Capítulo 6

Recogida de registros

Índice del capítulo

6.1. Introducción a los registros del sistema 43
6.2. Estado del arte 44
6.3. Recogida de registros: *syslog-ng* 45
6.3.1. Introducción al paquete *syslog-ng* 45
6.4. Consideraciones de seguridad: *stunnel* y *openssl* . 45

6.1. Introducción a los registros del sistema

Tradicionalmente, *syslog* ha permitido a los administradores obtener información de registros en sus sistemas de manera uniforme para toda la red, realizando la tarea de guardar, analizar y procesar los archivos de registro fácilmente.

Los registros habitualmente 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. Hoy día es también una cuestión de mejorar la fiabilidad, es decir, usar el sistema como una alerta temprana antes de que los problemas vayan a peor. También es ahora la integridad de los mensajes del sistema más importante que nunca, ya que permiten a los administradores levantar defensas basadas en datos reales.

Estas y otras necesidades han cambiado en los últimos años, y el servicio *syslogd* [43, 44] tradicional de BSD no puede cubrir todos estos aspectos, por lo que han aparecido una serie de nuevas utilidades que pretenden rellenar esas grietas y ofrecer funcionalidades completas que sustituyan al viejo *syslogd*.

Durante este capítulo vamos a estudiar algunas de las posibilidades que existen de cara a la recogida de registros en una red con múltiples generadores de registros. En primer lugar haremos una breve mención a las soluciones propuestas para el tratamiento de los eventos del sistema y del manejo de los mensajes. En segundo lugar haremos un breve acercamiento al paquete de *syslog-ng*, la utilidad que hemos seleccionado para el manejo de los mensajes de los registros.

Tras ello, en el tercer punto haremos unas menciones acerca de los aspectos de seguridad que nos permite utilizar *syslog-ng*. Por último, en el apéndice C, "*Recogida de registros*", veremos en detalle los aspectos relativos a la instalación y configuración de *syslog-ng* para un mejor manejo de los mensajes del sistema.

6.2. Estado del arte

En la actualidad la mayoría de las distribuciones de Linux basan su sistema de recogida de eventos del sistema y de manejo de los registros en la utilidad *syslogd* de Berkeley. Este programa, ideado en un principio para unas necesidades menores que las actuales, tiene una serie de carencias que nos llevan a querer sustituirlo por gestores de eventos más eficaces. Algunas de esas carencias son:

- Una clara falta de seguridad, al manejar mensajes en texto claro y sin efectuar ningún tipo de autenticación entre los sistemas.
- Transferencia de los mensajes sobre UDP, protocolo no orientado a conexión, lo que conlleva a los habituales problemas referentes a la pérdida de mensajes.
- Pérdida de la autoría del mensaje, al no propagar entre los distintos servidores el nombre del autor sino del retransmisor del mensaje.
- Una capacidad de configuración algo escasa que en la actualidad no es capaz de satisfacer esquemas complejos de múltiples máquinas y utilidades.

Existen una variedad de herramientas que pretenden subsanar algunas o todas estas carencias, de las que destacamos las siguientes:

- *syslog-sign* es una *RFC* propuesta por el *IETF* [46] para solucionar alguna carencia de *syslogd*. Busca ser compatible con *syslogd* y apenas añade una autenticación con llaves cliente-servidor, pero sigue basándose en UDP y no realiza encriptación de los mensajes.
- *syslog-reliable* es también una *RFC* [47] más compleja y que pretende solucionar el transporte (pasando a realizarse sobre TCP), la autenticación y la encriptación. Existe un intento de plasmar *syslog-reliable* en una herramienta por parte del *San Diego Supercomputer Center*, llamada *SDSC Secure Syslog* [48].
- *syslog-ng*, o *syslog de nueva generación* [49], es una aplicación bastante extendida como sustituta de *syslogd*. Ofrece una configuración mucho más potente y capaz que su precursor añadiendo poca dificultad. Ofrece transporte sobre TCP y sobre UDP para asegurar la compatibilidad con la versión anterior, y aunque no ofrece autenticación o encriptación (algo en lo que trabajan los autores) su configuración con otras aplicaciones externas para solucionar esta carencia es muy sencilla, como se verá en la sección 6.4, "*Consideraciones de seguridad: stunnel y openssl*", de este documento.

Nosotros hemos elegido *syslog-ng* por su combinación de sencillez y versatilidad, además de suponer una solución a las mayores carencias del *syslogd* habitualmente incluido en las distribuciones Linux. Además, *syslog-ng* se proporciona como *paquete Debian*, por lo que facilita aun más su uso.

6.3. Recogida de registros: *syslog-ng*

6.3.1. Introducción al paquete *syslog-ng*

syslog-ng es una utilidad que sustituye al tradicional *syslogd* de los sistemas Linux, el demonio de recogida de eventos del sistema ideado por Berkeley. Con esta sustitución, *syslog-ng* se encargará del manejo de los eventos del sistema de una manera más ordenada y efectiva, ya que actualmente estos eventos del sistema son de muy distinto origen y causan que los registros del sistema se llenen de mensajes poco importantes o *ruido* que puede llegar a ocultarnos los mensajes importantes.

syslog-ng incluye un sistema de filtrado de los mensajes no solo por la *facilidad* que los crea sino por su contenido e importancia y pretende mantener esa información sin alteraciones cuando los mensajes de eventos del sistema viajan por la red, algo que es especialmente importante cuando una máquina almacena en sus registros las notificaciones tanto propias como de otra variedad de máquinas remotas y es necesario mantener la identidad del propietario de cada uno de esos mensajes.

Hemos decidido usar *syslog-ng* por sus posibilidades de clasificación y tratamiento de los mensajes de eventos del sistema de varias máquinas a la vez, permitiéndonos recoger todos los registros en estructuras ordenadas que luego puedan ser cómodamente consultadas. Además de esto, como se verá en la sección 6.4, "*Consideraciones de seguridad: stunnel y openssl*", *syslog-ng* nos permite establecer mayores cotas que *syslogd* de seguridad en la entrega de los mensajes.

syslog-ng se proporciona como *paquete Debian* en su versión 1.6.5-2.2. En su instalación, se eliminarán las utilidades *klogd* y *sysklogd* que por defecto vienen en la distribución **Debian Sarge**. Mostramos la ficha del paquete ***syslog-ng*** en el Cuadro 6.1.

syslog-ng deberá ser instalado en las distintas máquinas, pudiendo actuar el mismo programa como emisor y receptor de los mensajes. Así, en la Figura 6.1 queda reflejada cómo se instalaría en la red.

6.4. Consideraciones de seguridad: *stunnel* y *openssl*

Se vio en la sección 4.4, "*Consideraciones de seguridad para NetFlow*", de este documento la carencia que presentaba el protocolo *NetFlow* al realizar sus comunicaciones debido a su transporte sobre UDP. *syslogd* también basaba sus

Paquete	***syslog-ng***
Autor	Balázs Scheidler < bazsi@balabit.hu >
Versión	1.6.5
Mantenedor	Attila Szalay < sasa@debian.org >
Versión del *paquete Debian*	1.6.5-2.2
Lenguaje	C
Web	http://www.balabit.hu/products/syslog-ng/

Cuadro 6.1: Ficha de *syslog-ng*

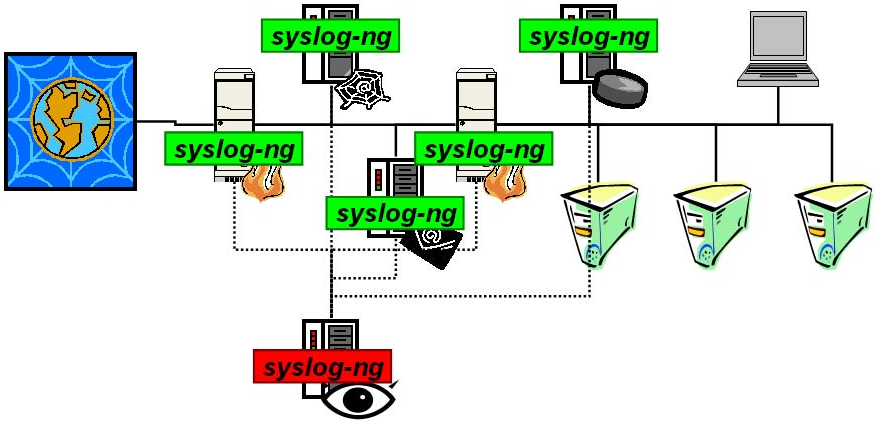

Figura 6.1: Ubicación de *syslog-ng*

capacidades de transferencia de mensajes a máquinas remotas sobre UDP, por lo que también aparece esta vulnerabilidad.

syslog-ng en cambio nos permite la posibilidad de transmitir su información por la red tanto sobre UDP como sobre TCP, y como se verá en el apéndice C.2, "*Consideraciones de seguridad: transporte mediante stunnel*", hemos elegido esta segunda opción precisamente pensando en poder asegurar sus comunicaciones.

stunnel es una utilidad que permite establecer túneles cifrados SSL para las comunicaciones entre máquinas remotas de una red [53]. Es una utilidad extendida que permite asegurar las comunicaciones de forma sencilla, siendo un uso frecuente del mismo utilizarlo para construir servidores de correo seguros sobre versiones no seguras de una manera rápida y simple.

Detallamos en el Cuadro 6.2 la ficha del paquete ***stunnel***.

Para utilizar las capacidades que *stunnel* nos ofrece deberemos configurar adecuadamente a *syslog-ng* para que lo utilice, con lo que nos quedará un esquema de funcionamiento como el indicado en la Figura 6.2.

Paquete	***stunnel***
Autor	Michal Trojnara < Michal.Trojnara@mirt.net >
Versión	3.26
Mantenedor	Julien Lemoine < speedblue@debian.org >
Versión del *paquete Debian*	3.26-3
Lenguaje	C
Web	http://www.stunnel.org/

Cuadro 6.2: Ficha de *stunnel*

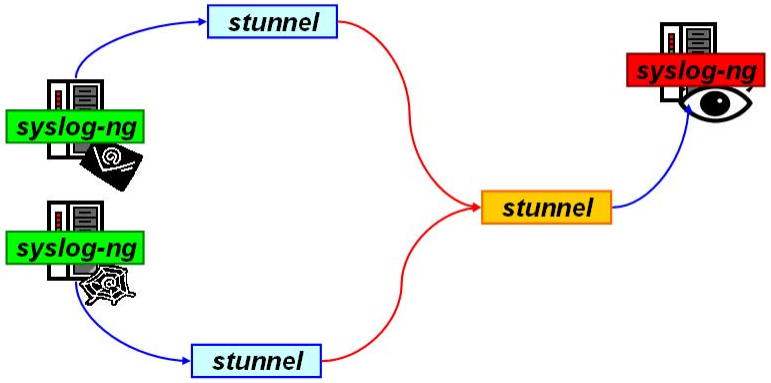

Figura 6.2: Uso de *stunnel*

De esta forma, cada utilidad *syslog-ng* se comunicará de forma no cifrada con una utilidad *stunnel* de forma local ya que ambas utilidades estarán en el mismo sistema, mientras que la comunicación entre las dos utilidades *stunnel* sí se realizará de manera cifrada atravesando nuestra red.

Por último, utilizaremos también el paquete ***openssl*** junto a *stunnel* para crear certificados [54, 55] que nos permitan realizar una autenticación entre las distintas máquinas remotas y el servidor que recoge los mensajes, con lo que añadiremos autenticación y acreditación a los mensajes transmitidos por las aplicaciones *syslog-ng*.

Mostramos la ficha del paquete ***openssl*** en el Cuadro 6.3.

Gracias a los certificados creados con *openssl*, haremos que *stunnel* utilice pares de certificados cliente-servidor de manera que el servidor de *stunnel* exija a los clientes el uso de un certificado para poder establecer el túnel con el servidor y se asegurará de que el certificado es válido, realizando así la autenticación de los clientes.

Paquete	***openssl***
Versión	0.9.7e
Mantenedor	Christoph Martin < christoph.martin@uni-mainz.de >
Versión del *paquete Debian*	0.9.7e-3
Lenguaje	C
Web	http://www.openssl.org

Cuadro 6.3: Ficha de *openssl*