

El Día a Día del Administrador de Sistemas: Policyd

¡FUERA!

El plugin Postfix Policyd lucha contra el spam utilizando técnicas como listas grises, detección de código, medidas de volumen, listas negras y detección y rotación HELO. **POR CHARLY KÜHNAST**

Le he añadido muchas cosas a mi querido y cansado Postfix a lo largo de los años, por ejemplo, Spamassassin para combatir el spam y filtros contra los virus. El último miembro de este club exclusivo de añadidos es Policyd. La herramienta Policyd, a diferencia de muchas otras herramientas externas, no utiliza el mecanismo *content_filter* para integrarse con Postfix. En vez de esto, prefiere *check_policy_service*, que se encuentra disponible en Postfix 2.2 o superior.

Esto me permite enganchar Policyd a mi juego de reglas existente en algún lugar sensato. No necesito enviar spam que ha sido rechazado por otras razones al servicio policy. La versión actual del programa Policyd C es la 1.73, que puede descargarse desde [1] y la instalación del demonio es muy sencilla. Tras desempaquetarlo, se introduce en el directorio *policyd* lo siguiente:

```
gmake build
gmake install
```

También se requiere MySQL. Policyd le proporciona un script SQL que automáticamente crea las tablas necesarias. Para finalizar, necesita crear una tarea en el cron:

```
0 * * * * /usr/local/policyd
/cleanup -c /usr/local/policyd
/policyd.conf
```

Esta tarea eliminará periódicamente las entradas antiguas de la base de datos. El fichero de configuración le permite habilitar o

SYSADMIN

ZENworks 7 64
Novell revela una versión mejorada de su herramienta ZENworks Linux Management.

Estrategias de Sendmail 67
Mostraremos algunas soluciones para el filtrado de virus y spam.

deshabilitar varios chequeos que Policyd realiza de forma individual. Algunos de estos chequeos me resultaron bastante útiles.

HELO

La mayoría de los spammers identifican al servidor mediante el comando HELO, mientras los hosts MTA legítimos envían sus FQDN. Para evitar las listas negras HELO, los spammers tienden a enviar correos con diferente información HELO. Para combatir esta táctica rastreadora, Policyd rechaza los mensajes que vienen desde la misma IP pero con diferentes HELOs.

Por supuesto, Policyd soporta las listas negras HELO como ya he dicho. Hay una regla especial que debería tenerse en cuenta: si un mailer me envía el FQDN de *mi propio* servidor, inmediatamente le doy con la puerta en las narices.

Emisor Throttling

Policyd puede impedir que un mismo emisor bloquee un servidor de correo con un gran volumen de mensajes. La dirección del From o parte de sus dominio, el nombre de usuario SASL o la dirección IP o el bloqueo de red son todos los criterios de detección que hay. Y el número de mensajes o el tamaño total, cualquier tope será el primero, son útiles como criterios de delimitación.

Receptor Throttling

Policyd puede impedir que el usuario reciba más de un número de mensajes en un período de tiempo. Los límites de este tipo son útiles en situaciones en las que se está tratando con direcciones genéricas como *info@doma.in* o *support@doma.in*.

Listas Grises

Si permite listas grises, Postfix primero rechazará temporalmente el correo entrante y mostrará el Error 450 como explicación. Si el servidor fuente vuelve a intentarlo tras esperar

un poco, Postfix aceptará el mensaje. Si no, descartará el primer mensaje. Esto es una técnica efectiva para correos masivos o redes bot, hasta que tiendan a utilizar colas para manejar errores.

En este caso, donde los spammer comprometen una pobre configuración del servidor de correo y explotan al servidor como un repetidor, las listas grises no le ayudarán. Un servidor de correo normal reenviará si recibe un Error 450, en este caso, las listas grises están condenadas a fracasar. Aunque Policyd es un añadido muy potente para Postfix.1.

RECURSOS

[1] Policyd: <http://policyd.sourceforge.net>

EL AUTOR

Charly Kühnast es Administrador de Sistemas Unix del centro de datos de Moers, cerca del famoso río Rin. Sus tareas incluyen velar por la seguridad del cortafuegos y ocuparse de la DMZ.

