribuciones Fedora. En el caso de Guadalinex es preciso instalarla mediante `apt-get`:

```
apt-get install logwatch
```

Mediante estos parámetros puedes modificarse la configuración durante la ejecución del análisis. Sin embargo, existe también un fichero de configuración `/etc/logwatch/logwatch.conf`[5] que puede establecer el valor de estos parámetros por defecto. Así, cuando se ejecute `logwatch` sin ningún parámetro, tomará los valores establecidos en este fichero. Los parámetros que aparecen en este fichero son:

- Directorio de Log por defecto

  ```
  LogDir = /var/log
  ```

- Directorio temporal por defecto

  ```
  TmpDir = /tmp
  ```

- Persona a la que se le envían los correos con los informes

  ```
  MailTo = root
  ```

- Indica si se envía por correo (NO) o si se muestra por *stdout* (YES)

  ```
  Print = No
  ```

- Para compatibilidad con `mktemp`

  ```
  UseMkTemp = Yes
  ```

- Si está definido, guardará los informes en la ruta indicada en lugar de enviarlo por correo o mostrarlo.

  ```
  Save = /tmp/logwatch
  ```

- Define si se busca en archivos con extension `gz` además de en los ficheros de log actuales.

  ```
  Archives = Yes
  ```

- El rango de tiempo por defecto para el informe (`Today, Yesterday, All`)

  ```
  Range = yesterday
  ```

- El detalle del informe por defecto (`Low = 0, Med = 5, High = 10`)

  ```
  Detail = Low
  ```

- El servicio por defecto para el que se hace el informe. Espera el nombre de un filtro en `/etc/log.d/scripts/services/*` o `All` para todo

  ```
  Service = All
  ```

- Si sólo quisiéramos un informe acerca de ftp

  ```
  Service = ftpd-messages
  Service = ftpd-xferlog
  ```

- Si queremos que únicamente se analice un fichero de log

  ```
  LogFile = messages
  ```

[5] Dependiendo de la distribución de linux el directorio con la configuración de Logwatch puede variar, p.e. `/var/log.d`.

- Localización del programa que envía los correos

  `mailer = /bin/mail`

- Si se establece como Yes se muestran sólo los mensajes referidos al host donde se ejecuta

  `HostLimit = Yes`

La salida generada por `logwatch` para el nivel de detalle por defecto puede ser como la siguiente:

```
##################### LogWatch 5.1 (02/03/04) ####################
Processing Initiated: Fri Mar 25 22:10:02 2005
Date Range Processed: today
Detail Level of Output: 5
Logfiles for Host: guadalinex
##################################################################
--------------------- samba Begin ------------------------
**Unmatched Entries**
nmbd/nmbd_nameregister.c:register_name(482) register_name: NetBIOS name
    G2004_1108431407 is too long. Truncating to G2004_110843140 : 6 Time(s)
--------------------- samba End ------------------------
-------------------- Disk Space --------------------
S.ficheros Tamaño Usado Disp Uso% Montado en
/dev/hda1 4,0G 2,7G 1,1G 72% /
tmpfs 93M 0 93M 0% /dev/shm
-------------------- Fortune --------------------
OpenOffice es potente, Abiword es más rápido
###################### LogWatch End #########################
```

En este caso el informe es reducido, pero dependiendo de la actividad del sistema será más amplio.

Continuando con el resto de ficheros de la utilidad Logwatch, se encuentra la siguiente estructura de directorios que soporta su funcionamiento:

`/etc/logwatch/logwatch.conf` Ya se habló anteriormente de este fichero. Realmente es un enlace simbólico a `/etc/log.d/conf/logwatch.conf`

`/etc/logwatch/conf/services/*` Configuración para los servicios que se van a analizar, así como los ficheros de registro que utilizan

`/etc/logwatch/conf/logfiles/*` Configuración para los ficheros de registro de los servicios a analizar

`/etc/logwatch/scripts/shared/*` Filtros comunes a servicios y/o ficheros de registro

`/etc/logwatch/scripts/logfiles/*` Filtros utilizados para determinados ficheros de registro

`/etc/logwatch/scripts/services/*` Filtros utilizados para los distintos servicios

La herramienta viene configurada para una serie de servicios bastante amplia, pero aún así, es posible ampliar el rango de servicios a analizar. Únicamente debe escribirse el filtro que extraiga la información que se busca de los ficheros de registro correspondientes a una aplicación.

Capítulo 3

Utilidades de administración

> "¿Para quién es Webmin? Webmin es una excelente herramienta tanto para administradores noveles como experimentados."
>
> *System Administation with Webmin*

3.1. Administración remota de sistemas

Webmin es una utilidad de administración de sistemas UNIX vía web, desarrollada por Jamie Cameron y basada en una serie de scripts escritos en Perl. Básicamente, puede decirse que Webmin es un conjunto de CGIs escritos en Perl. Esto le confiere una gran flexibilidad y portabilidad[1], permitiendo esta característica la ampliación con nuevos módulos y funcionalidades.

Webmin utiliza su propio servidor web, escuchando en el puerto que se le indique en la instalación, siendo éste totalmente independiente (si lo tiene) del que se tenga configurado mediante Apache.

3.2. ¿Por qué utilizar Webmin?

Mediante el uso de Webmin, se dispone de una interfaz gráfica fácil de utilizar y que proporciona soporte para un gran número de servicios y labores de mantenimiento del sistema.

Al basarse en una interfaz web, se puede acceder a la totalidad de sus funcionalidades desde prácticamente cualquier sitio de la red, independientemente del sistema operativo. El único requisito es disponer de una conexión a la red donde se encuentra instalado Webmin y de un navegador web.

Por su simplicidad de uso, está indicado tanto para administradores noveles como para los que tienen una experiencia de años. Para los primeros, proporciona una forma visual de acercarse a la administración de sistemas, al mostrar las opciones de los distintos servicios de forma gráfica. En el caso de los administradores con amplia experiencia hay que pensar en la cantidad de opciones definidas para los distintos servicios activos en el sistema, así como los scripts diseñados por ellos mismos para ayudarles en sus labores de administración y monitorización. Mediante el uso de Webmin, pueden crearse llamadas gráficas a estas funcionalidades, evitando así la necesidad de recordar todas y cada una de las opciones o scripts que se ejecutan en un momento dado.

En los siguientes apartados se describirán los pasos necesarios para tener Webmin instalado en un sistema y explicaremos algunas de las opciones más comunes.

[1] Se puede utilizar en más de 35 sistemas UNIX y Linux

3.3. Instalación de Webmin

Una vez que se tiene una ligera idea de lo que Webmin es, se verá de inmediato cómo puede instalarse para empezar a tener otro aspecto, más visual, de la administración de sistemas.

El mejor sitio desde donde bajarse la última versión disponible de Webmin es su web

`http://www.webmin.com/`

que permite bajar el paquete RPM o un tgz que contiene los ficheros de instalación. En el caso de instalar Webmin sobre un sistema Guadalinex puede utilizarse el procedimiento seguido a lo largo del curso, mediante `apt-get`.

```
apt-get install webmin
apt-get install webmin-core
```

La versión que se encuentra disponible en los repositorios de Guadalinex es la 1.130 de 26 de enero de 2004[2]. A pesar de no ser la última versión disponible, esto no presenta ningún incoveniente debido a que Webmin permite la actualización desde la interfaz web. Así, una vez finalizado el proceso de instalación se realizará la actualización para estar a la última versión.

Existe un bug en los paquetes que se instalan en Guadalinex y Debian en general. Está relacionado con la gestión de los temas de webmin y no presenta graves problemas. El bug consiste en que no se puede cambiar de tema, por lo que hay que limitarse a utilizar el tema por defecto para Debian. Este fallo no afecta al resto de funcionalidades de Webmin, que son las que realmente nos ocupan.

En el caso de optar por realizar la instalación a partir del tgz descargado el proceso es el siguiente:

```
root@guadalinex:~# cd /usr/local/
root@guadalinex:/usr/local# tar -zxvf /home/hugo/webmin-1.190.tar.gz
```

Una vez extraídos todos los ficheros del paquete tgz es el momento de comenzar el proceso de instalación.

```
root@guadalinex:/usr/local# cd webmin-1.190
root@guadalinex:/usr/local/webmin-1.190#  ./setup.sh
```

Este script servirá de guía a través del proceso de instalación.

```
*********************************************************************
*            Welcome to the Webmin setup script, version 1.190      *
*********************************************************************
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.
Installing Webmin in /usr/local/webmin-1.190 ...
*********************************************************************
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.
Config file directory [/etc/webmin]:
Log file directory [/var/webmin]: /var/log/webmin
*********************************************************************
Webmin is written entirely in Perl. Please enter the full path to the
Perl 5 interpreter on your system.
Full path to perl (default /usr/bin/perl):
```

[2] En el momento de escribir estos apuntes la versión más actualizada de Webmin es la 1.190 de 24 de marzo de 2005.

```
Testing Perl ...
Perl seems to be installed ok
******************************************************************
Operating system name:    Debian Linux
Operating system version: 3.1
******************************************************************
Webmin uses its own password protected web server to provide access
to the administration programs. The setup script needs to know :
 - What port to run the web server on. There must not be another
   web server already using this port.
 - The login name required to access the web server.
 - The password required to access the web server.
 - If the webserver should use SSL (if your system supports it).
 - Whether to start webmin at boot time.
Web server port (default 10000):
Login name (default admin):
Login password:
Password again:
Use SSL (y/n): y
Start Webmin at boot time (y/n): y
******************************************************************
Creating web server config files..
..done
Creating access control file..
..done
Inserting path to perl into scripts..
..done
Creating start and stop scripts..
..done
Copying config files..
..done
Configuring Webmin to start at boot time..
Created init script /etc/init.d/webmin
..done
Creating uninstall script /etc/webmin/uninstall.sh ..
..done
Changing ownership and permissions ..
..done
Running postinstall scripts ..
..done
Attempting to start Webmin mini web server..
Starting Webmin server in /usr/local/webmin-1.190
..done
******************************************************************
Webmin has been installed and started successfully. Use your web
browser to go to
 https://guadalinex:10000/
and login with the name and password you entered previously.
Because Webmin uses SSL for encryption only, the certificate
it uses is not signed by one of the recognized CAs such as
Verisign. When you first connect to the Webmin server, your
browser will ask you if you want to accept the certificate
presented, as it does not recognize the CA. Say yes.
```

Ya estaría instalado Webmin en el sistema, para comprobarlo puede ejecutarse:

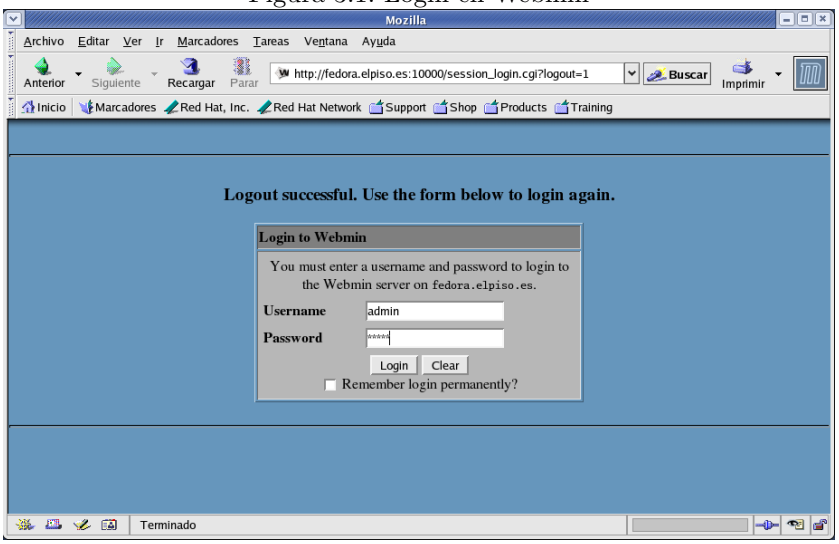
```
root@guadalinex:~# netstat -lp | grep 10000
tcp        0      0 *:10000                 *:*                     LISTEN      5631/perl
udp        0      0 *:10000                 *:*                                 5631/perl
```

Tal como se ha configurado, el puerto 10000 está a la escucha y preparado para recibir peticiones. Al estar Webmin basado en scripts realizados en Perl, será éste el proceso asociado al puerto 10000.

3.4. Primera toma de contacto

Tenemos Webmin recién instalado en nuestro sistema y estamos ansiosos por ver cómo funciona y cómo nos va a permitir administrarlo de una forma más "amigable". Si se escribe en nuestro navegador web `http://nombreservidor:10000/` aparecerá la pantalla de login en Webmin.

Figura 3.1: Login en Webmin

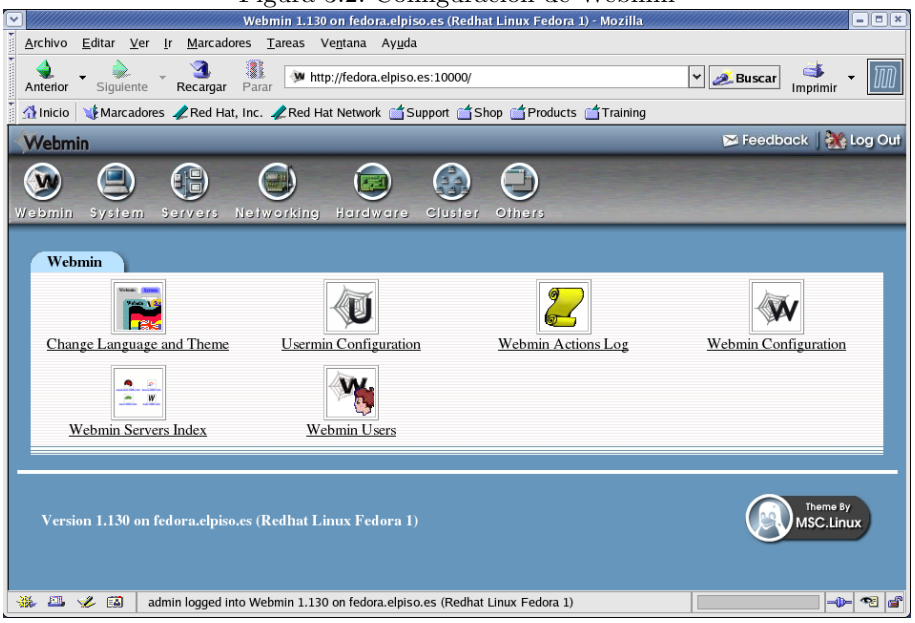


Hasta el momento, únicamente está definido el usuario `admin`[3]. Posteriormente se verá cómo añadir más usuarios, de momento es suficiente con el creado durante la instalación.

Una vez logado con éxito, la pantalla que nos sirve Webmin es la siguiente:

[3]En el caso de la instalación en Guadalinex el usuario es `root`.

Figura 3.2: Configuración de Webmin



Bueno, parece que la primera pantalla no tiene mala pinta ¿verdad? Puede intuirse que la herramienta va a ser bastante completa, sin olvidar que es ampliable con más módulos y scripts existentes en el sistema creados por el administrador.

En esta primera pantalla encontramos las siguientes secciones:

Change Language and Theme. Esta opción permite cambiar el idioma de Webmin.

Configuración Usermin. Permite la configuración del módulo opcional Usermin. Este módulo es una versión simplificada de Webmin diseñada más para usuarios del sistema que para administradores.

Configuración de Webmin. Es el módulo principal de configuración de Webmin. Permitirá actualizar Webmin, gestionar los módulos, gestionar la seguridad y los archivos de log.

Diario de Acción de Webmin. Cuando se habilita el sistema de log, este módulo permitirá búsquedas avanzadas en los logs.

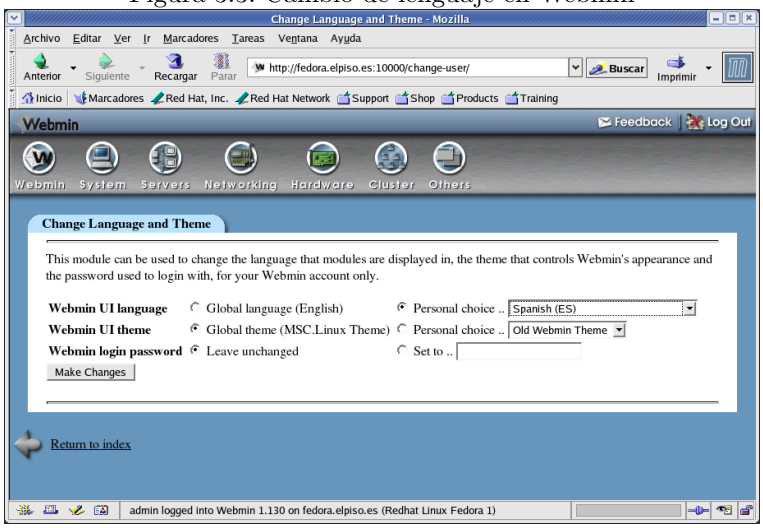
Usuarios de Webmin. Con la configuración de usuarios puede controlarse a qué módulos puede acceder cada usuario e incluso definir grupos para el acceso a módulos.

Índice de Servidores de Webmin. Permite añadir múltiples servidores Webmin existentes en la red para hacerlos accesibles desde una única interfaz.

No esperemos más y vamos a empezar a utilizar Webmin. Lo primero es cambiar el idioma y adaptar Webmin al castellano.

Dentro de esta opción puede cambiarse la palabra de entrada en Webmin del usuario actual (en nuestro caso sigue siendo admin). Aunque se haya cambiado el idioma, puede que algunos nombres de opciones sigan aún en inglés. Webmin es un proyecto que crece día a día y hay algunos aspectos que aún tienen que mejorar.

Figura 3.3: Cambio de lenguaje en Webmin



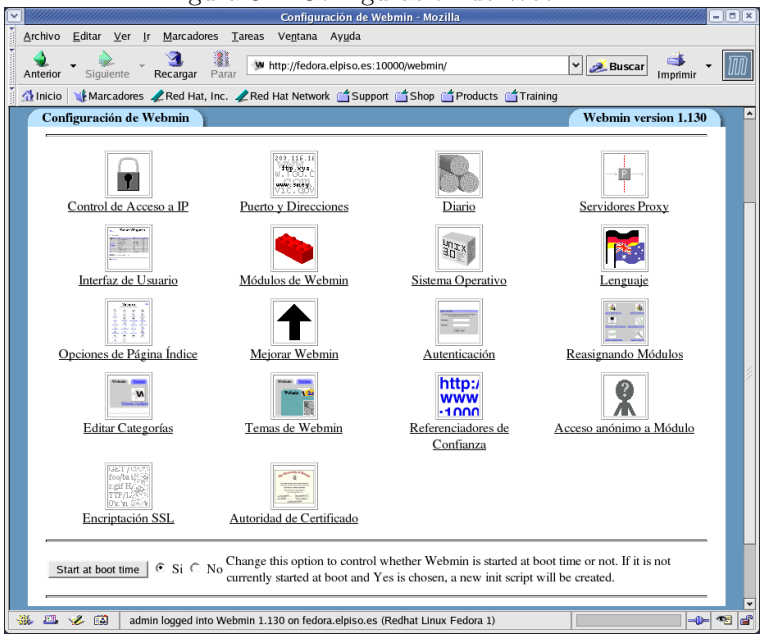
Otro módulo que aparece en esta pantalla inicial es Diarios de Accion de Webmin. Desde aquí se accede a los logs que vayan generándose por el uso de la herramienta, permitiendo una posterior monitorización del sistema. Esta funcionalidad es también configurable como se verá en la siguiente sección.

Posteriormente se volverá al resto de opciones referentes a usuarios y al índice de servidores Webmin. Ahora nos centraremos en seguir conociendo la herramienta.

3.5. Administración de Webmin

3.5.1. Configuración de Webmin

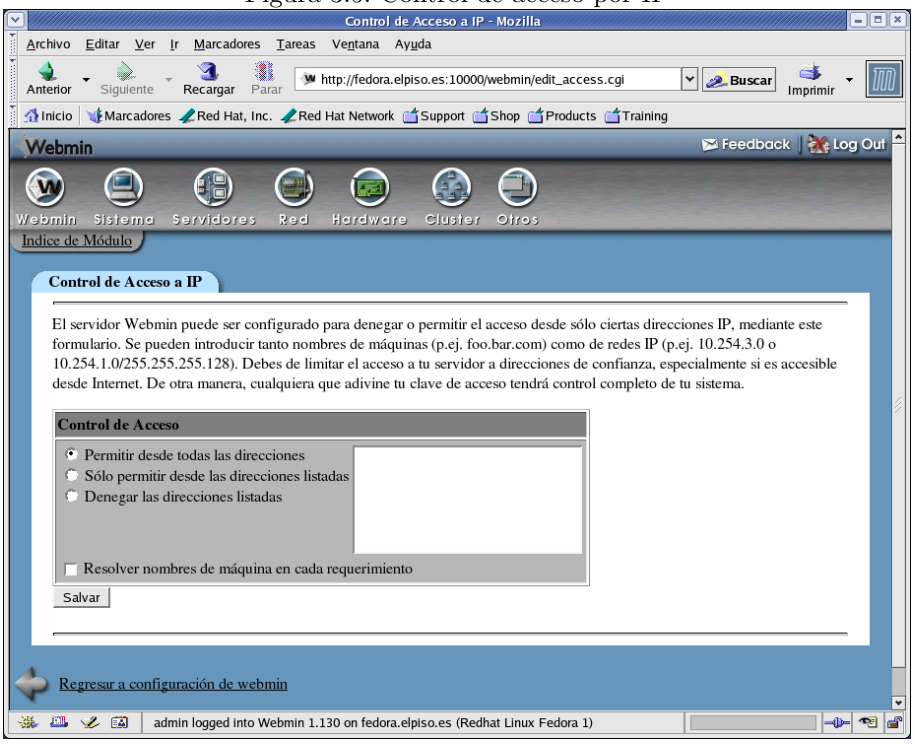
Figura 3.4: Configuración de Webmin



Este módulo permite configurar los aspectos más importantes de Webmin, así como instalar o actualizar nuevos módulos o incluso actualizar la propia herramienta.

Uno de los aspectos que no hay que olvidar es la seguridad en el acceso a Webmin. Es posible configurar esta herramienta para que se acceda únicamente desde las direcciones IP que se le indique. El módulo que controla este aspecto es Control de Acceso a IP.

Figura 3.5: Control de acceso por IP

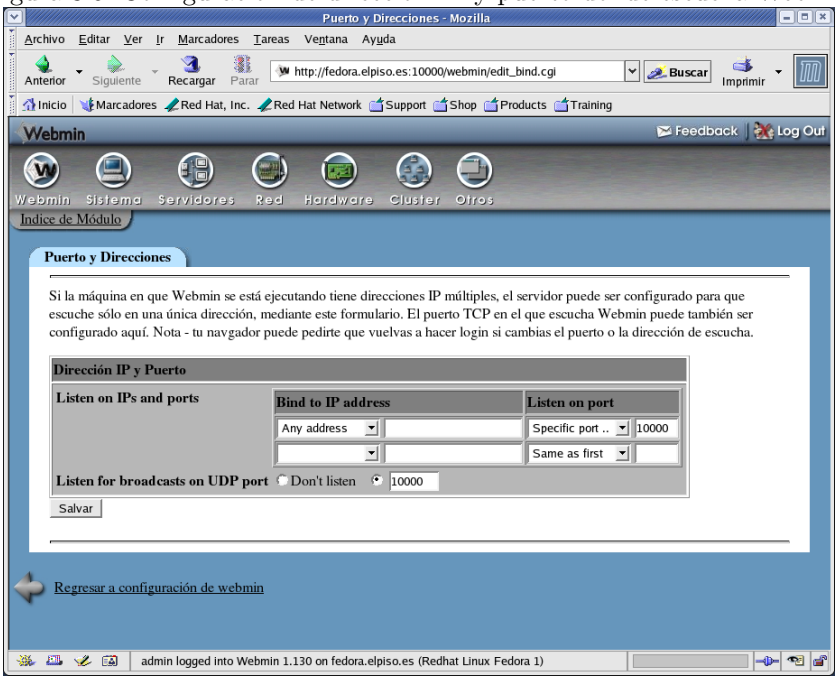


Por defecto está configurado para permitir el acceso desde cualquier dirección IP. Se indicará si se permite o niega el acceso desde las direcciones o redes que se especifiquen en la configuración de este módulo[4].

Otro módulo que aparece en esta sección es el relativo a la dirección IP y el puerto en el que estará a la escucha de peticiones. Este módulo es Puerto y Direcciones y, por defecto, configura Webmin a la escucha en todas las direcciones IP que tenga configuradas el sistema. En caso de tener varias interfaces de red con acceso a distintas redes, sería recomendable, por motivos de seguridad, configurar Webmin para que únicamente esté escuchando en la dirección IP que pertenezca a la red más segura.

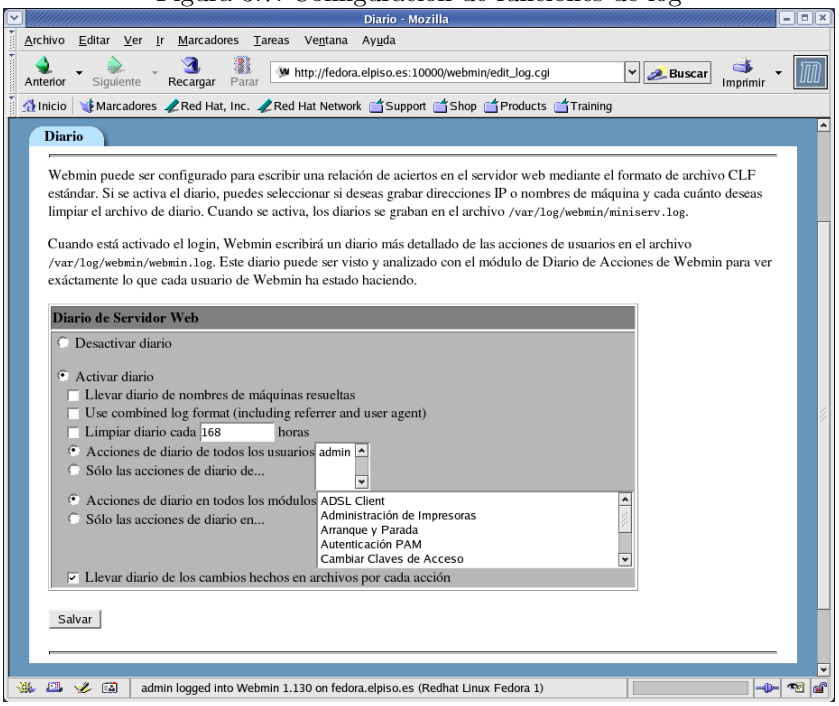
[4]En caso de que alguien obtenga alguna de las claves de acceso a Webmin, con este módulo se establece un nivel más de seguridad.

Figura 3.6: Configuración de dirección IP y puerto donde escucha Webmin



Como ya se dijo, es posible cambiar desde este módulo el puerto donde escucha Webmin. El valor que tiene establecido por defecto es el 10000, aunque puede aparecer otro, si así se lo hemos indicado durante el proceso de instalación.

Figura 3.7: Configuración de funciones de log



Otro módulo interesante y que ayudará a controlar el uso que se hace de Webmin es DIARIO. Hay que recordar que Webmin proporciona funcionalidades de log. Esto permite monitorizar fácil-

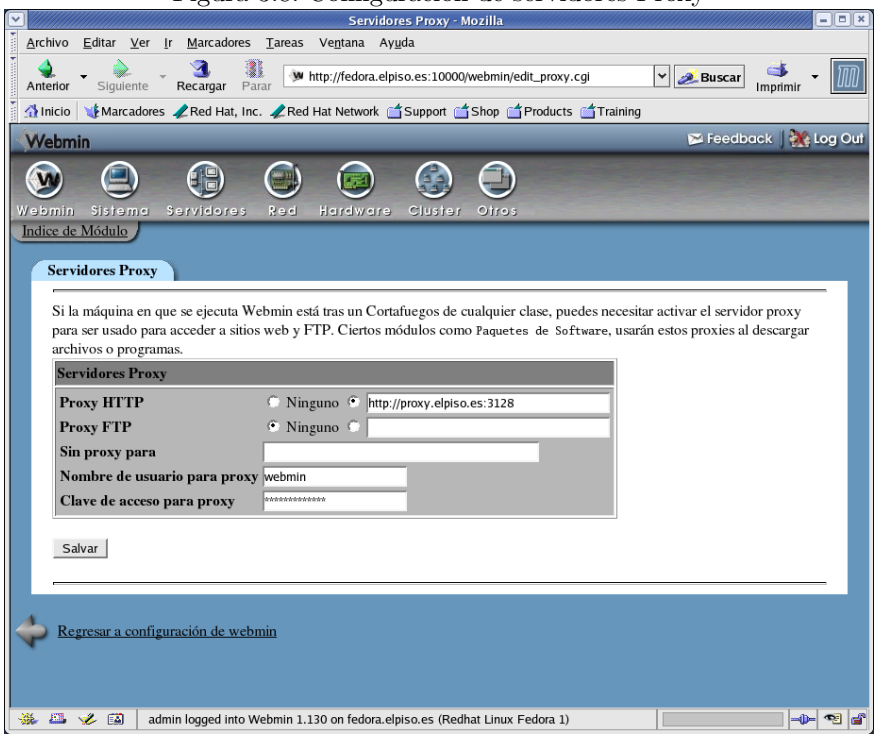
mente las acciones que realizan los distintos usuarios de Webmin, conociendo el momento concreto en que se ha llamado a un módulo y qué acción se ha realizado en el mismo.

Como puede verse, es posible tener un registro detallado de las acciones realizadas basado en el módulo donde se realizaron las acciones. La opción "**Llevar diario de nombres de máquinas resueltas**" hará que Webmin muestre el nombre de la máquina que se ha conectado en lugar de su dirección IP. También puede vaciar los ficheros de log en el intervalo que se establezca, efectuándose una rotación de los mismos.

Para evitar que el disco se llene de forma innecesaria, es conveniente realizar un estudio previo de la situación del sistema y establecer los módulos que es preciso monitorizar y excluir el resto de los logs de Webmin.

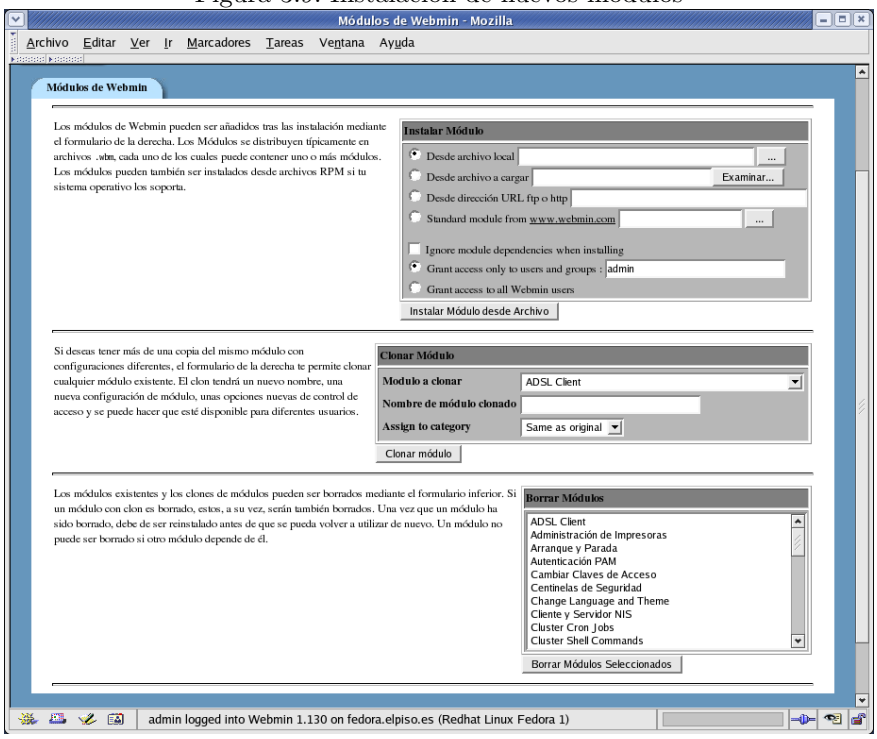
Puede que el servidor donde se encuentra Webmin alojado esté detrás de un cortafuegos o utilice un proxy para salir a internet. Será necesario configurar Webmin para permitirle la conexión a internet en el caso que requiera bajarse alguna actualización o algún módulo adicional, indicándole un proxy a través del cual pueda descargarse los módulos o actualizaciones necesarias.

Figura 3.8: Configuración de servidores Proxy



Una de las principales características de Webmin es su diseño modular. Así, es posible crear nuevos módulos que se integren por completo en la estructura de esta herramienta. Desde MÓDULOS DE WEBMIN es posible instalar nuevos módulos, ya sea desde un fichero local o desde una localización de otro servidor en internet. Los módulos de Webmin son paquetes tar que contienen la estructura completa del módulo. Estos módulos tienen la extensión .wbm.

Figura 3.9: Instalación de nuevos módulos



Pueden encontrarse bastantes módulos para Webmin hechos por otras personas en
`http://webmin.thirdpartymodules.com/`

La mayoría de ellos son gratuitos y están organizados por categorías para una búsqueda más eficiente.

Dentro de la administración de módulos existe la posibilidad de clonar módulos. Esto es especialmente útil para el caso en que sea necesario disponer de varios módulos de gestión de un servicio del sistema y que se ejecuten con distintas configuraciones. Los ficheros de configuración de los servicios debemos gestionarlos nosotros, haciendo copias de los ficheros de configuración para que cada una de las instancias del módulo utilice una configuración distinta.

Pueden también borrarse los módulos que no vayan a utilizarse o que no quieran gestionarse desde Webmin. Hay que tener en cuenta que esto borrará el módulo completamente del sistema, siendo necesario bajarlo de nuevo e instalarlo si posteriormente lo queremos utilizar. Una opción mejor es quitarlo del perfil de los usuarios que no queremos que lo utilicen, tal como veremos en la gestión de los usuarios.

Además de la instalación de nuevos módulos, la actualización de Webmin se realizará desde Mejorar Webmin. La actualización se refiere tanto a la herramienta Webmin como a los módulos que trae en la distribución estándar. Realizando regularmente este proceso de actualización, mantendremos Webmin en un estado óptimo, corrigiendo posibles errores o agujeros de seguridad que se detecten.

Esta visión general de algunos de los módulos de configuración de Webmin debe ser suficiente para empezar a utilizarlo. Hay más módulos que es recomendable investigar y ver las funcionalidades que presentan en lo referente a personalizar Webmin.

Gestión de usuarios

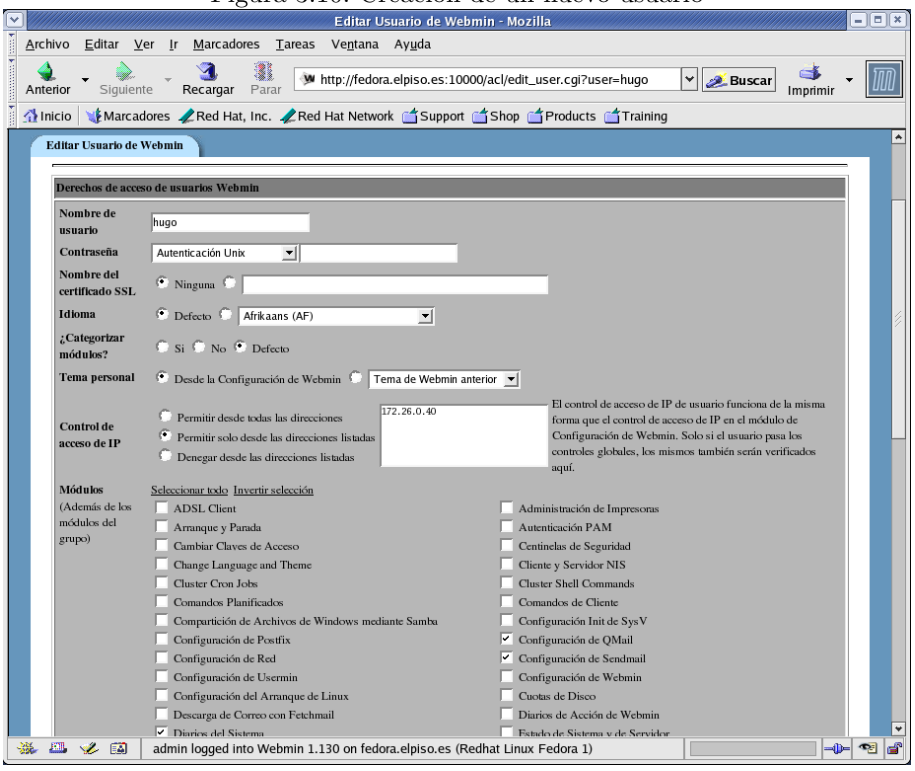
La gestión de usuarios de Webmin permite tener varios perfiles de administradores de sistemas. Por ejemplo, se puede disponer de un usuario en Webmin que se encargue de gestionar el servidor de correo, otro para gestionar el servidor web, otro para gestionar el servidor DNS. Así

el usuario que encargado de gestionar el correo no podrá interferir en las operaciones que realicen los administradores de web y DNS ya que no tendrá permisos para utilizar otros módulos que no sean los relacionados con el correo y para los que tiene acceso.

Dentro de la categoría Webmin entraremos en el módulo USUARIOS DE WEBMIN. El único usuario que existe es el usuario admin, con el que nos hemos validado en el sistema. Este usuario tiene acceso a todos los módulos instalados en el sistema.

Crearemos un nuevo usuario que se encargue de la administración del correo.

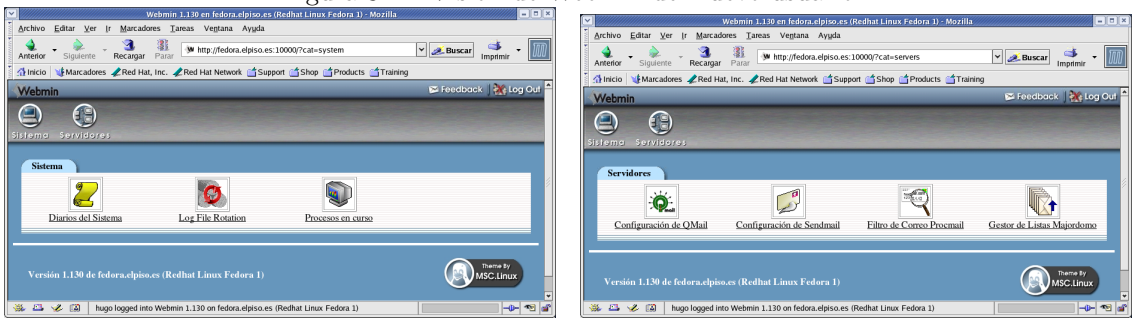
Figura 3.10: Creación de un nuevo usuario



A este usuario se le han asignado permisos para utilizar únicamente un grupo reducido de módulos. Es interesante también comprobar que en el apartado **Contraseña** hemos indicado que se utilice el método de autenticación Unix. Webmin puede gestionar los usuarios de forma independiente del sistema o basarse en los que hay creados. Cada una de estas opciones tiene sus ventajas y sus inconvenientes. La gestión de usuarios Unix es especialmente indicada para el caso que el usuario que va a utilizar Webmin también tenga definido un usuario en el sistema. Si esta circunstancia no se produce es cómoda la gestión interna por parte de Webmin de los usuarios. De esta forma se tiene la certeza que un usuario que tenga acceso a Webmin para labores de monitorización no tendrá acceso directo al sistema. Se logra así aislar a este usuario.

Tras este breve paréntesis en el que se ha visto cómo gestionar el sistema de usuarios, continuemos con la creación del usuario. Si pulsamos sobre **Logout** en la esquina superior derecha, saldremos del sistema y podremos entrar de nuevo con el usuario que acabamos de crear.

Figura 3.11: Visión de Webmin del nuevo usuario

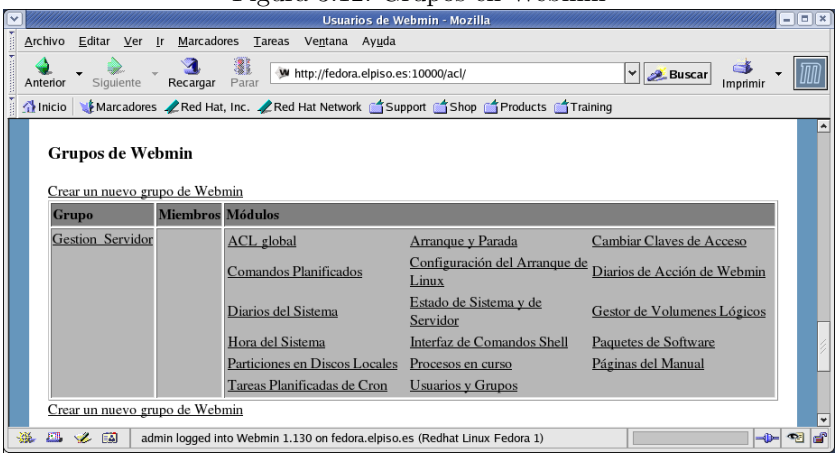


La visión obtenida ahora con este nuevo usuario no tiene nada que ver con la anterior, desde el punto de vista del usuario admin.

Pueden crearse tantos usuarios como sea necesario y asignarles los módulos que se estime necesarios para su labor de administración.

Al igual que ocurre en Linux, Webmin entiende el concepto de grupos. Los grupos en Webmin son similares a los de Linux y permiten simplificar la administración. Pueden crearse usuarios que tengan los mismos permisos y control de acceso. Cuando se crea un grupo en Webmin, se le asigna un nombre y se seleccionan los módulos a los que los miembros de este grupo tendrán acceso. Una vez creado el grupo, cualquier nuevo usuario podrá asignarse al grupo y automáticamente recibirá el acceso a los módulos del grupo, junto a los módulos a los que tenga acceso el usuario. En la implementación actual, un usuario únicamente puede pertenecer a un grupo, a diferencia de los grupos de Linux, en los que un usuario puede tener un grupo primario y varios grupos secundarios.

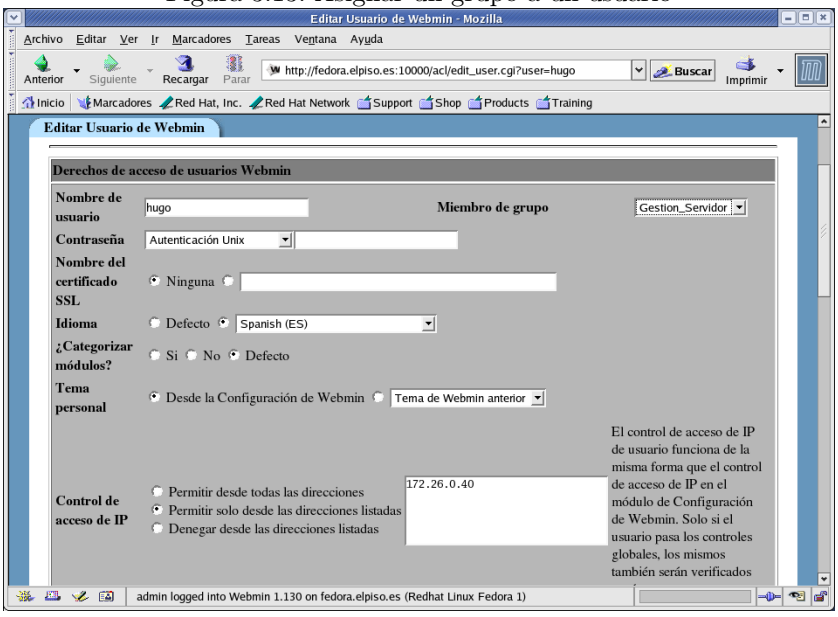
Figura 3.12: Grupos en Webmin



Hemos creado un grupo con acceso a todos los módulos relacionados con la administración general del sistema. De esta forma, cada vez que se cree un usuario para administrar un servicio concreto, es posible asignarle este grupo de administración general del servidor. Éste sería un ejemplo sencillo de uso de grupos en Webmin.

Es posible editar ahora el usuario recién creado anteriormente y asignarle el grupo que se acaba de crear.

Figura 3.13: Asignar un grupo a un usuario



3.6. Un ejemplo de configuración de servicio: Apache

3.6.1. Dónde configurar los servicios de nuestro sistema

Pulsando sobre la categoría SERVIDORES, se accede a una de las funcionalidades más interesantes de Webmin. Dentro de la categoría Servidores se encuentran los módulos encargados de la configuración de la mayoría de los servidores más utilizados.

El que un módulo esté instalado no quiere decir que el servicio que gestiona ese módulo esté instalado. Únicamente informa que existe soporte en Webmin para la configuración de un servicio. Es responsabilidad del administrador el tener instalado el servicio en el sistema.

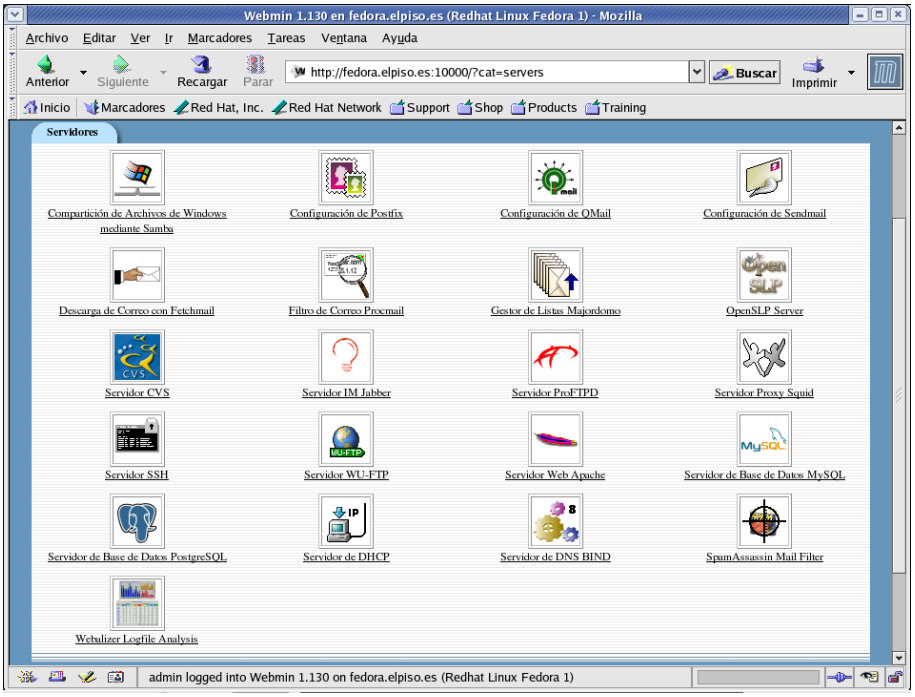
Una de las causas de la popularidad de Webmin es la posibilidad para el administrador de realizar algunas tareas de administración a través de Webmin, sin estar forzado a realizarlas todas. Además:

- a diferencia de otras herramientas gráficas de configuración para sistemas Linux, Webmin intenta dejar intacto el fichero editado.

- el hecho de configurar un servicio desde Webmin no quita que puedan editarse a mano los ficheros de configuración correspondientes.

Podrá utilizarse uno u otro método indistintamente, ya que una de las virtudes de Webmin es que no se dañarán las configuraciones hechas manualmente. Los comentarios y el orden de las directivas no son modificados por lo que no se producen conflictos entre ambos métodos.

Figura 3.14: Categoría Servidores



A continuación se verá uno de los módulos de configuración más utilizados. En concreto se verá qué funciones proporciona Webmin para configurar un servidor web. Pulsando sobre el icono de Apache se van editar los ficheros de configuración de Apache, normalmente[5] localizados en `/etc/httpd/conf`. La mayoría de los módulos de esta categoría pueden editar los ficheros de configuración bajo el directorio `/etc`.

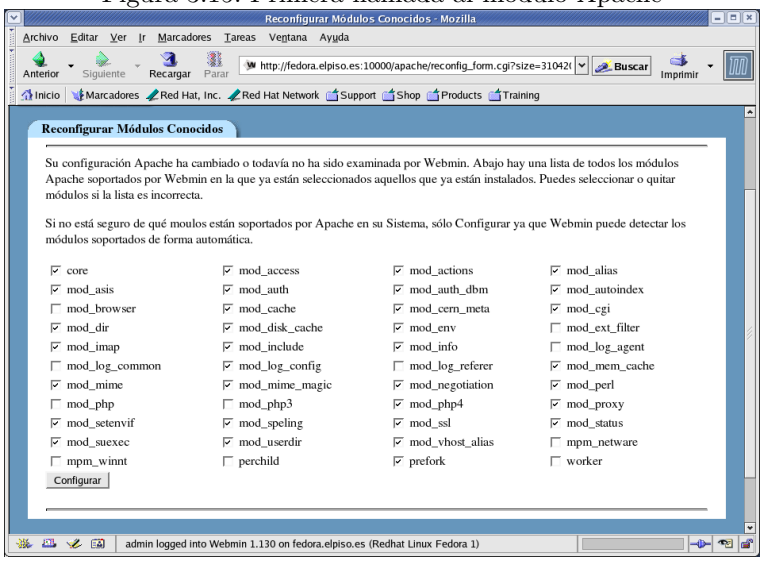
3.6.2. Módulo de configuración de Apache

El servicio que proporciona Apache es uno de los primeros que quiere verse en funcionamiento al instalar Linux. El módulo que proporciona Webmin es bastante completo y permite configurar Apache de la misma manera que manualmente, editando el fichero de configuración.

La primera vez que se ejecuta este módulo, Webmin detectará que anteriormente no se había ejecutado y preguntará por los módulos de Apache que hay instalados en el sistema. Al realizar una detección automática, en caso de duda, es recomendable aceptar la lista de módulos propuesta.

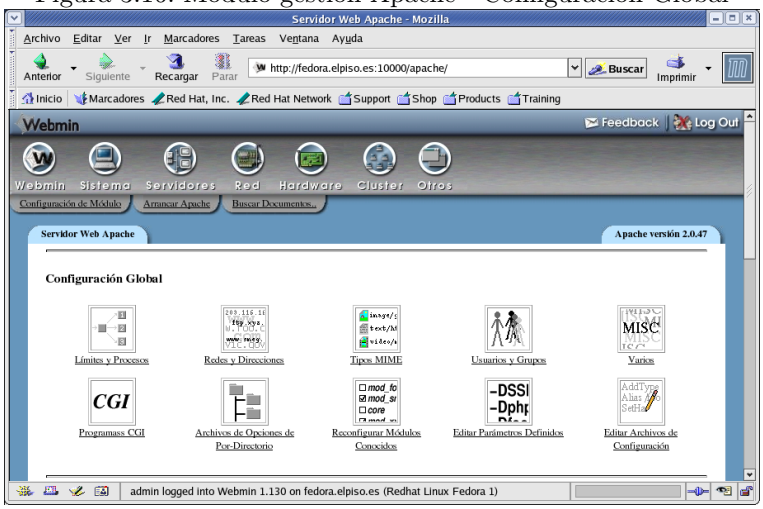
[5] En Debian: `/etc/apache2`

Figura 3.15: Primera llamada al módulo Apache



El módulo de gestión de Apache está dividido en varias secciones que cubren distintos aspectos de la configuración. En la página principal, estas secciones se agrupan en **Configuración Global** y **Servidores Virtuales**.

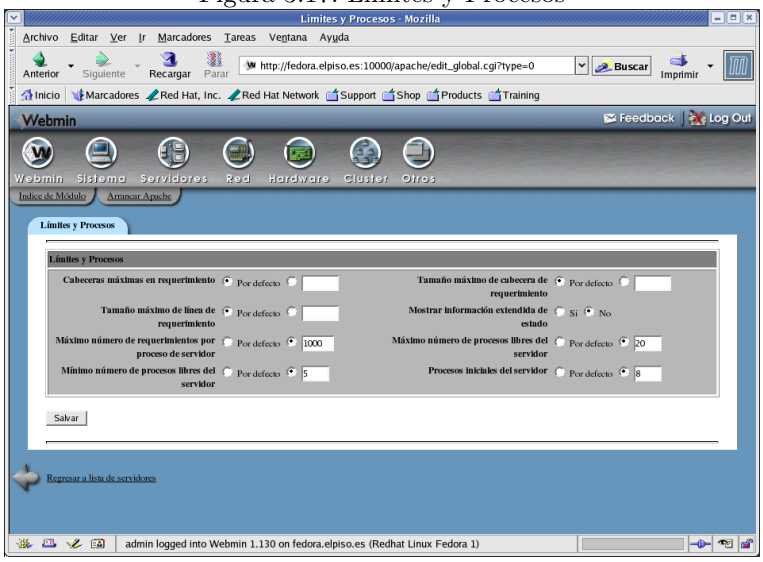
Figura 3.16: Módulo gestión Apache - Configuración Global



La **Configuración Global** proporciona acceso a las opciones que serán compartidas por todos los servidores virtuales que haya definidos. Las opciones configuradas aquí se aplicarán a todos los servidores virtuales y al servidor por defecto. Para configurar una opción para un servidor virtual específico, deberá configurarse en la sección **Servidores Virtuales**.

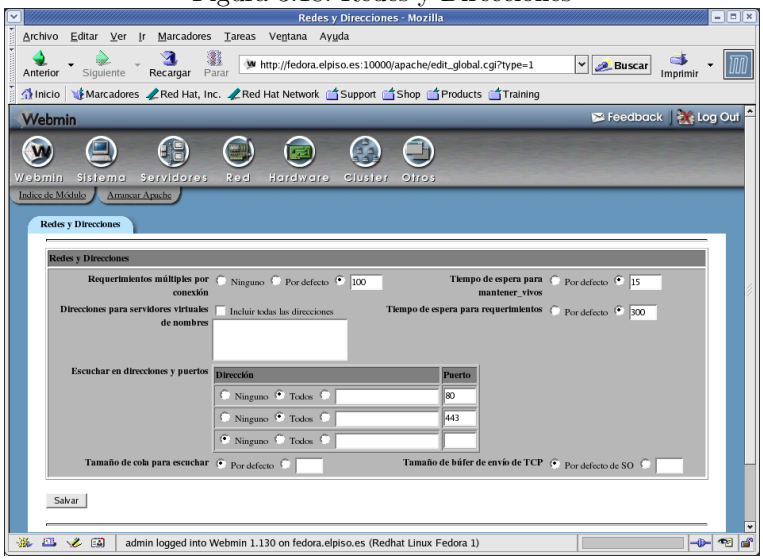
Límites y Procesos. Este módulo permite configurar algunos de los límites establecidos por defecto en Apache. El primer conjunto de límites es el relacionado con la longitud de las *request-headers* que serán aceptadas por el servidor. El segundo conjunto hace referencia a los límites de Apache en lo referente a conexiones y procesos.

Figura 3.17: Límites y Procesos



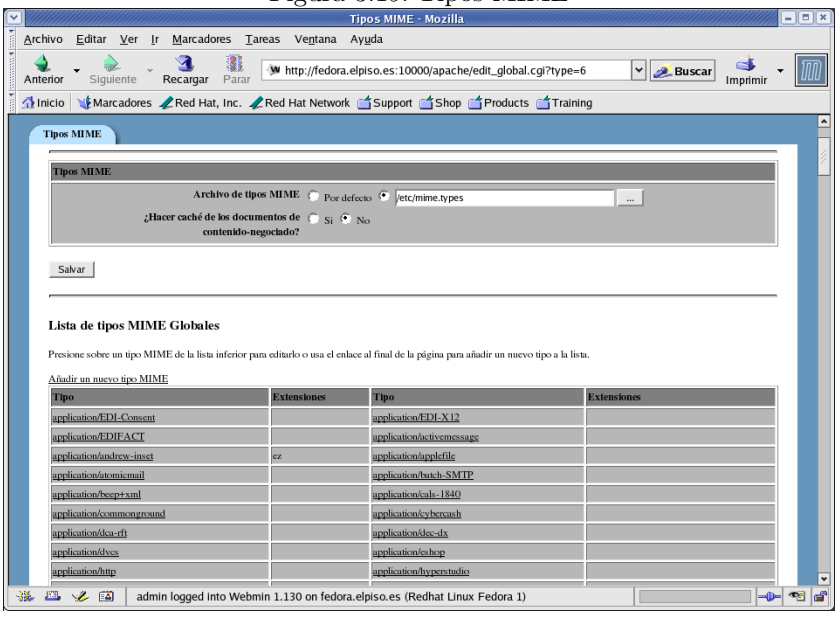
Redes y Direcciones. En este caso los parámetros disponibles son los relativos a las redes y puertos en los que puede configurarse Apache, así como algunos relativos a las conexiones.

Figura 3.18: Redes y Direcciones



Tipos MIME. Los tipos MIME proporcionan un método por el que el servidor y sus clientes conocerán el tipo de dato de un objeto determinado. Este módulo proporciona un mecanismo mediante el que podemos añadir nuevos tipos MIME a los ya definidos en Apache.

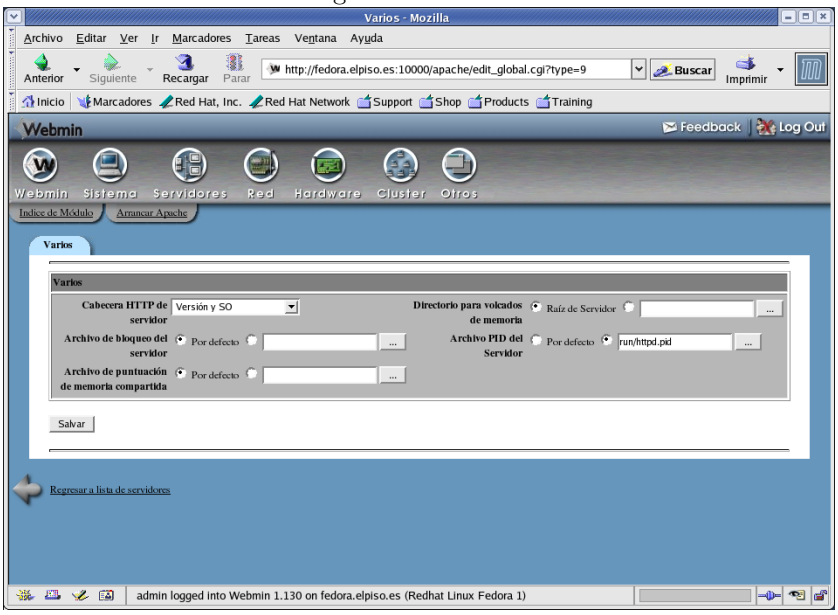
Figura 3.19: Tipos MIME



Usuarios y Grupos. Para cambiar el usuario y grupo bajo el cual se ejecutará Apache.

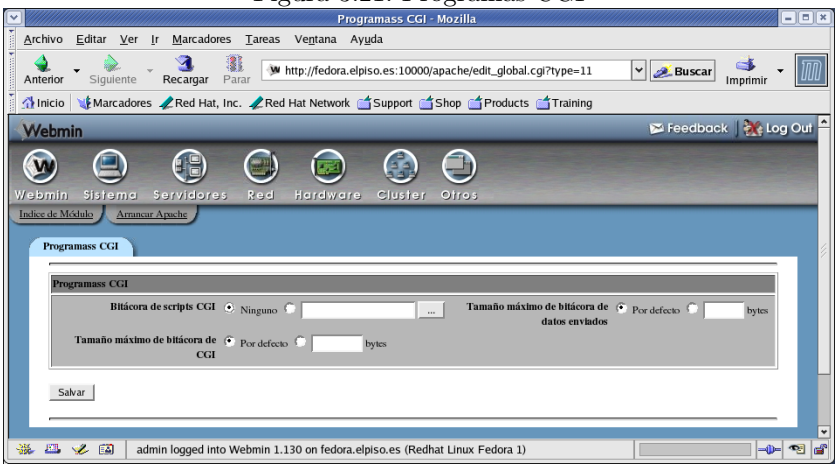
Varios. Como indica el nombre del módulo, aquí se configuran aspectos de Apache que no han sido incluidos en otros módulos.

Figura 3.20: Varios



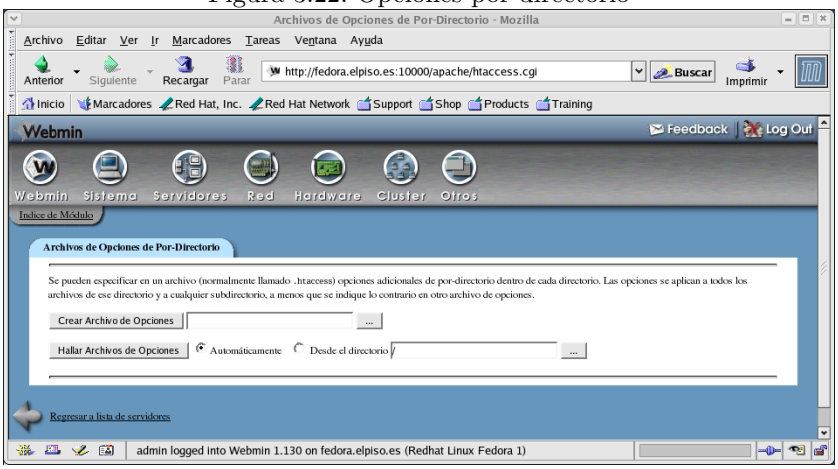
Programas CGI. Este módulo es un interfaz a las opciones de configuración global de los programas CGI en Apache.

Figura 3.21: Programas CGI



Archivo de Opciones de Por-Directorio. Las opciones adicionales de configuración para directorios específicos de la ruta del servidor web pueden realizarse mediante este módulo.

Figura 3.22: Opciones por-directorio

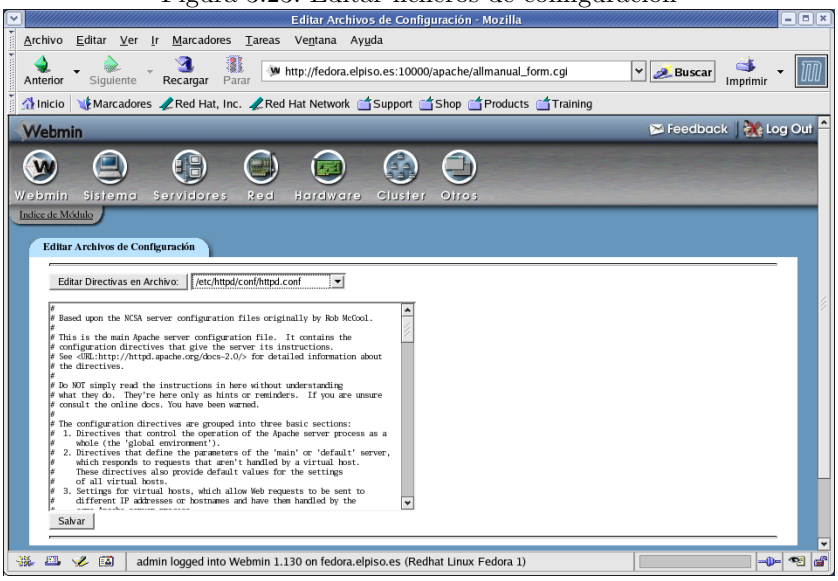


Reconfigurar Módulos Conocidos. Este módulo permite seleccionar los módulos que Apache va a arrancar en el servidor web. Este módulo se llama la primera vez que se accede a la configuración de Apache en Webmin.

Editar Parámetros Definidos. Mediante este módulo se cambia los parámetros con los que se arranca Apache.

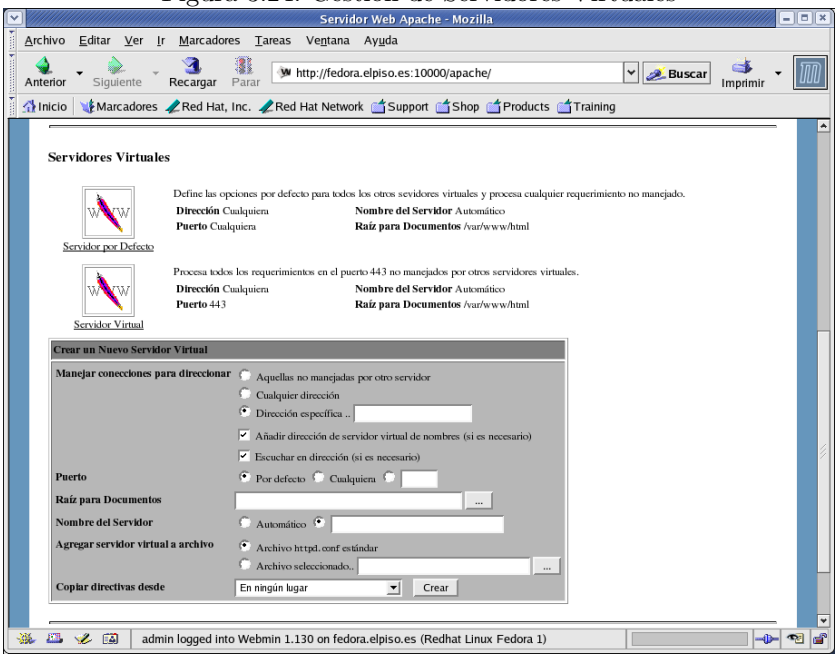
Editar Ficheros de Configuración. Si, a pesar de los módulos existentes, quiere editarse manualmente el fichero de configuración de Apache, también es posible hacerlo desde Webmin.

Figura 3.23: Editar ficheros de configuración



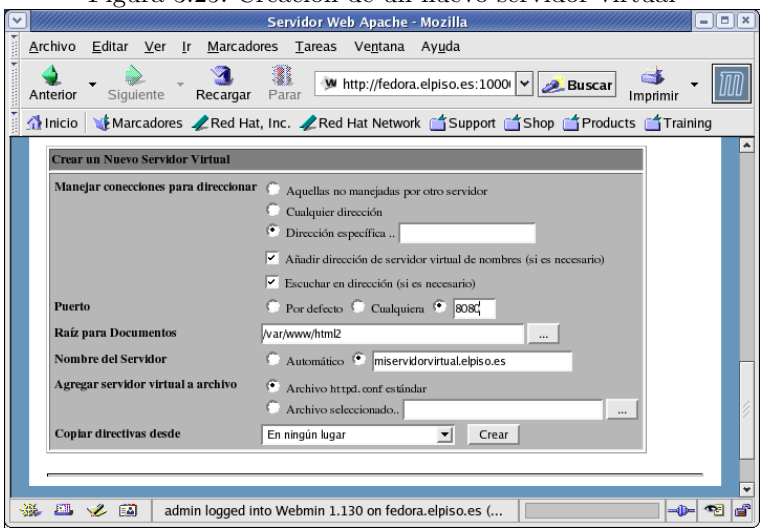
Gestión de servidores virtuales

Figura 3.24: Gestión de Servidores Virtuales



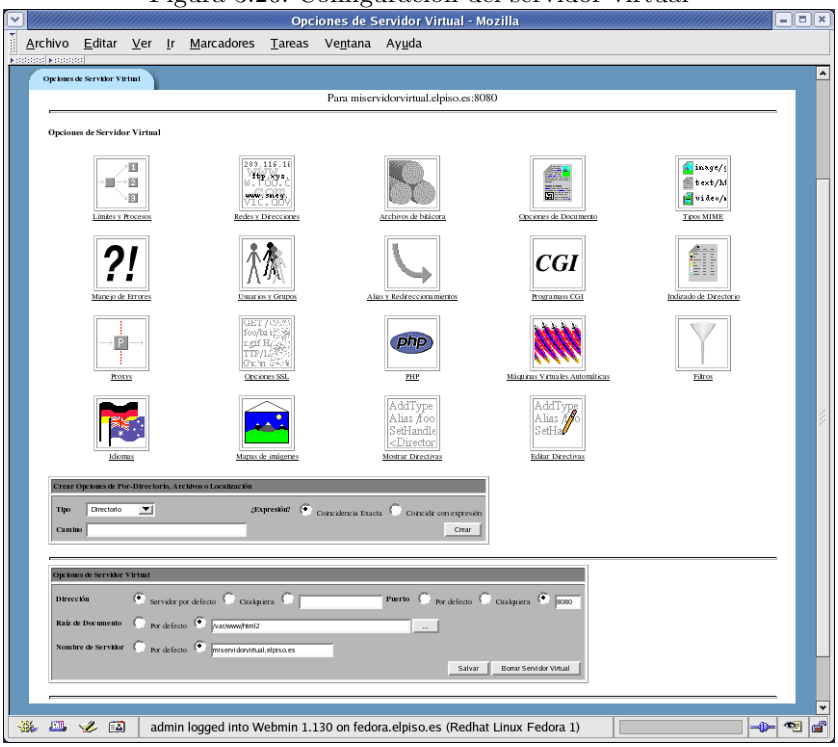
En el apartado referente a Apache ya se comentó algo al respecto de los servidores virtuales. Entremos en materia y veamos qué tendríamos que hacer para crear un nuevo servidor virtual. Supongamos que el nombre del nuevo servidor virtual será `miservidorvirtual.midominio.org` y estará a la escucha por el puerto 8080.

Figura 3.25: Creación de un nuevo servidor virtual



Con esta sencilla operación desde Webmin ya estaría configurado un nuevo servidor virtual. El siguiente paso sería personalizar la configuración del mismo. Para ello únicamente hay que pulsar sobre el icono correspondiente a `miservidorvirtual.midominio.org` que aparece en la pantalla principal del módulo Apache.

Figura 3.26: Configuración del servidor virtual



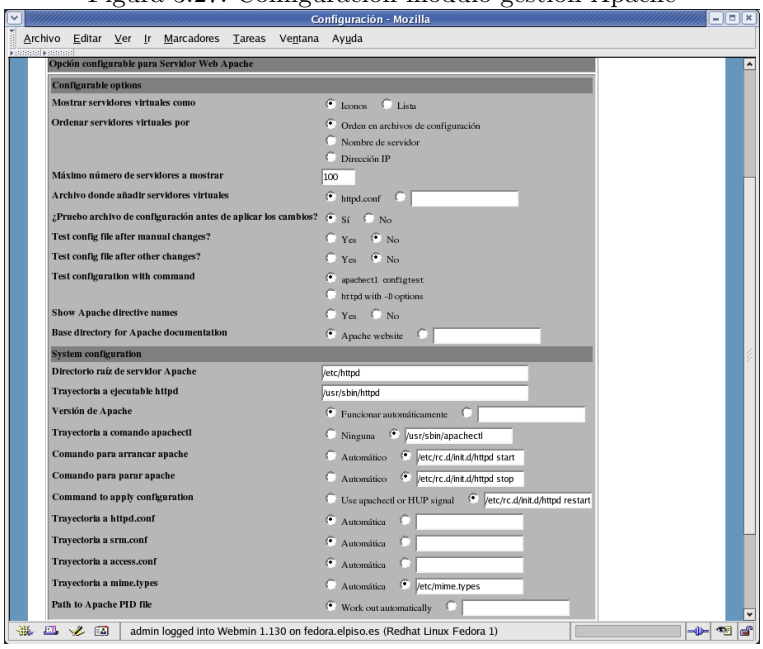
3.6.3. Consideraciones finales

La configuración desde Webmin de Apache puede comprobarse que es bastante sencilla, pero hay que tener en cuenta que son necesarios conocimientos previos sobre el servicio que se desea

configurar.

Hasta ahora se ha tratado de la configuración del servicio que proporciona Apache, pero es posible configurar este módulo de Webmin para modificar su comportamiento.

Figura 3.27: Configuración módulo gestión Apache



También es útil en este caso el uso de la funcionalidad tratada anteriormente **Clonar Módulos**. Normalmente no es necesario ejecutar más de un demonio `httpd` en el mismo servidor, pero en el caso que fuera necesario podemos utilizar la funcionalidad de clonar módulos.

3.7. Gestión de varios servidores Webmin

Dentro de la categoría Webmin existe un módulo denominado **Indice de Servidores Webmin**. Esta página nos da acceso a la lista de servidores Webmin existentes en la red local donde se encuentra instalado. Pulsando sobre el icono de cualquiera de los servidores Webmin que se defina se accede a la pantalla de login de dicho servidor Webmin.

Para añadir nuevos servidores Webmin de forma automática se habilitan los siguientes procedimientos:

Retransmisión para servidores. Hace que Webmin envíe una petición de broadcast al puerto 10000 de nuestra red local. Cualquier servidor Webmin existente en nuestra red responderá identificándose a sí mismo. De esta forma Webmin lo añade a la lista de servidores.

Explorar por servidores. También podemos especificar la red en la que queremos realizar la búsqueda de servidores Webmin.

Existe también la opción de añadir los servidores Webmin de forma manual.

Capítulo 4

Monitorización de Sistemas

4.1. Nagios

4.1.1. ¿Qué es Nagios?

Nagios es un sistema de monitorización de redes y servidores. Chequea de forma periódica los nodos y los servicios que se especifiquen a través de la red, alertando cuando se superan los indicadores definidos y cuando se vuelve de nuevo a una situación estable. Su gran versatilidad permite a Nagios monitorizar prácticamente cualquier cosa que esté en la red.

Originalmente fue diseñado para ejecutarse bajo sistemas Linux, aunque en la actualidad es posible su instalación en otros sistemas. Algunas de las características que incluye Nagios son:

- Monitorización de servicios (SMTP, POP3, HTTP, NNTP, PING, etc.).
- Monitorización de recursos del nodo (carga de procesador, uso de disco, etc).
- Posibilidad de creación de plugin personalizados que permiten el chequeo de servicios o parámetros no contemplados.
- Chequeo de los servicios de forma paralelizada.
- Notificaciones a los responsables cuando cambia el estado del sistema.
- Posibilidad de definir controles proactivos como respuesta a un estado.
- Rotado de log de forma automática.
- Interfaz web para visualizar el estado actual de los controles definidos.

4.1.2. Instalación de Nagios

Guadalinex

```
apt-get install nagios-text
```

Fedora

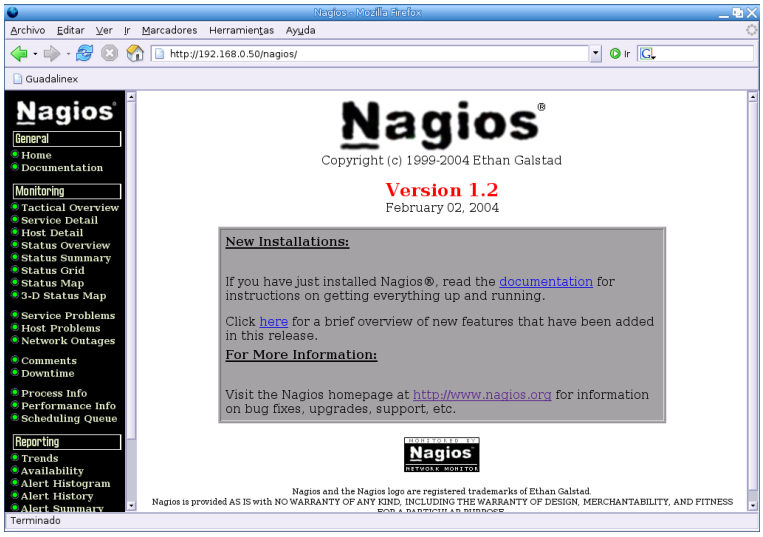
La podemos bajar, por ejemplo, de `http://www.nagios.org/download/` e instalarlos con

```
rpm -i nagios*
```

Durante la instalación será necesario indicarle el tipo de servidor web que se utilizará. También se solicitará la contraseña para acceder con el usuario `nagiosadmin` a la monitorización.

Finalizado el proceso de instalación únicamente hay que iniciar el servicio de Nagios con el script `/etc/init.d/nagios start` y acceder a la consola web de monitorización (`http://localhost/nagios`).

Figura 4.1: Pantalla inicial de Nagios



Tendremos que autenticarnos como usuario `nagiosadmin` y password la establecida en el proceso de instalación.

No será necesario modificar los ficheros principales de configuración de Nagios `/etc/nagios/nagios.cfg` y `/etc/nagios/cgi.cfg`.

4.1.3. Configuración de Nagios

La configuración de Nagios se basa en la definición de una serie de objetos. Mediante estos objetos se definirán los hosts, servicios, grupos de host, contactos, grupos de contactos, comandos, etc. Con estos elementos se define qué es lo que quiere monitorizarse y cómo quiere monitorizarse.

Servicios

Se refiere a los servicios que se van a monitorizar (SMTP, FTP, HTTP, ...) en los distintos servidores de la red. También entran en esta definición cualquier tipo de valor o métrica a aplicar sobre una medida realizada sobre un servicio. Junto con un servicio se define también el equipo que proporciona este servicio. El fichero que almacena la configuración de los servicios es `/etc/nagios/services.cfg`.

Algunos de los parámetros que definen un servicio en Nagios:

- `service_description`
- `host_name`
- `check_period`
- `contact_groups`
- `notification_options`
- `check_command`

Equipos

En el fichero `/etc/nagios/hosts.cfg` se incluirán todos los servidores que se van a monitorizar. Cada servidor tendrá al menos un servicio asociado, que será el que se monitorice.

Algunos de los parámetros que definen un equipo en Nagios:

- `host_name`
- `alias`
- `address`
- `check_command`

Grupos de equipos

Los grupos de equipos son conjuntos de equipos que tienen algo en común y que se agrupan para facilitar la administración. El fichero `/etc/nagios/hostgroups.cfg` define estos conjuntos de equipos. Relacionado con este concepto está los grupos de contactos.

Un equipo siempre pertenece a un grupo, siendo posible que un mismo equipo pertenezca a varios grupos.

Algunos de los parámetros que definen a un grupo de equipos en Nagios:

- `hostgroup_name`
- `alias`
- `contact_groups`
- `members`

Contactos

El fichero `/etc/nagios/contacts.cfg` define las personas, a través de las direcciones de correo electrónico, a las cuales se van a enviar las notificaciones que genera Nagios. Normalmente serán los responsables de los equipos o los encargados de su administración. Junto a la definición del contacto se definen también las condiciones en que la notificación se hará efectiva.

Algunos de los parámetros que definen a un contacto en Nagios:

- `contact_name`
- `alias`
- `host_notification_period`
- `service_notification_period`
- `service_notification_commands`
- `host_notification_commands`

Grupos de contactos

Al igual que ocurre con los equipos y los grupos de equipos, un contacto tiene que pertenecer a un grupo de contactos. Un grupo de contactos es un conjunto de personas (contactos) que se agrupan a la hora de recibir notificaciones. La configuración de un grupo de contactos se define en `/etc/nagios/contactgroups.cfg`.

Algunos de los parámetros que definen a un grupo de contactos en Nagios:

- `contactgroup_name`
- `alias`
- `members`

Comandos

Un comando es una tarea utilizada para chequear el estado de un servicio o de un aspecto concreto de un servidor. Se especifica la línea de comando y a partir de este momento se puede hacer referencia a este comando desde Nagios. Esto permite añadir nuevas funcionalidades a Nagios simplemente creando nuevos comandos. Los comandos se declaran en los ficheros `/etc/nagios/misccommands.cfg` y `/etc/nagios/checkcommands.cfg`

Algunos de los parámetros que definen a un comando en Nagios:

- `command_name`
- `command_line`

Periodos de tiempo

Se define un periodo de tiempo como un rango horario que se asigna para cada día de la semana. Este periodo de tiempo que se ha creado se puede asignar a una tarea concreta y formando así una planificación. Lo normal es definir el horario laboral para cada día de la semana y utilizarlo para el envío de notificaciones, de forma que solo se avise de un determinado problema si se produce en dicho intervalo de tiempo. La configuración de los periodos de tiempo se realiza en el fichero `/etc/nagios/timeperiods.cfg`.

Algunos de los parámetros que definen a un periodo de tiempo en Nagios:

- `timeperiod_name`
- `alias`
- `monday`, `tuesday`, `wednesday`, `thursday`, `friday`, `saturday`, `sunday`

4.1.4. Monitorizar un nuevo host

La configuración por defecto aparece con un nodo denominado `gw` y que se corresponde con el *gateway*. La mejor forma de comprender el funcionamiento de Nagios es añadir un nuevo nodo.

Es necesario añadir la definición del nuevo nodo a `/etc/nagios/hosts.cfg`. Por ejemplo, si nuestra IP es 192.168.0.50, quedaría

```
# 'guadalinex'
define host{
    use                     generic-host    ; Name of host template to use
    host_name               guadalinex
    alias                   Servidor Guadalinex
    address                 192.168.0.50
    check_command           check-host-alive
    max_check_attempts      10
    notification_interval   480
    notification_period     24x7
    notification_options    d,u,r
    }
```

A continuación se modifica el fichero `/etc/nagios/hostgroups.cfg`

```
# Definicion del grupo de nuestros servidores
define hostgroup{
        hostgroup_name  servidores
        alias           Servidores Linux
        contact_groups  linux-admin
        members         guadalinex
        }
```

Se modifica el fichero `/etc/nagios/contactgroups.cfg`

```
# 'linux-admin' contact group definition
define contactgroup{
        contactgroup_name       linux-admin
        alias                   Administradores Linux
        members                 administradores
        }
```

Se modifica el fichero `/etc/nagios/contacts.cfg`

```
# 'administradores' contact definition
define contact{
        contact_name                    administradores
        alias                           Administradores Linux
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,u,r
        service_notification_commands   notify-by-email
        host_notification_commands      host-notify-by-email
        email                           hugo@midominio.org
        }
```

Se modifica el fichero `/etc/nagios/services.cfg`

```
define service{
        use                             generic-service         ; Name of
            service template to use
        host_name                       guadalinex
        service_description             PING
        is_volatile                     0
        check_period                    24x7
        max_check_attempts              3
        normal_check_interval           5
        retry_check_interval            1
        contact_groups                  linux-admin
        notification_interval           240
        notification_period             24x7
        notification_options            c,r
        check_command                   check_ping!100.0,20%!500.0,60%
        }
```

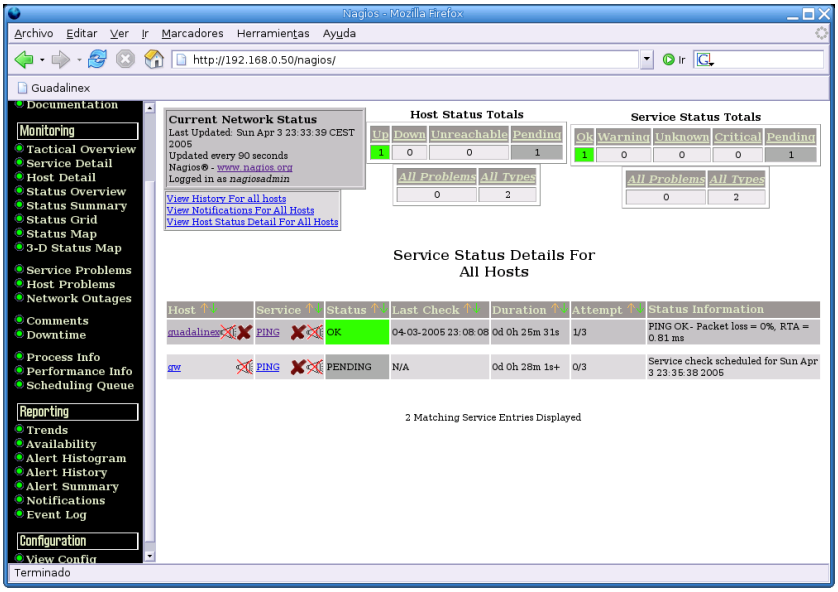
Una vez realizadas estas modificaciones:

```
root@guadalinex:~# /usr/sbin/nagios -v /etc/nagios/nagios.cfg
Nagios 1.2
Copyright (c) 1999-2004 Ethan Galstad (nagios@nagios.org)
Last Modified: 02-02-2004
License: GPL
Reading configuration data...
Running pre-flight check on configuration data...
Checking services...
        Checked 2 services.
Checking hosts...
        Checked 2 hosts.
Checking host groups...
        Checked 2 host groups.
Checking contacts...
```

```
        Checked 2 contacts.
Checking contact groups...
        Checked 2 contact groups.
Checking service escalations...
        Checked 1 service escalations.
Checking host group escalations...
        Checked 0 host group escalations.
Checking service dependencies...
        Checked 0 service dependencies.
Checking host escalations...
        Checked 0 host escalations.
Checking host dependencies...
        Checked 0 host dependencies.
Checking commands...
        Checked 88 commands.
Checking time periods...
        Checked 4 time periods.
Checking for circular paths between hosts...
Checking for circular service execution dependencies...
Checking global event handlers...
Checking obsessive compulsive service processor command...
Checking misc settings...
Total Warnings: 0
Total Errors:   0
Things look okay - No serious problems were detected during the pre-flight
    check
```

Para que la nueva configuración tome efecto es necesario reiniciar el servicio mediante la línea `/etc/init.d/nagios reload`. Una vez cargada la nueva configuración puede chequearse el estado del servicio a través del navegador, pulsando sobre SERVICE DETAILS:

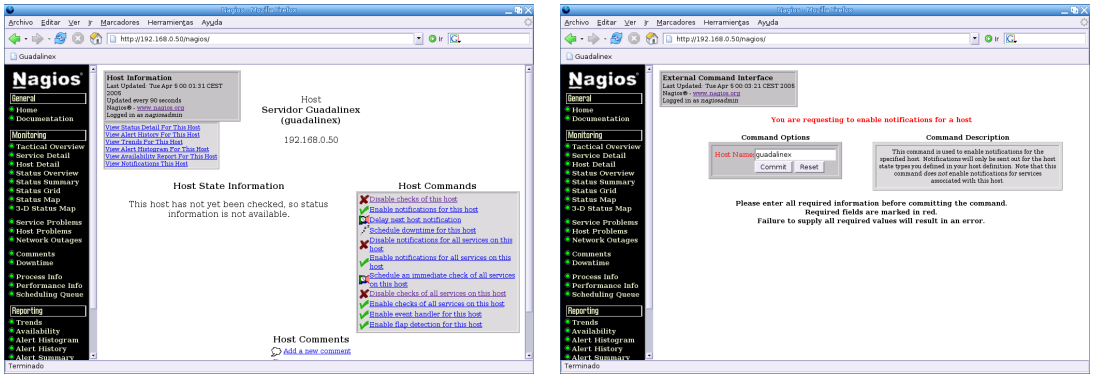
Figura 4.2: Monitorizar el nuevo host



Aquí no acaba el trabajo, existe un nuevo nodo definido en Nagios. Es necesario habilitar los chequeos y las notificaciones para este nodo, que aparecen deshabilitados (marca de color rojo

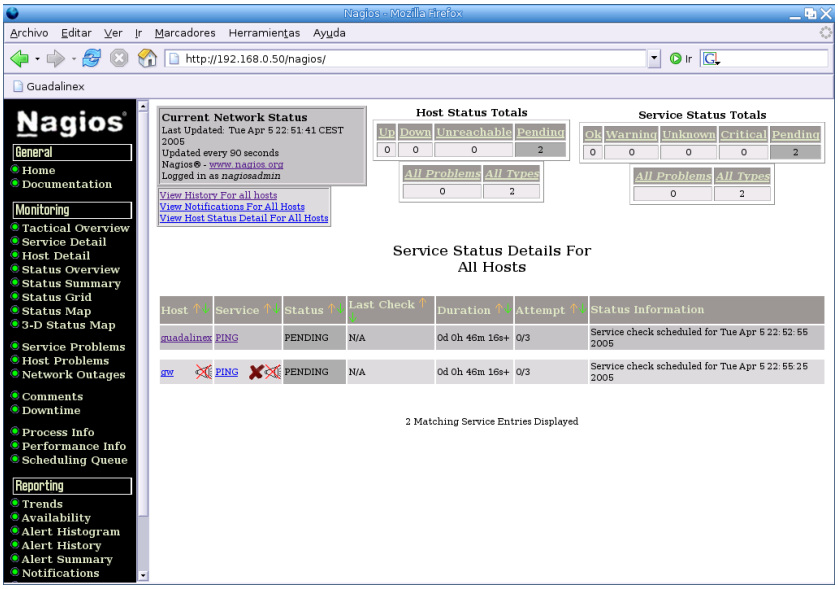
y altavoz tachado) en la consola web. Pulsando sobre el nombre del nuevo nodo, guadalinex, aparecen las propiedades del nodo y se permite habilitar todos los chequeos del nodo, de los servicios asociados al nodo y de las notificaciones. También se pueden habilitar los chequeos y notificaciones pulsando directamente sobre los símbolos.

Figura 4.3: Habilitar chequeos y notificaciones



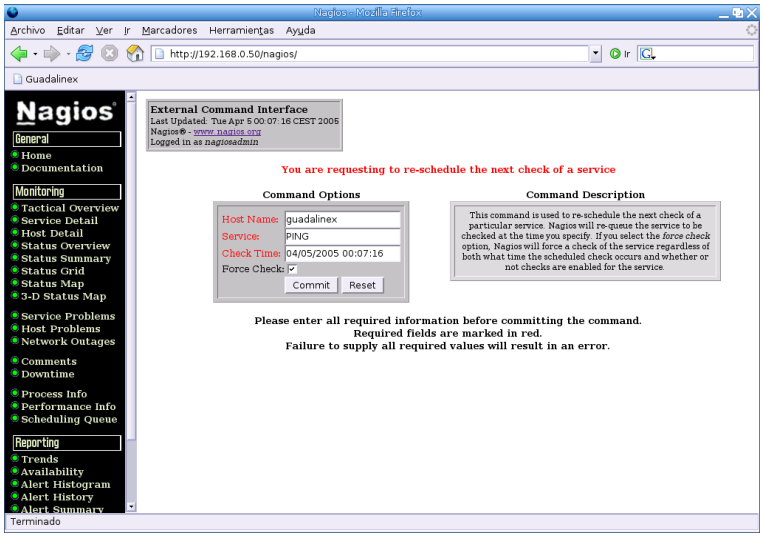
Una vez habilitados, desaparecen los indicadores anteriores.

Figura 4.4: Chequeos y notificaciones habilitados



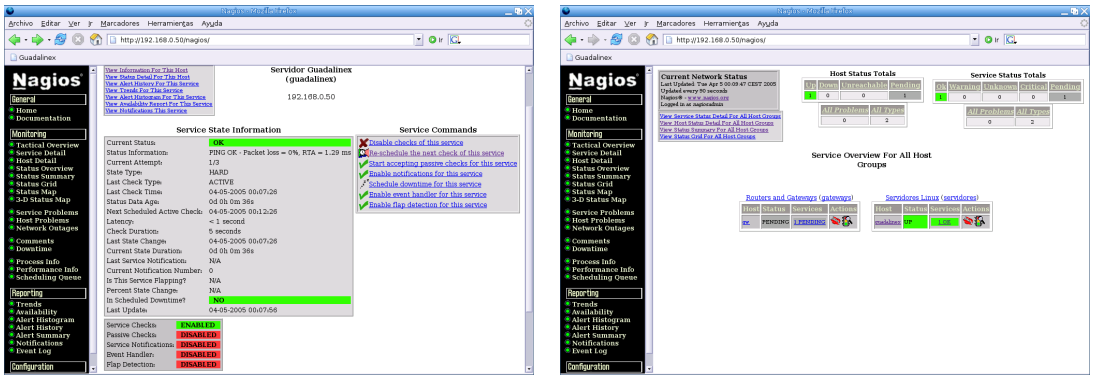
Por último, solo queda empezar a monitorizar el sistema. Si no queremos esperar a que se produzca el primer chequeo de forma automática, es posible forzarlo.

Figura 4.5: Forzar chequeo de un servicio



Una vez chequeado, Nagios mostrará el estado del servicio.

Figura 4.6: Estado de servicio OK



4.2. Monitorización de redes con ntop

Network top (`ntop`) es un software que nos permite monitorizar el tráfico de la red, con una gran potencia debido al gran número de protocolos que soporta. La utilidad `ntop` nos permite realizar un análisis de todo el tráfico que pasa a través de nuestro interfaz, por defecto el eth0. Si queremos sacar el máximo rendimiento a esta herramienta un buen sitio para hacerla funcionar es en una máquina por donde pase casi todo el tráfico de nuestra red: un cortafuegos o un proxy. Cuanto mayor porcentaje del tráfico de nuestra red pase por el interfaz o interfaces monitorizados por `ntop`, mayor y más real será la información.

Anteriormente hemos visto algún software de monitorización pero éstos no nos proporcionaban determinadas características que nos da `ntop`, por ejemplo: modelo de los equipos y S.O., trafico acumulado entre dos equipos, equipos que generan mayor cantidad de tráfico,...

Es fácil de instalar y de usar, ya que es vía web y se le pueden incorporar otras herramientas como el `rrdtools` para la generación de gráficas que facilitan la obtención de resultados.

4.2.1. Instalación

Para la instalación de `ntop` vamos a utilizar Guadalinex 2004[1], de tal forma que es suficiente con:

```
root@Gestion:~# apt-get install ntop
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
ntop
0 actualizados, 1 se instalarán, 0 para eliminar y 126 no actualizados.
3 no instalados del todo o eliminados.
Necesito descargar 2402kB de archivos.
Se utilizarán 6525kB de espacio de disco adicional después de desempaquetar.
Des:1 http://http.guadalinex.org sarge/main ntop 2:3.0-3 [2402kB]
Descargados 2402kB en 45s (53,3kB/s)
Preconfiguring packages ...
```

A continuación nos aparece el asistente de configuración:

Figura 4.7: Configuración de ntop

(a) Interfaz de red (b) Usuario

Elegimos el interfaz por el que monitorizar y a continuación seleccionamos el usuario para ejecutar `ntop`.

Así se configurará de forma automática el *Network top* y todos aquellos paquetes de los que dependa (libgd2, apache2,...).

Una vez instalado y antes de arrancarlo debemos establecer la contraseña del usuario admin, para esto utilizaremos el comando `ntop -A`. Con esta opción nos pedirá introducir dicha contraseña y una vez realizado podremos arrancar el demonio con `/etc/init.d/ntop start`.

Ntop tiene su propio servicio http y https, por defecto se habilita el primero en el puerto 3000, si queremos habilitar otro puerto para http utilizaremos la opción `-w puerto` y si queremos habilitar el https utilizaremos la opción `-W puerto`. Para que estas opciones las tome al arrancar el demonio de ntop debemos editar el fichero `/etc/default/ntop` y descomentar el parámetro `OPTGET` y darle los valores que queramos, por ejemplo `OPTGET=" -w 2000 -WWW 2002`".

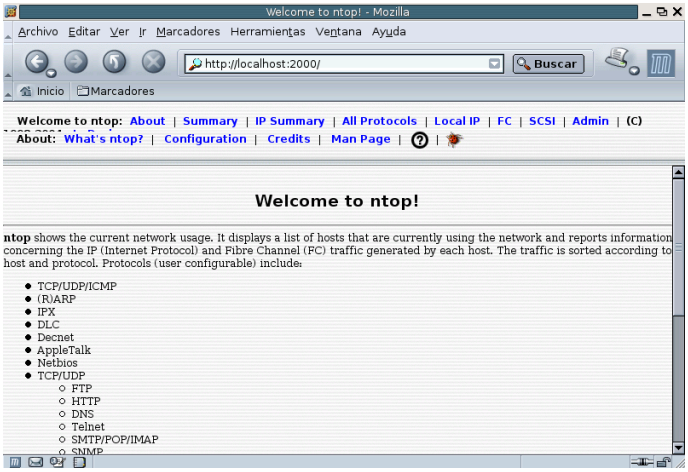
Con esto podemos empezar a trabajar con `ntop` mediante un navegador y podemos acceder al manual html para ver el resto de diferentes opciones.

[1]El paquete rpm para Fedora lo podemos bajar desde:
`http://www.ntop.org/ntop.html`

4.2.2. Datos en ntop

Una vez arrancado el demonio de `ntop`, podemos ver los primeros resultados directamente[2] en la url `http://localhost:2000`.

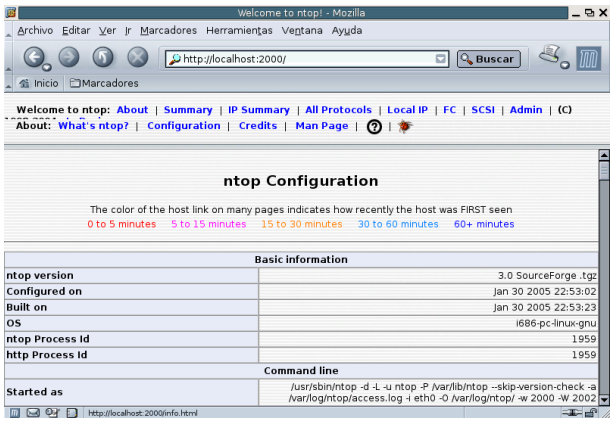
Figura 4.8: Inicio de ntop



En la pantalla de bienvenida, y según la distribución que estemos utilizando, nos aparecerá un menú con los distintos apartados en los que podemos entrar:

About: Muestra una explicación del programa, la configuración de ntop, los créditos y el manual en formato html.

Figura 4.9: Usando ntop -About



Summary: Nos muestra un resumen de las estadísticas obtenidas de forma global. Muestra los diferentes tipos de tráfico y sus carácterísticas, lista todos los equipos y el ancho de banda utilizado, la carga de la red y otras características como las vlans.

[2] Si no hemos cambiado los puertos será `http://localhost:3000`

Figura 4.11: Usando ntop - IP Summary

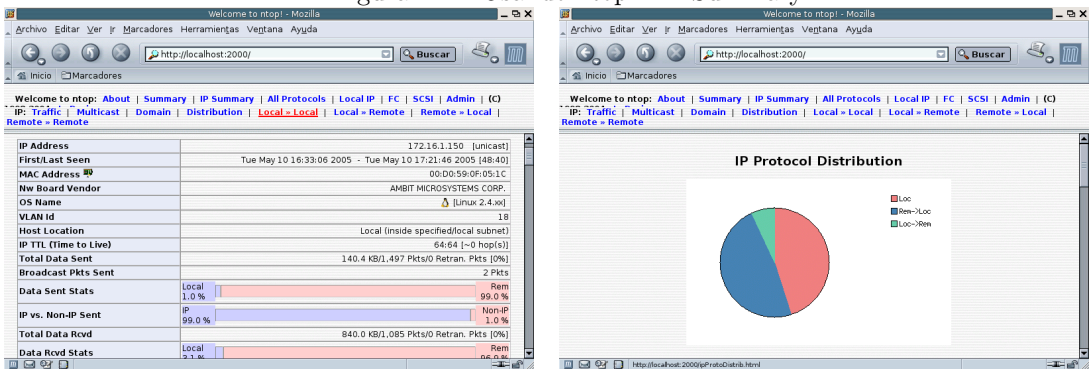
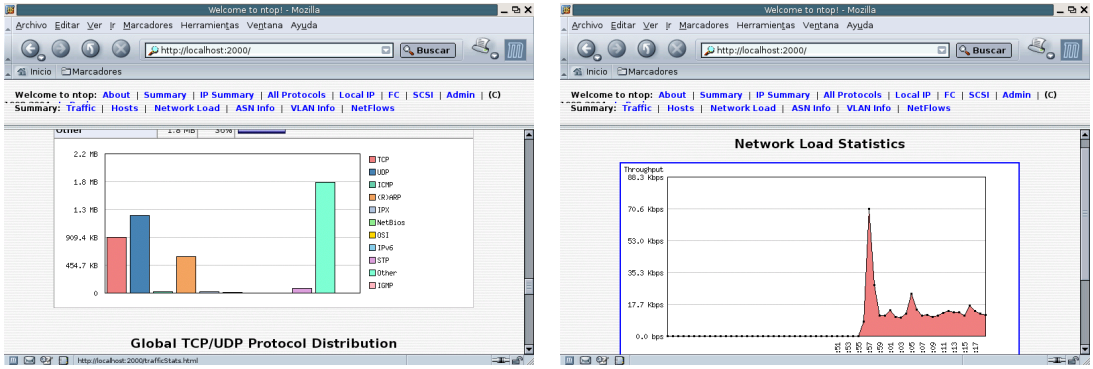


Figura 4.10: Usando ntop - Summary



IP Sumary Podemos obtener el tipo de tráfico cursado por cada host y acceder a la información del equipo. Nos permite ver las estadísticas distinguiendo entre tráfico local y remoto.

All Protocols En este apartado encontramos estadísticas de paquetes enviados y recibidos, así como una distribución de la actividad por franja horaria.

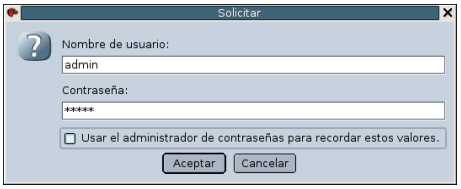
Local IP En este apartado se muestran diferentes cuadros comparativos de puertos utilizados por clientes y servidores, los sistemas operativos usados por las máquinas, los servicios de cada máquina o un cuadro con el tráfico entre máquinas.

FC Muestra los datos de las interfaces Fibre Channel.

SCSI Muestra los datos de las conexiones SCSI.

Admin Nos permite gestionar `ntop` vía web. Utilizando la primera vez el usuario admin con la contraseña inicial podemos dar de alta nuevos usuarios, crear nuevos filtros, añadir y configurar plugins, resetear las estadísticas, cambiar el interface e incluso parar el servicio.

Figura 4.12: Usando ntop - Admin



Estos apartados descritos anteriormente se corresponden con la distribución de Guadalinex 2004, en otras distribuciones la presentación de los menús puede variar un poco pero los datos siguen siendo los mismos. Como siempre lo mejor es instalarlo, ponerlo en funcionamiento e ir viendo el partido que podemos sacarle. Seguro que gran parte de la información nos puede resultar de bastante utilidad, sobre todo si tenemos que detectar máquinas que generen grandes cantidades de tráfico o tráfico no deseado.

Bibliografía

[1] *Securing and Optimizing Linux: The ultimate solution.* Gerhard Mourani

[2] *A brief tutorial on dump and restore.* http://www.nethamilton.net/docs/

[3] *Página oficial de AMANDA.* http://www.amanda.org/

[4] *Backups en disco duro con AMANDA* http://www.kleenux.org/articulos/amanda-tapeless/amanda-tapeless.html

[5] *Administración de sistemas Linux.* Dee-Ann LeBlanc

[6] *Seguridad Pactica en UNIX e Internet.* Simson Garfinkel y Gene Spafford

[7] *System Administation with Webmin.* Joe Cooper

[8] Página oficial de Nagios. http://www.nagios.org/

[9] Página oficial de ntop. http://www.ntop.org/