

Introducción

En esta práctica vamos a eventos de dos maneras:

- Con Webmin, siguiendo este tutorial:

[Administrar eventos de Ubuntu 18.04 LTS con Webmin - SomeBooks.es](#)

- Con logcheck

[Recibir informes sobre sucesos de Ubuntu Server 20.04 LTS con Logcheck - SomeBooks.es](#)

Administrar eventos de Ubuntu con Webmin

Ya sabemos que cualquier incidencia, o cualquier funcionamiento anómalo del sistema queda anotado en los archivos de registro dentro del directorio `/var/log`. Además, como su número puede ser considerable, en ocasiones estos archivos se organizan en subdirectorios. Con tanto archivo, realizar un seguimiento manual de los eventos que se vayan produciendo puede ser algo complicado. Podemos emplear la herramienta de administración remota llamada Cockpit, o también Webmin. Con Webmin podemos realizar casi cualquier tarea administrativa de forma remota, y puede ser más cómodo el centralizarlo todo en la misma herramienta.

Comenzamos conectándonos a Webmin-> categoría Sistema en el panel izquierdo->clic sobre Históricos (logs) del sistema. Mostrará la página con todos los archivos de eventos reconocidos en este momento. Para cada archivo, podremos comprobar si se encuentra activo en estos momentos y las preferencias que tiene almacenadas. Para consultar los eventos que contiene un archivo, basta con hacer clic sobre su botón Ver. Podemos elegir el nº de líneas que queremos ver (en el ej. 100), una lista desplegable, para elegir un archivo diferente y un cuadro de texto, con el título Mostrar sólo las líneas que contengan el texto, donde podremos escribir una parte del mensaje de error que nos interesa y filtrar por él.



Log destination	Active?	Messages selected
File /var/log/auth.log	Yes	auth,authpriv.* View
File /var/log/syslog	Yes	*.*; auth,authpriv.none View
File /var/log/cron.log	No	cron.*
File /var/log/daemon.log	No	daemon.*
File /var/log/kern.log	Yes	kern.* View
File /var/log/lpr.log	No	lpr.*
File /var/log/mail.log	Yes	mail.* View
File /var/log/user.log	No	user.*
File /var/log/mail.info	No	mail.info
File /var/log/mail.warn	No	mail.warn
File /var/log/mail.err	Yes	mail.err View
File /var/log/debug	No	news.none; mail.none
File /var/log/messages	No	mail,news.none
Users :omusrmsg:*	Yes	*.emerg

Consultar los eventos de un archivo

Puede pasar desapercibido es que el botón Refrescar es, en realidad, una lista desplegable. Si la desplegamos, comprobaremos que dispone de diferentes valores de tiempo (5 segundos, 15 segundos, etc). Si queremos dejarlo como estaba (actualización manual), basta con elegir la opción Automatic refresh: Off. Por último, en la parte inferior de la pantalla, tenemos dos botones más:

- Regresar a detalles de diario: Para editar el archivo de registro del que estamos viendo el contenido.
- Regresar a diarios de sistema: Para volver a la página principal de Diarios del sistema.

a) Adjunta captura de pantalla mostrando los eventos del archivo auth.log. El archivo auth.log almacena los eventos relacionados con la seguridad y las autorizaciones. Dile que muestre solo las últimas 30 líneas y los eventos que hagan referencia a SSH.

The screenshot shows the Systemd Journal interface with the following settings: 'Last' 30 lines of 'All messages', 'since' 'Latest available', and 'Filter lines with text' 'ssh'. The filtered log entries are as follows:

```

Jan 31 12:35:15 ip-172-31-91-158 systemd[1316]: Closed gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Jan 31 12:35:15 ip-172-31-91-158 systemd[1316]: Stopping gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation)...
Jan 31 12:35:15 ip-172-31-91-158 systemd[1316]: Closed gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Jan 31 12:35:05 ip-172-31-91-158 systemd[1316]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation)...
Jan 31 12:35:05 ip-172-31-91-158 systemd[1316]: Starting gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation)...
Jan 31 12:35:05 ip-172-31-91-158 systemd[1316]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Jan 31 12:31:51 ip-172-31-91-158 systemd[950]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Jan 31 12:31:51 ip-172-31-91-158 systemd[950]: Starting gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation)...
Jan 31 12:31:51 ip-172-31-91-158 systemd[950]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Jan 31 12:31:51 ip-172-31-91-158 sshd[945]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Jan 31 12:31:51 ip-172-31-91-158 sshd[945]: Accepted publickey for ubuntu from 217.217.36.194 port 57243 ssh2: RSA SHA256:2Sau1/yTy4/BFpawapIj82xNecQ2vQLdc1QAEgMyUzo
Jan 31 12:30:18 ip-172-31-91-158 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jan 31 12:30:18 ip-172-31-91-158 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 31 12:29:50 ip-172-31-91-158 systemd[1]: Listening on ssh.socket - OpenBSD Secure Shell server socket.
-- Boot fa3bc8ec546a44ef957df1e6df8973bc --
Jan 31 09:35:33 ip-172-31-91-158 systemd[1]: Closed ssh.socket - OpenBSD Secure Shell server socket.
Jan 31 09:35:33 ip-172-31-91-158 systemd[1]: ssh.socket: Deactivated successfully.
Jan 31 09:35:26 ip-172-31-91-158 systemd[1023]: Closed gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Jan 31 09:35:26 ip-172-31-91-158 systemd[1023]: Stopping gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation)...
Jan 31 09:35:26 ip-172-31-91-158 systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
Jan 31 09:35:26 ip-172-31-91-158 systemd[1]: ssh.service: Deactivated successfully.
Jan 31 09:35:26 ip-172-31-91-158 systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
Jan 31 09:35:26 ip-172-31-91-158 sshd[1018]: pam_unix(sshd:session): session closed for user ubuntu
Jan 31 09:00:52 ip-172-31-91-158 systemd[13701]: Closed gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation).
Jan 31 09:00:52 ip-172-31-91-158 systemd[13701]: Stopping gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation)...
Jan 31 09:00:52 ip-172-31-91-158 systemd[13701]: Closed gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Jan 31 09:00:41 ip-172-31-91-158 systemd[13701]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation)...
Jan 31 09:00:41 ip-172-31-91-158 systemd[13701]: Starting gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent emulation)...
Jan 31 09:00:41 ip-172-31-91-158 systemd[13701]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper.
Jan 31 08:35:22 ip-172-31-91-158 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jan 31 08:35:21 ip-172-31-91-158 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...

```

Editar o borrar un archivo de diario.

Podemos acceder de dos formas diferentes:

- haciendo clic sobre su nombre en la página principal
- haciendo clic sobre el botón Regresar a detalles de diario. Al hacerlo, obtendremos una nueva página que nos muestra un formulario como el de la imagen siguiente.

En el formulario podremos cambiar opciones como el tipo de destino, el archivo de registro o el estado en el que se encuentra (activo/no activo). También podemos actuar sobre las prioridades o los tipos de mensajes a tratar. Ojo con las modificaciones!! pueden dejar de registrarse eventos de sistema que sean importantes para su estabilidad y/o seguridad.

También podemos hacer clic sobre el botón Borrar. Esto hará que dejen de recabarse los datos del diario, pero no se eliminarán los archivos.


The screenshot shows a web form titled 'Log destination'. It has several sections:

- Log to:** Radio buttons for 'File' (selected), 'Named pipe', 'Local users', 'All logged-in users', and 'Syslog server on'. The 'File' section has a text input for the path (e.g., '/var/log/auth.log') and a checkbox for 'Sync after each message?'.
- Logging active?:** Radio buttons for 'Yes' (selected) and 'No'.
- Message types to log:** Two rows of dropdown menus for 'Facilities' and 'Priorities'. The first row has 'Many' selected for facilities and 'All' for priorities. The second row has 'Many' selected for facilities and 'None' for priorities.
- Buttons:** 'Save' (green), 'View logfile' (blue), and 'Delete' (red).

Haciendo clic sobre el botón Regresar a detalles de diario volveremos a la página principal de Diarios del sistema. En ella, haremos clic sobre Aplicar cambios para activar los ajustes que hayamos realizado.

File /var/log/mail.err	Yes	mail.err
File /var/log/debug	No	news.none ; mail.none
File /var/log/messages	No	mail,news.none
Users :omusrmsg:*	Yes	*.emerg
File /dev/tty8	No	*.=notice ; *.=warn
Output from journalctl -n 1000	Yes	SystemD logs
Output from dmesg	Yes	Kernel messages
File /var/webmin/miniserv.error	Yes	Webmin error log


⊕ Add a new system log

View log file:  View

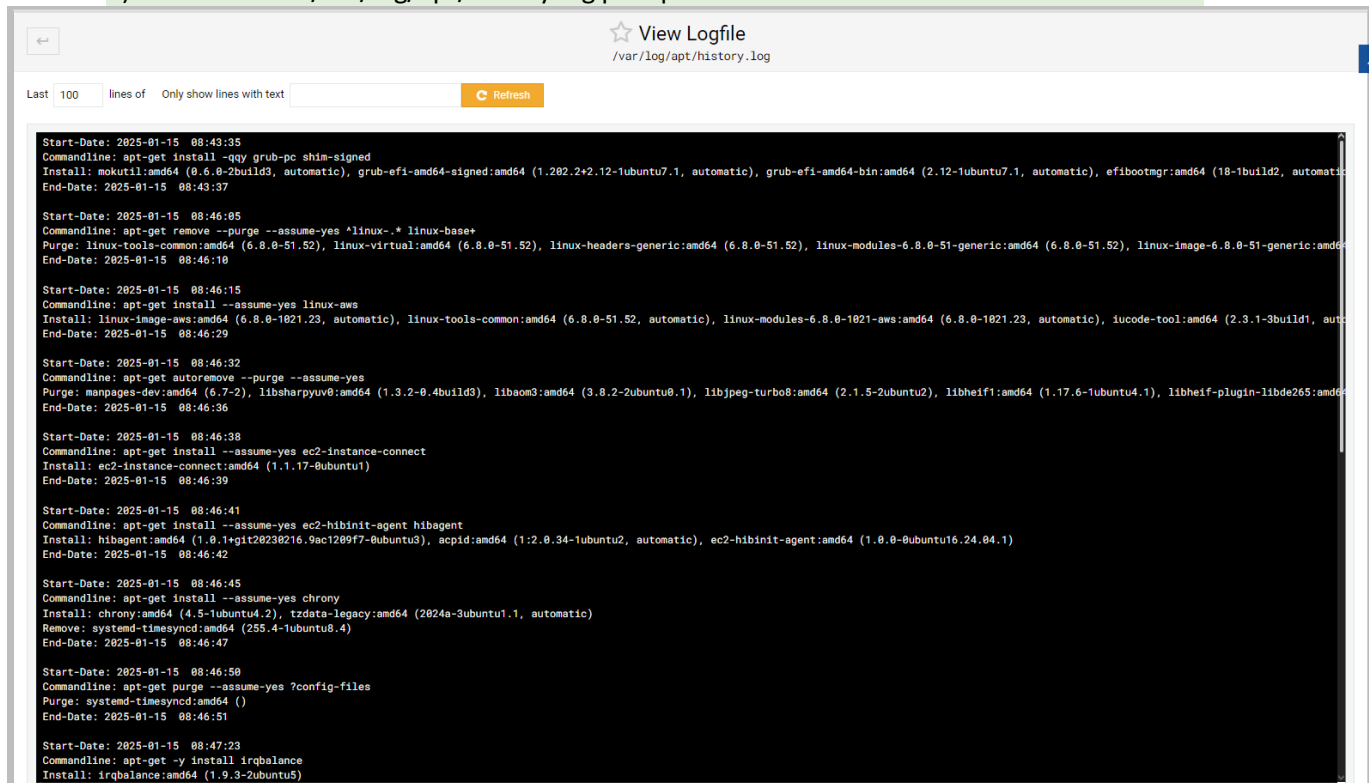
 Apply Changes

Click this button to make the current configuration active by killing the running syslog process and restarting it.

Consultar un archivo de diario sin cambiar la configuración


Desde la página principal del módulo Diarios del sistema, se puede consultar cualquier archivo de diario sin cambiar la configuración existente. Basta con escribir la ruta del archivo en el cuadro de texto View log file. Si no conocemos la ruta completa, podemos hacer clic sobre el botón contiguo (). Así podemos seleccionar la ubicación del archivo que nos interese. Cuando lo veamos, haremos clic sobre él y le damos al botón de seleccionar. Esto nos llevará de vuelta a la página anterior, pero ahora el cuadro de texto contendrá la ruta completa del archivo que queremos consultar. Ahora ya podemos darle al botón View.

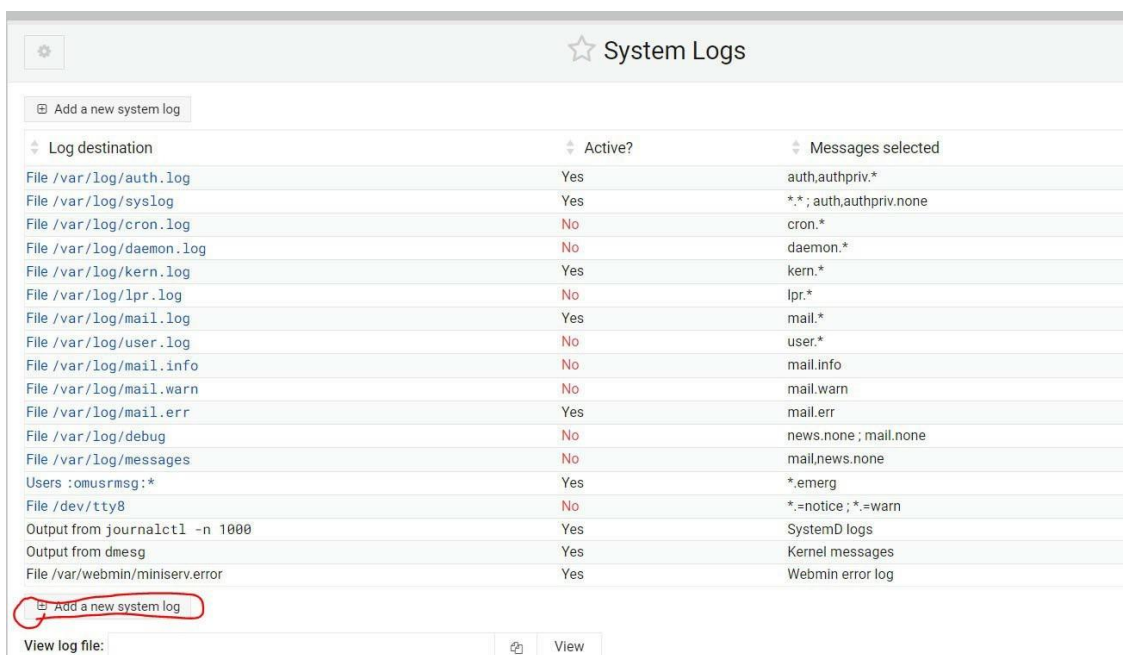
b) Seleccionar el /var/log/apt/history.log para poder verlo



El resultado será, como antes, una nueva página titulada View Logfile / Ver archivo de diario.

Añadir un nuevo archivo de diario a la página Diarios del sistema.

Si vamos a consultar a menudo un determinado archivo de diario que no aparezca en la lista predeterminada, lo podemos añadir. Click botón Añadir un nuevo diario de sistema. Para seleccionar el archivo podemos escribir su nombre, incluyendo la ruta completa, aunque, quizás sea más cómodo utilizar el botón que hay a la derecha del cuadro de texto ().



Navegamos por el árbol de directorios hasta que localicemos el archivo que nos interesa. Cuando lo veamos, haremos clic sobre él. Después, como mínimo, elegiremos el tipo de mensajes que deben mostrarse (Facilities/Facilidades) y prioridad. Cuando estemos listos, damos a Salvar para guardar los cambios.

- c) Seleccionar el `/var/log/apt/history.log` para que se incorpore a la lista predeterminada. Elegir todos mostrar Todos los mensajes. E

← Add System Log

Log destination

Log to

☒ File

☒ Sync after each message?

☐ Named pipe

☐ Local users

☐ All logged-in users

☐ Syslog server on

Logging active?

☒ Yes ☐ No

Message types to log

Facilities

☒ All ☐ Many

Priorities

☒ None ☐ All ☐ At or above...

Save

← Return to module index

- d) En la página de Diarios del sistema, comprobamos que ya aparece el archivo que acabamos de incorporar

⚙️ ☆ System Logs RS

⊞ Add a new system log

Log destination	Active?	Messages selected
File /var/log/auth.log	Yes	auth,authpriv.*
File /var/log/syslog	Yes	*.*;auth,authpriv.none
File /var/log/cron.log	No	cron.*
File /var/log/daemon.log	No	daemon.*
File /var/log/kern.log	Yes	kern.*
File /var/log/lpr.log	No	lpr.*
File /var/log/mail.log	Yes	mail.*
File /var/log/user.log	No	user.*
File /var/log/mail.info	No	mail.info
File /var/log/mail.warn	No	mail.warn
File /var/log/mail.err	Yes	mail.err
File /var/log/debug	No	news.none;mail.none
File /var/log/messages	No	mail,news.none
Users :omusrmsg:*	Yes	*.emerg
File /dev/tty8	No	*.=notice;*.warn
File /var/log/apt/history.log	Yes	*.none
Output from journalctl -n 1000	Yes	SystemD logs
Output from dmesg	Yes	Kernel messages
File /var/webmin/miniserv.error	Yes	Webmin error log

⊞ Add a new system log

View log file: View

Apply Changes Click this button to make the current configuration active by killing the running syslog process and restarting it.

Informes sobre sucesos de Ubuntu Server con Logcheck

A diferencia de Webmin y Cockpit Logcheck compara las entradas recientes en el registro de sucesos con un conjunto de reglas predefinidas. Dichas reglas identifican los eventos como urgentes o los desestiman como rutinarios. Al final, envía el resultado por correo electrónico al administrador del sistema. También hace un seguimiento de los eventos procesados, para no repetirlos en sucesivas ejecuciones. Este modo de funcionar nos permite automatizar, en parte, la supervisión del sistema y mejorar la seguridad.

Antes de instalar: para funcionar, Logcheck necesita que se encuentre instalado y configurado el servidor de correo PostFix. Si en el momento de instalar Logcheck, Postfix no se encuentra en el sistema, se añadirá como una dependencia más e, incluso, se ejecutará su asistente de configuración.

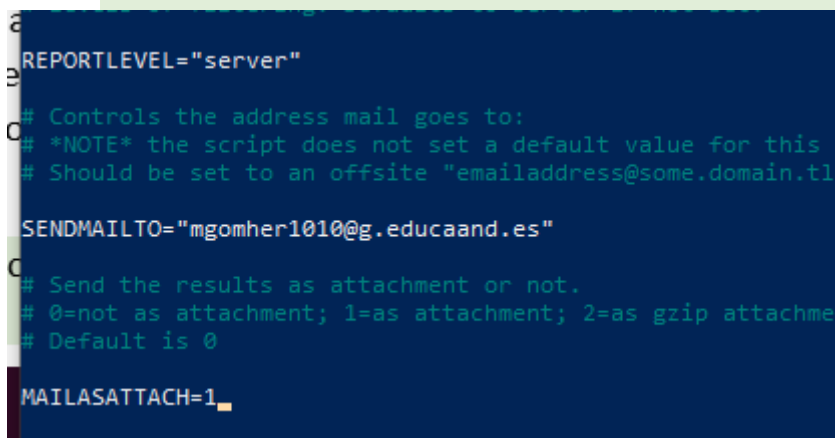
Como es habitual antes de instalar un programa, lo 1º es actualizar la base de datos de paquetes de nuestro equipo, para asegurarnos de que instalamos la última versión del software que necesitamos. Después hacemos un upgrade instalar las últimas versiones de los paquetes actualizables, es decir, aquellos que tienen una versión más moderna en el repositorio que en nuestro equipo. Y a continuación instalamos Logcheck. Logcheck se encuentra en los repositorios oficiales de Ubuntu. Realizamos:

```
sudo apt update sudo
apt upgrade
sudo apt install logcheck
```

Configurar Logcheck

Hay que editar su archivo de configuración: /etc/logcheck/logcheck.conf para decirle la dirección de correo a la que deben enviarse los informes, que se encuentra en la variable SENDMAILTO. Nota: intenta evitar direcciones de correo que incluyen signos (como, por ejemplo, somebooks_es@g.educaand.com), Logcheck puede no funcionar correctamente. Ojo!.. algunas direcciones de correo pueden no funcionar, porque sus respectivos servidores los filtran. También le diremos que los informes deben incluirse como archivos adjuntos. Esto se hace asignando a la variable MAILASATTACH el valor 1. El informe se genera en formato de texto plano.

e) Adjunta la captura de pantalla con tu correo al que se enviarán los informes, así como la variable MAILASATTACH a 1.



```
REPORTLEVEL="server"
# Controls the address mail goes to:
# *NOTE* the script does not set a default value for this
# Should be set to an offsite "emailaddress@some.domain.tl
SENDMAILTO="mgomher1010@g.educaand.es"
# Send the results as attachment or not.
# 0=not as attachment; 1=as attachment; 2=as gzip attachment
# Default is 0
MAILASATTACH=1
```


Ya podemos probar Logcheck. Durante su instalación, se ha creado un usuario, también llamado logcheck, para evitar que el comando se ejecute como root. De hecho, si intentas ejecutarlo con privilegios de root, obtendrás un error. Para ejecutar el comando logcheck con el usuario logcheck, necesitamos recurrir al argumento -u del comando sudo. Su formato general es este...

```
sudo -u usuario comando
```

Nosotros, además, añadiremos dos argumentos a logcheck:

- -o, que sustituye el envío del correo electrónico por la salida en pantalla, para ver el resultado de forma inmediata.
- -t, que inhibe el seguimiento de los eventos procesados, lo que nos permite seguir haciendo pruebas sin perder los eventos anteriores.

Por lo tanto, el comando nos queda así:

```
sudo -u logcheck logcheck -o -t
```

```
aso@ubuntuServerRuth:~$ sudo nano /etc/logcheck
[sudo] password for aso:
aso@ubuntuServerRuth:~$ sudo nano /etc/logcheck/logcheck.conf
aso@ubuntuServerRuth:~$ sudo -u logcheck logcheck -t
sendmail: fatal: open /etc/postfix/main.cf: No such file or directory
Error closing sendmail: non-zero exit (75) at /usr/bin/mime-construct line 571.
aso@ubuntuServerRuth:~$
```

En nuestro caso hay un error porque Postfix no está configurado (yo al instalar el paquete en su momento seleccioné “sin-internet”). Si tienes que configurarlo, hazlo con la orden:

```
sudo dpkg-reconfigure postfix
sudo systemctl restart postfix
```

selecciona sitio de internet (hay bastantes opciones posibles). Cuando configures, ve leyendo los mensajes, te guiarán en lo que hacer.

f) Adjunta captura de pantalla comprobando que Logcheck funciona

```
2025-01-31T12:45:51.655009+00:00 ip-172-31-91-158 adduser[4423]: Adding new group 'logcheck' (GID 118) ...
2025-01-31T12:45:51.650408+00:00 ip-172-31-91-158 groupadd[4428]: group added to /etc/group: name=logcheck, GID=118
2025-01-31T12:45:51.657187+00:00 ip-172-31-91-158 groupadd[4428]: group added to /etc/gshadow: name=logcheck
2025-01-31T12:45:51.658248+00:00 ip-172-31-91-158 groupadd[4428]: new group: name=logcheck, GID=118
2025-01-31T12:45:51.661510+00:00 ip-172-31-91-158 adduser[4423]: Adding new user 'logcheck' (UID 114) with group 'logche
ck' ...
2025-01-31T12:45:51.681499+00:00 ip-172-31-91-158 useradd[4435]: new user: name=logcheck, UID=114, GID=118, home=/var/li
b/logcheck, shell=/usr/sbin/nologin, from=/dev/pts/2
2025-01-31T12:45:51.706472+00:00 ip-172-31-91-158 adduser[4423]: Not creating home directory '/var/lib/logcheck'.
2025-01-31T12:45:51.756717+00:00 ip-172-31-91-158 adduser[4450]: Adding user 'logcheck' to group 'adm' ...
2025-01-31T12:45:51.776212+00:00 ip-172-31-91-158 usermod[4452]: add 'logcheck' to group 'adm'
2025-01-31T12:45:51.776298+00:00 ip-172-31-91-158 usermod[4452]: add 'logcheck' to shadow group 'adm'
2025-01-31T12:45:51.813371+00:00 ip-172-31-91-158 chfn[4462]: changed user 'logcheck' information
2025-01-31T12:45:51.818733+00:00 ip-172-31-91-158 postfix/sendmail[4470]: fatal: open /etc/postfix/main.cf: No such file
or directory
2025-01-31T12:45:52.018505+00:00 ip-172-31-91-158 kernel: audit: type=1400 audit(1738327551.978:128): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="rsyslogd" pid=4488 comm=
"apparmor_parser"
2025-01-31T12:45:55.258152+00:00 ip-172-31-91-158 dbus-daemon[505]: [system] Activating via systemd: service name='org.f
reedesktop.PackageKit' unit='packagekit.service' requested by ':1.30' (uid=0 pid=4517 comm="/usr/bin/gdbus call --system
--dest org.freedesktopto" label="unconfined")
2025-01-31T12:45:55.272760+00:00 ip-172-31-91-158 PackageKit: daemon start
2025-01-31T12:45:55.315236+00:00 ip-172-31-91-158 dbus-daemon[505]: [system] Successfully activated service 'org.freedes
ktop.PackageKit'
ubuntu@ip-172-31-91-158: ~$
```

Ahora vamos a asegurarnos de que se reciben los correos electrónicos. Para ello repetimos el comando, pero eliminando la opción -o:

```
sudo -u logcheck logcheck -t
```

Si todo ha sido correcto, unos instantes después tendremos, en la bandeja de entrada de la cuenta de correo que hayamos configurado como destinataria, un nuevo mensaje. Ojo! si Logcheck no encuentra mensajes nuevos, no enviará ningún correo electrónico.

g) Adjunta captura de pantalla del correo y comprueba que incorpora un archivo adjunto con el informe generado.

```
ubuntu@ip-172-31-91-158:~$ sudo systemctl restart postfix
ubuntu@ip-172-31-91-158:~$ sudo -u logcheck logcheck -t
ubuntu@ip-172-31-91-158:~$
```

Configurar los ficheros que monitoriza Logcheck

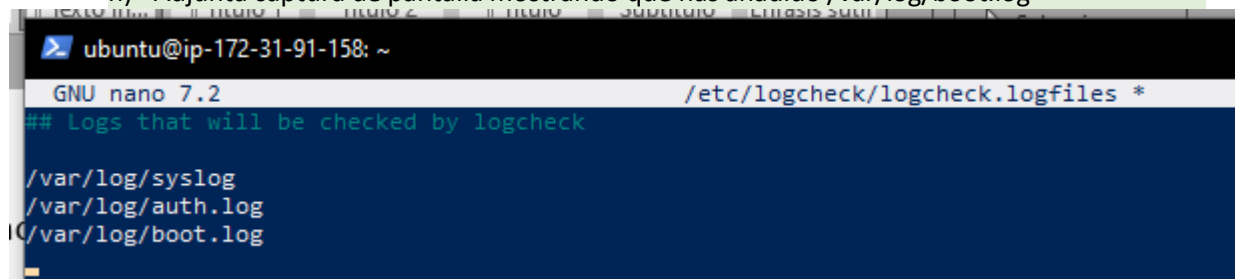
El archivo `/etc/logcheck/logcheck.logfiles` contiene el nombre de los archivos de sucesos que Logcheck analiza. Por defecto son:

- `auth.log`
- `syslog`,

pero podemos añadir los que queramos; poer ej. `/var/log/boot.log`, que es donde se anotan las incidencias de inicio del sistema. También podemos añadir los ficheros generados por cualquier aplicación, como `/var/log/apache2/error.log` o `/var/log/apache2/localhost/error.log`. Cuando terminemos de escribirlo, guardamos los cambios.

```
sudo nano /etc/logcheck/logcheck.logfiles
```

h) Adjunta captura de pantalla mostrando que has añadido `/var/log/boot.log`



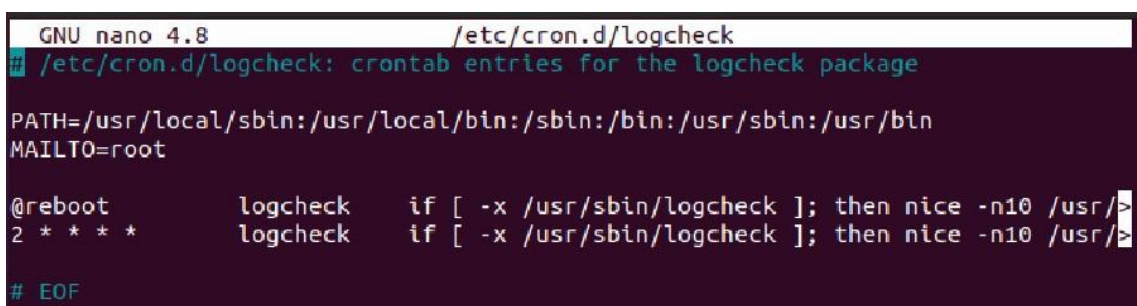
```
GNU nano 7.2 /etc/logcheck/logcheck.logfiles *
## Logs that will be checked by logcheck
/var/log/syslog
/var/log/auth.log
/var/log/boot.log
```

La frecuencia con la que se ejecuta Logcheck:

Logcheck ya se ha autoinstalado en el cron, en el fichero `/etc/cron.d/logcheck`. El archivo `/etc/cron.d/logcheck` representa una tarea para cron e indica con qué frecuencia se generan los informes. Si vemos su contenido:

```
sudo nano /etc/cron.d/logcheck
```

Comprobamos que Logcheck se pondrá en marcha con cada reinicio o en el minuto 2 de cada hora.



```
GNU nano 4.8 /etc/cron.d/logcheck
# /etc/cron.d/logcheck: crontab entries for the logcheck package

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

@reboot    logcheck    if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck; fi
2 * * * * logcheck    if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck; fi

# EOF
```


Modificamos el archivo para ajustar la frecuencia de los informes según nuestras necesidades (el de arriba está sin modificar es por defecto, modifica tú el tuyo).

i) Adjunta captura de pantalla modificando el crontab y explica la modificación efectuada

```
GNU nano 7.2 /etc/cron.d/logcheck *
# /etc/cron.d/logcheck: crontab entries for the logcheck package

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

@reboot    logcheck    if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck -R; fi
*/30 * * * *    logcheck    if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck; fi

# EOF
```

Con este cambio, va a enviar el logcheck cada 30 minutos.

Las reglas de filtrado

Es necesario entender este punto: Hay que instruir a logcheck para que no nos avise de las cosas irrelevantes, y él nos va a avisar **de todo el resto de cosas**, por tanto si en esos avisos recibimos información que no nos interesa tendremos que añadir reglas a su configuración para que las obvie en las siguientes ocasiones. **Por suerte viene con bastante reglas preconfiguradas** así que lo más común que aparece en los logs ya está ignorado de entrada. Vamos a añadir un par de reglas para que veáis como seguir trabajando con él. Las reglas de Logcheck se almacenan en archivos de texto, dentro de diferentes carpetas, según su tipo:

- Las que identifican un suceso como un intento de intrusión se guardan en el directorio /etc/logcheck/cracking.d.
- Las que excluyen un suceso como un intento de intrusión se guardan en el directorio /etc/logcheck/cracking.ignore.d.
- Las que identifican un suceso como una alerta de seguridad se guardan en el directorio /etc/logcheck/violations.d.
- Las que excluyen un suceso como una alerta de seguridad se guardan en el directorio /etc/logcheck/violations.ignore.d.
- Lo que queremos que ignore se guarda en: /etc/logcheck/ignore.d.server/

Las demás son consideradas sucesos del sistema. Logcheck procesa los sucesos según una serie de reglas redactadas como expresiones regulares. Estas expresión regular son los patrones que aparecen en los archivos de sucesos cuando se produce un determinado evento. Por ejemplo, una regla podría ser así:

```
login.*: .*LOGIN FAILURE.* FROM .*root
```

Con ella buscamos líneas en las que el subsistema login indique cualquier fallo al tratar de iniciar sesión como root. Si quieres profundizar puedes encontrar información detallada sobre el filtrado de sucesos en /usr/share/doc/logcheck-database/README.logcheckdatabase.gz.

Vamos a añadir una regla de prueba. Para ver que funciona, primero añadimos un usuario con useradd

Useradd fulanito

sudo -u logcheck logcheck -o -t

```
LEN=36 IOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
Oct  7 19:28:43 ubuntu-serverRuth useradd[16852]: new group: name=fulanito, GID=1001
Oct  7 19:28:43 ubuntu-serverRuth useradd[16852]: new user: name=fulanito, UID=1001, GID=1001, home=/home/fulanito, shell=/bin/sh, from=/dev/pts/0
```

veo que me lo reporta. Ahora vamos a configurar una nueva regla: la de que no nos avise cuando emplea useradd. Creamos un nuevo archivo en la carpeta correspondiente: /etc/logcheck/ignore.d.server/mis-reglas. En este fichero inventado simplemente tenemos que teclear una lista de expresiones. Si una línea del log que esté siendo analizada concuerda con una de estas expresiones, no seremos informados de ella:

- j) Añade tu la regla necesaria (investiga como hacerlo) y comprueba si funciona. En la captura, explica la regla que has añadido. Si quieres probar otra regla distinta de la propuesta también es válido si la pruebas

```
GNU nano 7.2 /etc/logcheck/ignore.d.server/ssh-login-fail *
sshd.*Failed password for
```

Esta nueva regla elimina de los logs las conexiones por ssh.

```
ubuntu@172-31-91-158:~$ sudo -u logcheck /usr/sbin/logcheck -o
This email is sent by logcheck. If you no longer wish to receive
such mail, you can either uninstall the logcheck package or modify
its configuration file (/etc/logcheck/logcheck.conf).

E: File could not be read: /var/log/boot.log

System Events
-----
2025-01-31T13:12:27.951384+00:00 ip-172-31-91-158 postfix/error[21010]: E0CBF4B411: to=<mgomher1010@eg.educaand.es>, relay=none, delay=0.04, delays=0.03/0/0/0.01, dsn=5.0.0, status=bounced (g.educaand.es)
Jan 31 13:12:27 ip-172-31-91-158 postfix/error[21010]: E0CBF4B411: to=<mgomher1010@eg.educaand.es>, relay=none, delay=0.04, delays=0.03/0/0/0.01, dsn=5.0.0, status=bounced (g.educaand.es)
```

Como podemos ver, ya no aparecen.