

## El día a día del administrador de sistemas: Postfilter

## BUENAS NOTICIAS

**N**NTTP (Protocolo de Transferencia de Noticias por Red) se escribió hace ya bastante tiempo, pero Usenet probablemente aún siga rondando cuando el último foro de Web 2.0 esté mordiendo el polvo. Esto no sería una mala noticia si el protocolo tuviera algún mecanismo de protección. Tal y como está la situación, la gente de Usenet tiende a portarse mal. Como administrador, una vez me enfurecí con la comunidad Usenet (*abuse@kuehnast.com*: *Buzón saturado*), y luego tuve que aguantar los comentarios del tipo: “¿Qué quieres decir con que es malo publicar en varios grupos a la vez?”.

Postfilter añade al servidor un sistema de protección contra spam y abuso. No voy a explicar los pasos de la instalación aquí, ya que el sitio web [1] tiene una guía fantástica.

Postfilter filtra los mensajes de mis usuarios con un conjunto de reglas configurable, dándome la posibilidad de filtrar las palabrotas al estilo de Spamassassin. Las coincidencias se puntúan y el servidor bloquea los mensajes a partir de un umbral predeterminado. La restricción de la publicación de un mismo mensaje en múltiples grupos es bastante útil en los escenarios reales. La variable *max\_crosspost* en *postfilter.conf* define el número de grupos de noticias en los que un mensaje puede ser publicado, suponiendo que los usuarios lo pongan en práctica. El valor por defecto de 10 es muy alto en mi opinión. Si no se aplica, se usa el valor de *max\_fup\_no\_crosspt*. Aquí es mejor el valor por defecto de 3, pero yo lo reduzco a 1, por si las moscas.

Se puede restringir el tamaño de un mensaje; *max\_total\_size* está establecido en 32 kbytes por defecto. Esto es demasiado generoso, a menos que uno de sus usuarios sea un

Si los protocolos fueran seres humanos, NNTP sería una persona amable y ligeramente patosa que siempre ve la parte buena de los demás – incluso si estos tiran basura en su buzón de correo. Postfilter es un guardián para NNTP. **POR CHARLY KÜHNAST**

Max Crosspost	3 Groups	How many groups could the users insert in the <b>Newsgroups</b> header?
Max Followup	3 Groups	How many groups could the users insert in the <b>Followup-To</b> header?
Max Crosspost without followup	3 Groups	How many groups could the users insert in the <b>Newsgroups</b> header without adding a <b>Followup-To</b> ?
Max Total Size	32 KB	How many bytes could an article include as <b>total</b> weight (headers plus body)?
Max Head Size	2 KB	How many bytes could an article include as <b>headers</b> weight?
Max Body Size	32 KB	How many bytes could an article include as <b>body</b> weight?
Max Hierarchies	3 Hierarchies	How many hierarchies could the users insert in the <b>Newsgroups</b> header?
Max Hierarchies in Followup-To	3 Hierarchies	How many hierarchies could the users insert in the <b>Followup-To</b> header?
Lines limits	50%	Quoted Lines
	50%	Empty Lines
	50%	Blank Lines
Max Grace time	30 Minutes	How many minutes could the users' time differ from the server's time?
Max line length	80 chars	How many characters could each line include?

Figura 1: Si le tiene alergia a vi, la web le proporcionará un medio limitado para crear una configuración de Postfilter mediante clics de ratón.

autor de bestsellers. Para un control más preciso, pueden establecerse por separado el tamaño de la cabecera y del cuerpo.

Las citas largas, mensajes que principalmente contienen textos de otros colaboradores, son una molestia constante en los grupos de noticias. La respuesta de Postfilter a este comportamiento tan vago es *max\_quoted\_ratio*. La variable acepta valores entre 0.0 y 1.0. Si se establece un valor de 0.7 significa que un máximo de un 70% del mensaje puede ser una cita.

### ¿Es esa la Hora?

Mientras que estas restricciones están diseñadas principalmente para impedir que mis usuarios hagan locuras entre ellos mismos, hay otros parámetros que nos proporcionan protección contra los spammers y los clientes mal configurados. Primero se mira la fecha y la hora: los spammers suelen utilizar fechas futuras en las cabeceras para situarse en lo alto de la lista de los mensajes no leídos. Postfilter tiene la variable *max\_grace\_time* que rechaza los mensajes con fechas que no correspondan con la del servidor.

Por defecto está establecida a 1800 segundos, es decir, media hora.

Por supuesto, es posible ejercer un control más riguroso sobre la frecuencia de publicación. De hecho, puede establecerse el número de mensajes, y el tamaño en bytes, que se permite publicar durante un periodo de tiempo especificado clasificado por usuario, dominio o dirección IP; así como el número de errores permitidos que puedan tener en el proceso antes de que Postfilter los bloquee. *allow\_control\_cancel* tampoco está mal: permite o rechaza los mensajes cancelados.

### Conclusiones

No hay que exagerar los límites, los administradores pueden evitar los problemas y pueden mantener a la mafia de Usenet a raya. Después de todo, creer en la gente no tiene porqué ser una mala experiencia. ■

## SYSADMIN

### Historias de administradores . . . . 60

Estudios reales de vinculación Ethernet, VLANs y servidores DHCP problemáticos.

### Argus . . . . . 64

Esta útil herramienta le ayudará a analizar el ancho de banda y a detectar las amenazas.

## RECURSOS

[1] Postfilter: <http://news.aioe.org/spip.php?rubrique24>