Existen varias alternativas para el monitoreo de servidores: ganglia, nagios y monit por dar solo unos ejemplos, pero para evitar configurar tanta cosa, todos mis servidores tienen logwatch, logcheck y snoopy.

logcheck es una utilidad que revisa los logs del sistema y genera un reporte, eliminando las entradas que son normales en un sistema (ejecuciones de cron, por ejemplo) para mostrar únicamente aquellas sospechosas.

snoopy es una librería que funciona como wrapper del execve() de libc, para guardar un registro de todos los comandos ejecutados en el sistema, un .bash_history que no puede ser modificado o borrado por el usuario.

Un problema de tener estas dos utilidades corriendo es que snoopy va a guardar el registro de los comandos ejecutados por logcheck cuando parsea los logs, formando un circulo vicioso que terminara generando un reporte con las acciones de logcheck, ¡marcadas como alertas!. En palabras cristianas, un email de 500k con información repetida.

La solución es crear los archivos /etc/logcheck/ignore.d.server/snoopy y /etc/logcheck/violations.ignore.d/snoopy con esta línea (probado y usado en Debian GNU/Linux):

```
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ snoopy.*uid\:109.*
```

El mismo esquema se puede usar para pasar por alto diferentes comandos del sistema, como sendmail y procmail, que generalmente son bastante comunes. Para validar que las expresiones regulares nos funcionen, se puede usar el útil grep o la página Rex V

Artículo original de

http://www.sisfo.com/blog/tag/sysadmin/