

SYSLOGD - Gestion de logs en sistemas Unix

By freed0m

Creado 22 Jun 2005 - 11:00

El sistema de registro de eventos de Unix es un servicio llamado syslog, permite llevar un registro detallado de los eventos que se están produciendo en el sistema, estos pueden ser originados tanto por el kernel como por aplicaciones del sistema.

El registro de estos eventos puede hacerse en ficheros tanto locales como remotos, según definamos a nuestro interés en el fichero `/etc/syslog.conf`.

Nuestro servicio syslogd puede estar configurado también para recibir eventos remotos de otros sistemas que soporten este protocolo como podrían ser firewalls, routers, etc.

Las reglas contenidas en este fichero se componen de dos partes, la primera parte que indica la **selección** y una segunda parte que corresponde a la **acción**. A su vez, **la selección se divide en dos partes separadas** en la notación con un punto, indicando la primera parte el **servicio que envía** el mensaje de registro y la segunda parte la **prioridad**.

POSIBLES SERVICIOS

auth: Mensajes de autenticación.

auth-priv: Mensajes de autenticación que no son creados por el sistema.

cron: Mensajes relacionados con el servicio Cron.

daemon: Mensajes relacionados con los servicios en ejecución.

kern: Mensajes relacionados por el kernel

lpr: Mensajes del servicio impresión.

mail: Mensajes del servicio Mail

news: Mensajes del servicio News.

mark: Mensajes de control.

security (auth): Mismo eventos que auth.

syslog: Mensajes del propio syslog.

user: Mensajes de los usuarios.

uucp: Mensajes generados por los servicios uucp.

local0 a local7: Eventos personalizables por el usuario.

PRIORIDADES ... de menos a más.

debug: Mensajes con prioridad de **depuración**.

info: Mensajes de carácter **informativo**.

notice: Mensajes con prioridad de **notificación**.

warning: Mensajes con prioridad de **advertencia**.

warn (warning): Mensajes con prioridad de **advertencia**.

err (error): Mensajes con prioridad **err**.

crit: Mensajes con prioridad **crítica**.

alert: Mensajes con prioridad de **alerta**.

emerg: Mensajes con prioridad **emergencia**.
panic (emerg): Mensajes con prioridad **emergencia**.

CARACTERES ESPECIALES EN SYSLOG.CONF

- **ASTERISCO *** se usa como comodín para indicar todas las prioridades si se ubica después del punto, o todos los servicios, si se ubica antes del punto.
Por ejemplo:

```
news.* /var/log/news
```

Guardaría en el fichero `/var/log/news` todos los mensajes referentes al servicio de news independientemente de su criticidad.

Sin embargo en el siguiente caso:

```
*.warn /var/log/warn
```

Lo que sucede es que todos los mensajes con una criticidad de warning se almacenarían en el fichero `/var/log/warn`

- **BLANCO ' '** indica que no hay prioridad definida para el servicio almacenado.
- **COMA ,** permite especificar múltiples servicios con el mismo patrón de prioridad en una línea.

En el ejemplo:

```
news,kern.=info /var/log/newsykernel
```

se almacenarían en el fichero `/var/log/newsykernel` todos los mensajes de cualquier prioridad y de los servicios de news y del kernel.

- **PUNTO Y COMA ;** podremos registrar los eventos de varios servicios y prioridades a un mismo destino, separándolos por `;`.

Por ejemplo:

```
*.=info;*.=notice /var/log/messages
```

registraría los eventos de carácter informativo y de notificación de todos los servicios en el fichero `/var/log/messages`.

- **IGUAL =** con este carácter podemos identificar el nivel de prioridad exacto de los mensajes que queremos almacenar en determinado fichero.

Por ejemplo:

```
*.=info /var/log/todoinfo
```

almacenaría en el fichero `/var/log/todoinfo` toda la información de nivel informativo de todos los servicios.

- **EXCLAMACIÓN !** cuando este caracter va precediendo a las prioridades sirve para ignorarlas, teniendo la posibilidad de escoger la prioridad especificada mediante (!=prioridad seleccionada).
Otra de las opciones es seleccionar la prioridad especificada más todas las de superiores con la notación (!prioridad).
Cuando se utiliza junto con los caracteres "=" y "!", el signo de exclamación debe preceder obligatoriamente al signo igual, de la forma "!=".

POSIBLES ACCIONES

- **FICHERO**

Podemos grabar en fichero la salida de los mensajes del sistema, indicando la ruta completa de acceso, si precedemos la entrada con el carácter "-" estaremos dejando en el búfer de memoria la información del log, aunque esto puede provocar la pérdida de información si el sistema se para después de un intento de escritura a disco, se puede obtener un sustancial incremento de la velocidad, característica a tener en cuenta cuando se estén ejecutando programas que mandan una importante cantidad de mensajes a syslogd.

- **DISPOSITIVO FÍSICO**

Tenemos la opción de enviar los eventos del sistema a un dispositivo físico, habitualmente una terminal o una impresora. Esta configuración suele emplearse para dar mayor veracidad a los eventos, ya que su posible modificación en función del dispositivo será menor.

En el caso:

```
*.* /dev/tty12
```

Enviamos todos los mensajes del sistema al terminal 12.

```
kern.crit /dev/console
```

Enviamos todos los mensajes del kernel con prioridad crítica a la consola.

- **TUBERIA CON NOMBRE (Pipe)**

Algunas versiones de syslogd permiten enviar los eventos a ficheros de tipo pipe indicándolo con el símbolo |, dicho fichero ha de ser creado antes de iniciar syslogd, mediante **mkfifo** (Make FIFOs (named pipes) with the specified names) o **mknod** (mknod - make block or character special files).

Estas opciones son útiles para depurar aplicaciones y también cuando se quieren procesar los registros de eventos con cualquier aplicación.

En este ejemplo:

```
*.* |/var/log/ficherofifo
```

estaremos enviando a `ficherofifo` de tipo pipe la información de todos los eventos del sistema.

- **SISTEMA REMOTO**

Si queremos almacenar los eventos de nuestro sistema en una máquina remota, la nomenclatura es la misma que para otros casos, salvo que en esta situación, utilizaremos el carácter @precediendo al nombre de host o a su ip.

Por ejemplo:

```
mail.* @hardlock.net
```

Log del sistema remoto donde estamos registrando nuestros eventos generados por el daemon de correo.

```
Jun 14 20:25:17 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGIN, user=freed0m, ip=[::ffff:192.168.192.34]
Jun 14 20:25:17 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGOUT, user=freed0m, ip=[::ffff:192.168.192.34], top=0, retr=0,
time=0
Jun 14 20:25:54 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGIN, user=freed0m, ip=[::ffff:192.168.192.34]
Jun 14 20:25:54 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGOUT, user=freed0m, ip=[::ffff:192.168.192.34], top=0, retr=0,
time=0
Jun 14 20:29:30 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGIN, user=freed0m, ip=[::ffff:192.168.192.34]
Jun 14 20:29:30 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGOUT, user=freed0m, ip=[::ffff:192.168.192.34], top=0, retr=0,
time=0
Jun 14 20:32:09 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGIN, user=freed0m, ip=[::ffff:192.168.192.34]
Jun 14 20:32:09 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGOUT, user=freed0m, ip=[::ffff:192.168.192.34], top=0, retr=0,
time=0
Jun 14 20:35:28 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGIN, user=freed0m, ip=[::ffff:192.168.192.34]
Jun 14 20:35:28 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGOUT, user=freed0m, ip=[::ffff:192.168.192.34], top=0, retr=0,
time=0
Jun 14 20:35:40 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGIN, user=freed0m, ip=[::ffff:192.168.192.34]
Jun 14 20:35:40 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGOUT, user=freed0m, ip=[::ffff:192.168.192.34], top=0, retr=0,
time=0
Jun 14 20:48:52 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGIN, user=freed0m, ip=[::ffff:192.168.192.34]
Jun 14 20:48:53 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGOUT, user=freed0m, ip=[::ffff:192.168.192.34], top=0, retr=0,
time=0
Jun 14 20:54:06 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGIN, user=freed0m, ip=[::ffff:192.168.192.34]
Jun 14 20:54:07 172.red-80-35-173.pooles.rima-tde.net pop3d-ssl:
LOGOUT, user=freed0m, ip=[::ffff:192.168.192.34], top=0, retr=0,
time=0
```

▪ USUARIOS DEL SISTEMA

Si queremos enviar los eventos a los usuarios conectados en el sistema, se especifica la lista de usuarios que deben recibir un tipo de mensajes escribiendo sus nombres de usuario separados por comas:

Por ejemplo:

```
*.alert root, freed0m
```

- **TODOS LOS USUARIOS DEL SISTEMA**

Para enviar los eventos del sistema a todos los usuarios conectados, utilizaremos el caracter * en el campo de acción.

Por ejemplo:

```
*.=emerg *
```

Esta configuración enviaría mediante `wall` a todos los usuarios conectados al sistema los eventos de emergencia.

FICHEROS DE LOG IMPORTANTES

syslog es probablemente el fichero de log más importante del sistema, se guardan en texto claro, los mensajes relativos a la **seguridad** del sistema, accesos e intentos de acceso a servicios. En función de la configuración del daemon **syslogd** la información almacenada será una u otra.

messages se almacenan los datos **informativos** prioridad baja o media.

utmp archivo binario donde se almacena información relativa a la **conexión/desconexión de usuarios** al sistema. Formato utmp (Usuario, Tipo de conexión, Fecha de la conexión, tipo de conexión).

utmp archivo binario donde se almacena información relativa a los **usuarios conectados** en un momento determinado.

lastlog fichero binario donde se guarda la información relativa a la última conexión de usuario con fecha y hora.

faillog fichero binario donde se almacena la información del último intento de **acceso fallido** .

loginlog intentos fallidos de login cuando se han producido 5 o más seguidos.

btmpt intentos fallidos de conexión al sistema.

Referencias: <http://es.tldp.org/>

Source URL:

<http://www.hacktimes.com/?q=node/21>