

## Registro de Sistema de Próxima Generación: Syslog-NG

# La Caja Negra



Syslog permite a los administradores obtener información de registro en sus sistemas de manera uniforme para toda la red. Realizando la tarea de guardar, analizar y procesar los archivos de registro fácilmente, pero lo que la gente espera de los registros del sistema ha cambiado en los últimos años y el servicio Syslog tradicional simplemente no lo puede ofrecer. Syslog-NG [1] cubre este hueco.

Los registros tradicionalmente se usan para comprobar la salud del sistema. Muchos administradores ni siquiera se molestan en mirar los registros a menos que se encuentren con un problema en el sistema. Pero hoy, es también una cuestión de mejorar la fiabilidad, esto es, usar el sistema como una alerta temprana para impedir que las cosas vayan a peor. La integridad de los mensajes de un sistema es también ahora más importante que nunca, ya que permiten a los administradores levantar defensas basadas en datos reales. Los administradores también buscan habitualmente más flexibilidad en la configuración y en el manejo de las redes.

Han salido varios proyectos que intentan conseguir este objetivo de mejorar el servicio del Syslog tradicional. Uno de

El registro de los eventos del sistema es un reto para cualquier administrador. Y la debilidad del servicio Syslog tradicional se hace particularmente patente en grandes redes. Syslog-NG es un sustituto que realmente vale la pena. **POR**

**CHRISTIAN SCHMITZ**

los más difundidos es Syslog-NG (Syslog de próxima generación) que se lanzó bajo licencia GPL. Muchas distribuciones Linux ya han adoptado Syslog-NG. Otras alternativas disponibles son Reliable Syslog, en su primera implementación, SDSC Secure Syslog [5] y Syslog Sign. El último todavía está en fase beta.

### Problemas con BSD Syslog

El servicio syslog tradicional se presentó en Septiembre de 1983 en la Universidad de California (Berkeley). No tenía documentos de diseño y el software estaba pobremente documentado. Pasados 18 años BSD Syslog se terminó de documentar en el RFC 3164 [7].

Syslog se ha convertido en un estándar de facto. El servicio es fácil de configurar, usando un fichero de configuración central llamado *syslog.conf*. Pero hay unas cuantas buenas razones para no estar satisfecho con la funcionalidad de *syslogd*:

### Falta de métodos de autenticación

Syslogd no puede distinguir entre distintos hosts. Si el servicio se lanza con la opción *-r*, acepta mensajes UDP en el puerto 514 sin importar cual es su origen. Esto permite a los atacantes invadir el servidor de registro con paquetes UDP o transmitir mensajes manipulados. Aparte de utilizar la funcionalidad de un firewall simple, no hay forma de proteger al servidor de registros.

### • Mensajes en texto claro

Syslog siempre usa texto claro (texto no cifrado) para transmitir mensajes a través de la red. Esto permite fácilmente

espíar los mensajes y conseguir el acceso a la información privilegiada.

### • Configuración poco flexible

La configuración de Syslog usa un sistema poco flexible con 20 posibles orígenes y 8 prioridades. Esto puede ser un obstáculo en grandes redes o para servidores con múltiples servicios.

### • Uso inconsistente de orígenes y prioridades

Para la mayoría de las aplicaciones los administradores no tienen una opción para administrar mensajes bajo un origen específico. En algunos casos se puede establecer una opción cuando se compila la aplicación, pero en tiempo de ejecución hay realmente pocas opciones disponibles.

### • No registra el origen de la fuente

Cuando un mensaje pasa por distintos servidores de registro es imposible descubrir la fuente del mismo. Syslog no almacena el FQDN (Fully Qualified Domain Name) del host. Cada host que propaga un mensaje modifica la dirección IP registrada.

### • Uso de transferencia de mensajes no orientado a la conexión (UDP)

Syslogd solo puede usar el protocolo UDP para transferir los mensajes. Si un paquete se pierde por problemas en la red el mensaje nunca llegará al destino.

## Syslog-NG

Existen grupos de desarrolladores que están trabajando para eliminar estos problemas y desarrollando un sistema de registros (ver los cuadros "Syslog-Sign" y "Reliable Syslog"). Actualmente Syslog-NG es el mejor de ellos. Este desarrollo se basa en el servicio Syslog tradicional al que se le han añadido nuevas carac-

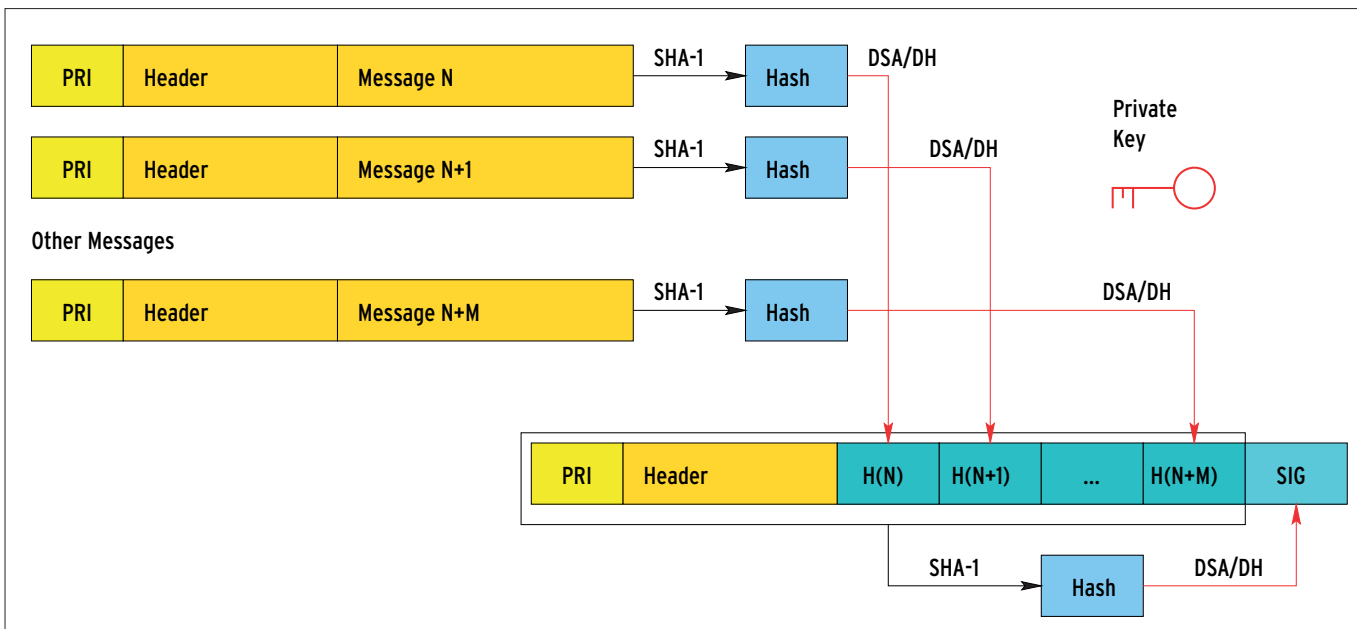


Figura 1: Syslog-Sign aplica una función hash a cada mensaje que se envía. Después transfiere un paquete con todos los valores hash de un grupo de mensajes, notificándolo al administrador de la transmisión además de las firmas de los mensajes.

terísticas sin sacrificar la compatibilidad con el RFC 3164. Aunque actualmente carece de características tales como la firma digital y encriptación, los desarrolladores están intentando añadir la encriptación en una versión futura. Actualmente se necesita stunnel [4] para manejar la encriptación.

Syslog-NG puede cambiarse de UDP a

### Syslog-Sign

Syslog-Sign es una extensión del RFC 3164 [7] que mantiene la compatibilidad hacia atrás con el BSD Syslog. Como sugiere su nombre, este nuevo desarrollo usa la firma digital para proteger los mensajes de ser manipulados por un atacante. En el arranque, cada host crea un par de claves asimétricas que son usadas para firmar cada grupo de mensajes. Luego el host transmite el grupo de mensajes al servidor de registro en un único mensaje (véase la figura 1). Este método es particularmente útil para proteger los mensajes almacenados. Como mantiene la compatibilidad con el RFC 3164, Syslog-Sign usa UDP para transmitir los mensajes. Los mensajes se pueden perder por la red y al no estar encriptados en sí mismos, un atacante espiando la red podría acceder a información privilegiada.

La verificación de la clave aun no está clara. Un atacante podría ser capaz de distribuir claves manipuladas ya que Syslog-Sign utiliza un mensaje normal para distribuir la clave pública. Aún se está trabajando en una implementación para FreeBSD [6]

TCP para proporcionar más fiabilidad en la entrega de mensajes. En este caso, la herramienta usa el puerto 514 por defecto. Aunque actualmente el puerto 514 está reservado para rlogin. Si quiere que los dos funcionen al mismo tiempo habrá que reconfigurar el servidor.

Muchas distribuciones incluyen actualmente Syslog-NG. Si se quiere usar el sucesor de Syslog en SuSE, hay que escribir la siguiente línea en `/etc/sysconfig/syslog` y relanzar el servicio.

```
SYSLOG_DAEMON='syslog-ng'
```

El archivo de configuración central, `/etc/syslog-ng/syslog-ng.conf`, es ligeramente más complejo que el tradicional del `syslogd`. En vez de incluir *original* y *priority*, contiene el llamado *logpaths* que está formado por *source*, *filter* y *destination*.

Hay ocho controladores fuente diferentes (véase Tabla 1). El controlador *internal* es obligatorio. Syslog-NG usa esta fuente especial para transmitir mensajes que tienen que ver con el propio servicio.

### Fuentes

Cuidado: Los controladores *file* y *pipe* no deben confundirse con las acciones de `syslogd`, *file* y *pipe*. Syslog-NG los usa como fuente desde las cuales el servicio lee mensajes y no como destino a los que

redirigir los mensajes. El controlador *file* se encarga de *klogd*, por ejemplo leyendo los mensajes del kernel desde `/proc/kmsg`.

Cada uno de estos controladores tiene una o más opciones, que pueden especificarse entre paréntesis seguido del nombre del controlador, por ejemplo, TCP y UDP necesitan saber el número de puer-

### Reliable Syslog

Reliable-Syslog [8], que está especificado en el RFC 3195, usa BEEP (Block Extensible Exchange Protocol) para transferir los mensajes. Este protocolo del nivel de aplicación está basado en TCP. Está orientado a la conexión y tiene mecanismos de autenticación y verificación. Y proporciona protección contra ataques.

Usa dos tipos de formato de mensajes: El modo RAW que es compatible con el estilo del servidor syslog RFC 3164. Y el modo COOKED que usa un formato de mensaje XML. Los mensajes COOKED además almacenan atributos adicionales como direcciones IP, FQDNs y tipos de dispositivos. La longitud del mensaje puede ser arbitraria. SDSC (San Diego Supercomputer Center) usa una implementación de Reliable-Syslog con la licencia BSD-licensed Secure Syslog [5]. Esta versión es compatible con el BSD Syslog. Requiere de las bibliotecas Roadrunner BEEP, OpenSSL, Glib2 y Pkg-Config. Además de los perfiles RAW y COOKED, también soporta el perfil llamado *Security Profile*.

**Tabla 1: Controladores fuentes**

Fuente	Descripción
internal	Controlador para el propio servidor de mensajes. Obligatorio.
unix-stream	Abre un socket Unix específico en modo SOCK_STREAM y se queda a la escucha de mensajes.
unix-dgram	Abre un socket Unix en modo SOCK_DGRAM y recibe mensajes a través de él.
file	Abre el fichero especificado.
pipe, fifo	Abre el pipe especificado y lee mensajes.
udp	Escucha mensajes en un puerto UDP.
tcp	Escucha mensajes en un puerto TCP.
sun-stream	Abre el dispositivo de flujo especificado (sólo Solaris)

to en el que escuchar y *file* necesita el nombre del archivo. Los sistemas Linux usan el controlador *unix-stream* localmente; el controlador usa un socket de dominio Unix orientado a la conexión. Cada conexión abierta requiere su propio proceso, un hecho que un atacante podría explotar para realizar un DoS (ataque por denegación de servicio).

*max-connections* puede impedir esto especificando un número máximo de conexiones concurrentes al servicio syslog. Está establecido a 10 por defecto. El manual de referencia [2] contiene una lista completa de los controladores fuente.

## Filtros y Destinos

Los filtros describen como Syslog-NG debería manejar los mensajes que recibe de las diversas fuentes. Éste es uno de los puntos fuertes del nuevo sistema de registro. Los administradores pueden usar filtros para ordenar los mensajes y pasarlos a los destinos apropiados.

**Tabla 2: Funciones filtro**

Filtro	Descripción
facility	Se refiere a los mensajes que origina la utilidad especificada.
level, priority	Se refiere a los mensajes con la prioridad especificada.
program	Filtra los mensajes donde el campo nombre del programa contienen la expresión regular especificada
host	Filtra los mensajes donde el campo nombre de host contiene la expresión regular especificada.
match	Aplica la expresión regular especificada al mensaje entero.
filter	Llama a otra regla de filtro.

Las funciones de filtro (véase la Tabla 2) pueden conectarse usando operadores booleanos (*and*, *or*, *not* y paréntesis). Para aplicar un filtro el resultado de la operación debe ser *true*. Algunas funciones de filtros pueden manejar expresiones regulares como opciones.

Los destinos especifican donde y por qué medios un mensaje debe ser redirigido y procesado. Tal y como en las fuentes hay disponibles un número de controladores de destino, cada uno de los cuales pueden tener distintas opciones. La Tabla 3 proporciona una lista de controladores disponibles.

Syslog-NG llama al controlador una sola vez y lo mantiene ejecutándose hasta que el servicio recibe la señal SIGHUP y termina. Esto hace que el controlador sea muy eficiente. Si Syslog-NG se lanzase por un programa externo por cada mensaje entrante un atacante podría lanzar múltiples procesos que sería similar a un ataque tipo DoS contra el sistema.

Syslog-NG también tiene un número de opciones globales. Por ejemplo, *chain\_hostname* y *sep\_hostname* especifican como Syslog-NG debe manejar los nombres de host cuando pasa un mensaje a través de múltiples servidores de registros. Esto permite a los administradores descubrir donde se originó el mensaje. El manual de referencia [2] contiene una lista completa de opciones globales.

## Ejemplo de Configuración

Para ilustrar la estructura de *syslog-ng.conf* la siguiente sección muestra un archivo de configuración simple dividido en secciones. Si está interesado en hacer un archivo más complejo puede consultarlo en [3].

```
source local {
    internal ();
    unix-stream("/dev/log");
    file("/proc/kmsg");
};
```

La fuente específica aquí está identificada por su nombre *local* y comprende un número de fuentes locales. Los controladores fuentes son *internal* (obligatoriamente) y el controlador *unix-stream*, los cuales usan el archivo de dispositivo */dev/log* y el controlador *file* que lee los

mensajes del kernel desde */proc/kmsg*.

La próxima sección crea una fuente de red:

```
source remote {
    tcp(
        ip(192.168.0.24) port(3333)
        max-connections(10)
    );
};
```

Esta fuente se referencia como *remote*; y su controlador es *tcp*. Syslog-NG ahora escuchará los mensajes en el puerto TCP 3333. Incluso si el ordenador tiene múltiples direcciones IP el servidor sólo escuchará en 192.168.0.24. La opción *max-connections* está establecida en 10; el ordenador aceptará un máximo de 10 conexiones concurrentes al Syslog-NG. No es necesario especificar una única fuente para los mensajes remotos. Muchos administradores crean una fuente individual que maneja todos los controladores. Dicho esto, fuentes separadas suministrarán una estructura más limpia.

## Selección de Mensajes

Ahora a por los filtros. Nuestro primer ejemplo maneja mensajes cuyo nivel de registro corresponde a los valores *warn*, *err*, *crit*:

```
filter warning {
    level(warn, err, crit);
};
```

Esta regla simple, que aplica los filtros basados en las prioridades, es bastante

**Tabla 3: Controladores destinos**

Destino	Descripción
file	Escribe el mensaje al archivo especificado.
pipe, fifo	Pasa el mensaje al pipe especificado.
unix-stream	Reenvía el mensaje al socket Unix SOCK_STREAM.
unix-dgram	Reenvía el mensaje al socket Unix SOCK_DGRAM.
udp	Envía el mensaje al puerto UDP especificado.
tcp	Envía el mensaje al puerto TCP especificado.
usertty	Envía el mensaje a la consola especificada por el usuario, si el usuario está conectado.
program	Lanza el programa especificado y envía un mensaje a la entrada estándar de programa (Stdin).

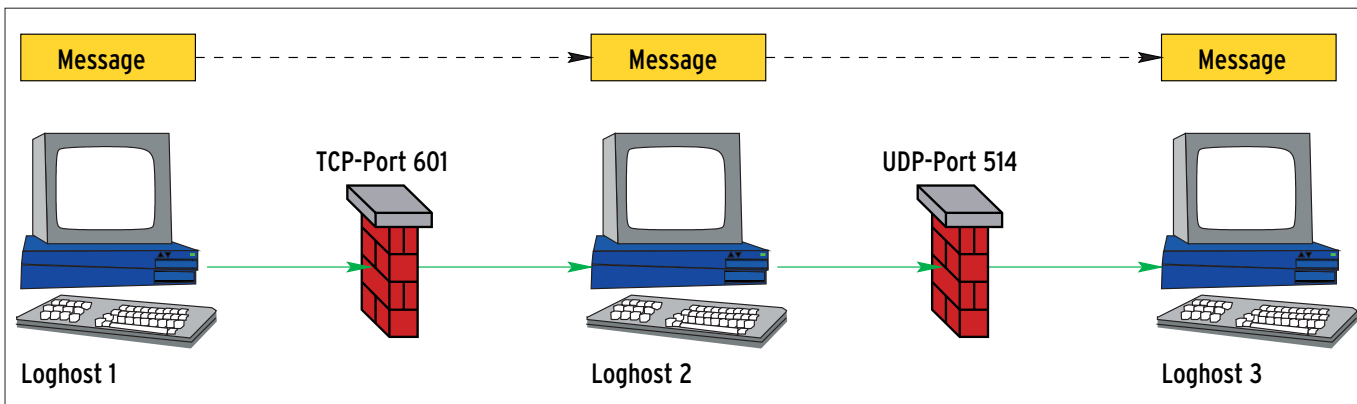


Figura 2: Dependiendo de la configuración, Syslog-NG utiliza TCP o UDP para reenviar mensajes a través de la red. Esto permite modificar Syslog-NG para su uso en entornos segmentados con múltiples cortafuegos.

común al tradicional syslogd. La mayor ventaja de la variante Syslog-NG es el uso de las expresiones regulares. Una introducción a esta técnica la podemos encontrar en diversos libros de Perl, así como en la documentación para el programa Logsurfer [9]. Esta herramienta automática de análisis de archivos de registro hace un uso intensivo de las expresiones regulares y proporciona una referencia de 50 páginas.

Veamos una expresión regular extremadamente simple que busca todos los mensajes que tienen algo que ver con FTP, que se cumple si la cadena *ftp* aparece en cualquier parte del mensaje:

```
filter ftp { match("ftp"); };
```

Y aquí tenemos otra regla de filtro que sólo permite a los mensajes críticos pasar y que también es útil para la salida a TTY10. La salida por consola no debería ser muy verbosa:

```
filter console {
  level(err) and
  not facility(
    authpriv) or
  level(warn) and
  facility(kern);
};

filter email {
  facility(mail);
};
```

El filtro *console* usa funciones, valores y expresiones booleanas. Esta regla trata cualquier mensaje de error que no se ha

originado por la utilidad *authpriv*, y todos los avisos del Kernel. El filtro *email* sólo permite pasar los mensajes del sistema de correo.

## Los Destinos

Todo lo que necesitamos ahora son unos cuantos destinos a los que mandar los mensajes. La siguiente entrada de configuración le dice a Syslog-NG que escriba los mensajes al archivo de registro */var/log/mail* (nombre de destino: *email*) o a la consola */dev/tty10*.

```
destination email {
  file("/var/log/mail");
};

destination console {
  file("/dev/tty10");
};
```

Una ruta de registro describe la ruta completa desde la fuente, a través del fil-

tro hasta el destino. Es una regla que engloba el nombre de la fuente, un filtro y un destino. La primera de las siguientes reglas lee mensajes desde la fuente *local* y manda las entradas que coinciden con la regla de filtro *console* al destino *console*. La segunda regla almacena los mensajes del sistema de correo local en */var/log/mail*.

```
01 log {
02   source(local);
03   filter(console);
04   destination(console);
05 };
06
07 log {
08   source(local);
09   filter(console),
10   destination(email);
11 };
```

Si un host necesita reenviar los mensajes recibidos a través de la red desde una fuente a otro host de registro, simplemente hay que configurar un destino apropiado para Syslog-NG.

```
destination loghost {
  udp(ip(172.16.0.33)
  port(514));
};

log {
  source(remote);
  filter(ftp);
  destination(loghost);
};
```

Lo importante es que el servidor de registro, *loghost*, esté

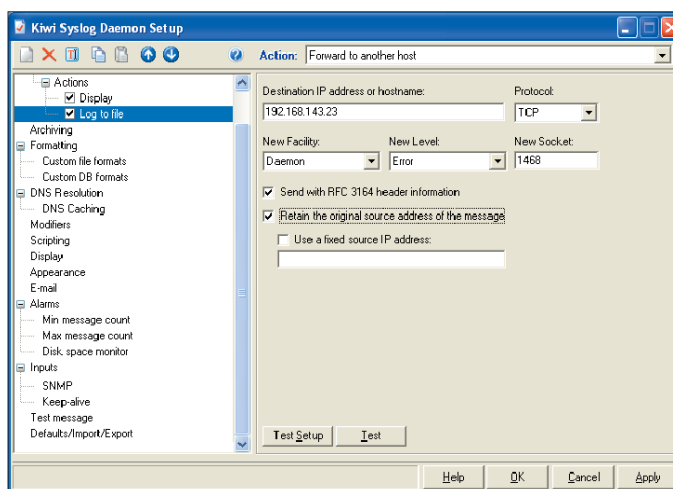


Figura 3: El servidor Syslog de Kiwi Enterprises permite a los administradores incluir ordenadores con Windows en su configuración de registros.

escuchando el puerto 514 definido por la dirección IP 172.16.0.33 en su archivo de configuración. Este método de conversión de direcciones puede ser extremadamente útil (Véase la figura 2).

## Opciones Globales

Para completar el archivo de configuración, ahora hace falta poner las opciones globales, que se colocan al principio del archivo. Algunas de las opciones especifican como Syslog-NG manejará los nombres de hosts de los mensajes, cuando redirigir los mensajes a otro servidor de registro. Habilitando `keep_hostname` se le dice a Syslog-NG que mantenga los nombres existentes.

Si se deshabilita `keep_hostname`, `chain_hostname` (alias: `long_hostname`) decide lo que hacer con el nombre. Sin el encadenamiento (`chain_hostname`), el servidor de registro insertará su propio nombre, con encadenamiento añadirá su nombre al nombre ya existente. Esto permite a los administradores trazar la ruta de los mensajes hasta su origen.

```
options {
  keep_hostname(no);
  chain_hostname(yes);
  sync(0);
};
```

La opción `sync` especifica el número de líneas que Syslog-NG guardará en la caché, antes de escribirla en el archivo. Un número alto aumentará el rendimiento, pero incrementará el riesgo de perder los mensajes si el sistema cae.

El listado 1 contiene un archivo de configuración. Éste ilustra como de avanzado es Syslog-NG con respecto a los conceptos de flexibilidad y escalabilidad, en comparación con su predecesor.

## Casi Perfecto

Las funciones filtros permiten a los administradores hacer los registros a medida, para reflejar las infraestructuras de redes complejas. La configuración es clara a pesar de su flexibilidad. Incluso se puede compensar la carencia de utilidades de encriptación y autenticación, si

se está preparado para realizar un trabajo extra [4]. Si se precisa integrar las utilidades de encriptación, autenticación y no repudio, se debe ver *SDSC Secure Syslog*. Sin embargo, este servidor requiere más mantenimiento.

Sin duda, Syslog-NG es el más completo, ya que se puede configurar para soportar su infraestructura con muy poco esfuerzo. ■

### Listado 1: Configuración Syslog-NG

```
01 # Opciones Globales
02 options { keep_hostname(no); chain_hostnames(yes); sync(0); };
03
04 # Fuentes
05 source local { internal(); unix-stream("/dev/log");
file("/proc/kmsg"); };
06 source remote { tcp(ip 192.168.0.24) port(3333)
max-connections(10);};
07
08 # Filtros
09 filter warning { level(warn, err, crit); };
10 filter email { facility(mail); };
11 filter ftp { match("ftp"); };
12 filter console {
13 level(err) and not facility(authpriv)
14 or level(warn) and facility(kern);
15 };
16
17 # Manda mensajes críticos a TTY10
18 destination console { file("/dev/tty10"); };
19 log { source(local); filter(console); destination(console); };
20
21 # Escribe mensajes de correo a un archivo
22 destination email { file("/var/log/mail"); };
23 log { source(local); filter(email); destination(email); };
24
25 # Redirige los mensajes a otra red
26 destination loghost { udp(ip(172.16.0.33) port(514)); };
27 log { source(remote); filter(ftp); destination(loghost); };
```

## Syslog y Windows

Muchas redes tienen PCs Linux y Windows. Bajo circunstancias ideales, una solución centralizada de registro debería admitir ambos sistemas. Sin embargo, se requiere software extra para permitir que los sistemas Windows envíen y reciban mensajes syslog.

El servidor de Syslog de la empresa Kiwi <http://www.kiwisyslog.com> es un ejemplo de programa que proporciona este servicio. Soporta Windows 9x, NT, 2000 y XP. Además de la versión gratuita, hay una versión comercial con funcionalidades ampliadas.

La versión gratuita es adecuada para simplemente añadir máquinas Windows a los entornos syslog de Linux. Se configura por medio de una interfaz gráfica y se puede lanzar tanto como un servidor de registro como un cliente. Como Syslog-NG, el software de Kiwi puede usar TCP o UDP para enviar los mensajes. Además tiene algunas bonitas, aunque superfluas, florituras como gráficos de barras de colores y otros gráficos estadísticos.

## RECURSOS

- [1] Pagina de inicio de Syslog-NG: [http://www.balabit.com/products/syslog\\_ng/](http://www.balabit.com/products/syslog_ng/)
- [2] Manual de Syslog-NG: [http://www.balabit.com/products/syslog\\_ng/reference/book1.html](http://www.balabit.com/products/syslog_ng/reference/book1.html)
- [3] Configuración de ejemplo: <http://www.campin.net/syslog-ng.conf>
- [4] Syslog-NG encryption howto: <http://venus.ece.ndsu.nodak.edu/~jezerr/linux/secure-remote-ogging.html>
- [5] Secure Syslog por SDSC: <http://security.sds.edu/software/sdsc-syslog/>
- [6] Syslog-sec: <http://sf.net/projects/syslog-sec/>
- [7] RFC 3164, "The BSD Syslog Protocol": <http://www.ietf.org/rfc/rfc3164.txt>
- [8] RFC 3195, "Reliable Delivery for Syslog": <http://www.ietf.org/rfc/rfc3195.txt>
- [9] Logsurfer: <http://www.cert.dfn.de/eng/logsurfer/>