1 Práctica 4: Gestión basada en notificación mediante syslog

Objetivos:

- Demostrar que se conoce en qué consiste el sistema de auditoría syslog.
- Demostrar que se sabe configurar un syslog remoto.
- Demostrar que se sabe configurar el comportamiento del sistema con los ficheros de log.

Herramientas necesarias.

- Ordenador con sistema operativo Linux (en el laboratorio se utiliza la distribución Ubuntu).
- Sistema syslog instalado (Ubuntu ya lo trae por defecto).

Descripción

Distintas entidades (dispositivos y aplicaciones) en los sistemas operativos reportan mensajes de varios tipos y con diferentes contenidos. Estos mensajes pueden alertar de problemas de distintos nivel de gravedad o informar sobre un evento que ha sucedido. Los mensajes son enviados a un proceso (*sysklogd*) del sistema. Estos mensajes son guardados en ficheros log localizados en /var/log/ en los sistemas Linux. La consulta de estos ficheros permite conocer información valiosa sobre los accesos que ha habido en los sistemas o sobre los errores que han generado las aplicaciones y dispositivos.

Desde las aplicaciones desarrolladas por el usuario, es posible enviar mensajes de error al sistema log, mediante llamadas específicas (syslog).

Los mensajes de log se pueden clasificar por el nivel de severidad. Hay 8 posibles niveles, que se listan a continuación:

Nivel de seguridad	Denominación	Descripción
0	Emergency (emer)	System unusable
1	Alert (alert)	Inmediate action required
2	Critical (crit)	Cirtical condition
3	Erros (err)	Error condition
4	Warnings (warn)	Warning condition
5	Notifications (notice)	Normal but significant conditions
6	Informational (info)	Informational message
7	Debugging (debug)	Debbugging message

A su vez puede haber mensajes de distintos tipos en función de la fuente o naturaleza del mismo:

- ***Auth:*** mensajes de autenticación (proceso loggin en el sistema).
- ***Cron:*** mensajes del planificador.
- ***Daemon:*** mensajes de demonios corriendo en el sistema.
- ***Kern:*** mensajes del kernel.
- ***Lpr:*** mensajes de impresoras.
- ***Mail:*** mensajes del sistema de correo sendmail.
- ***User:*** mensajes de aplicaciones y procesos de usuario.
- ***Local0-local7:*** mensajes locales.
- ***Syslog:*** mensajes del propio sistema syslog.

Se puede configurar el sistema syslog para guardar los mensajes en ficheros diferentes en función de su severidad y/o fuente. Por ejemplo los mensajes del kernel de error (kern.err) se pueden guardar en un fichero concreto (error.log). O todos los mensajes de error (*.err), sin importar la fuente, o bien todos los mensajes de impresora sin importar el nivel de severidad (lpr.*).

Los ficheros que guardan los mensajes podrían crecer de forma indefinida con el tiempo, hay que configurar cómo el sistema syslog gestiona esto, por ejemplo se puede configurar que los reinicie cada semana, y guarde las últimas 4 semanas.

Los mensajes de log, además de enviarse a ficheros, pueden enviarse a otros dispositivos y aplicaciones (terminal, sendmail, host…).

Por defecto cada equipo guarda sus propios mensajes de logs; en una red puede ser interesante configurar los equipos para que envíen los mensajes de log a un sistema. Esto permite poder centralizar y tratar estos mensajes desde un sistema de gestión.

El principal objetivo de esta práctica es aprender a configurar un sistema de syslog remoto.

Realice los siguientes ejercicios y rellene la ficha adjunta en el anexo 1 con los resultados de los mismos.

IMPORTANTE: Antes de modificar los ficheros de configuración realice una copia de los mismos (p.e. cp /etc/syslog.conf /etc/syslog.conf.old), cuando acabe la sesión recupere estos ficheros (mv /etc/syslog.conf.old /etc/syslog.conf).

Desarrollo de la práctica

Ejercicio 1. Configurar un cliente syslog.

Configurar un cliente syslog para que envíe todos los mensajes y de todas las fuentes a un servidor remoto, y los guarde en el fichero /var/log/entreprise.log.

Ejercicio 2. Configurar el servidor syslog.

Realizar la configuración en el servidor para que reciba mensajes desde otros hosts.

Reiniciar el servicio (/etc/init.d/sysklogd restart) y verificar que se envían logs remotos, provocando eventos y verificando que se guardan en el fichero correspondiente.

Ejercicio 3. Verificar la configuración del ciclo de vida de los ficheros de logs.

Verificar la configuración del comportamiento del sistema ante los ficheros de configuración (/etc/logrotate.conf).

Ejercicio 4. Aplicaciones de gestión de log.

Buscar aplicaciones de gestión más avanzadas y comentar las ventajas que implica con respecto al esta implementación básica.

Presentación y evaluación

Cada alumno entregará al profesor los resultados de la práctica en el documento anexo, la semana siguiente a la de la realización de la práctica.

En caso de retraso en la fecha de entrega se producirá una penalización en la nota de la práctica.

Bibliografía

- Páginas man: sysklogd, syslog.conf, logrotate.conf.
- Manuales de ayudas, por ejemplo:
    - http://www.aboutdebian.com/syslog.htm

ANEXO 1.
Nombre y apellidos:

1. ¿Qué cambios ha realizado en el fichero de configuración del cliente de syslog.conf?

2. ¿Qué cambios ha realizado en la configuración del servidor?. ¿Cómo ha verificado su funcionamiento correcto?

3. ¿Cómo están configurados los ficheros de syslog en logrotate.conf?

4. ¿Qué ventaja aporta syslog-ng? ¿Indique alguna otra aplicación describiendo sus ventajas?