Reporte Logs

Héctor Andrey Hernández Alonso

Ingeniería en Informática 2015

249757

201501400580

Administración de Sistemas

Grupo 240003

14 de noviembre 2018

1. Resumen

Los archivos de registro son los registros que Linux almacena para que los administradores realicen un seguimiento y controlen los eventos importantes sobre el servidor, el kernel, los servicios y las aplicaciones que se ejecutan en él.

Linux proporciona un repositorio centralizado de archivos de registro que se pueden ubicar en el directorio **/ var / log**.

2. Contenido

Los archivos de registro generados en un entorno Linux generalmente se pueden clasificar en cuatro categorías diferentes:

1) Registros de aplicaciones
2) Registros de eventos
3) Registros de servicio
4) Registros del sistema

Directorios en /var/log

- /var/log/message: registro de los mensajes generales del sistema.
- /var/log/auth.log: log de autenticación.
- /var/log/kern.log: registro del kernel, muy interesante para detectar problemas con el núcleo.
- /var/log/cron.log: registro de la herramienta de crond
- /var/log/maillog: registro del servidor de emails.
- /var/log/qmail: registro de Qmail.
- /var/log/httpd: registro de errores y accesos del servidor web Apache
- /var/log/lightpd: registro de errores y acceso a Lighttpd.
- /var/log/boot.log: registro de inicio del sistema, si se producen problemas al inicio, es aquí donde tenemos que acudir.
- /var/log/mysqld.log: registro para la base de datos MySQL.
- /var/log/secure: log de autenticación, muy importante para la seguridad, ya que podrás ver lo referente a la autenticación del sistema.
- /var/log/utmp o /var/log/wtmp: registro de logins.

Al monitorear los archivos de registro de Linux, puede obtener información detallada sobre el rendimiento del servidor, la seguridad, los mensajes de error y los problemas subyacentes.

Permiten anticipar los próximos problemas antes de que realmente ocurran.

Funcionamiento del Sistema de Logs

El sistema de logs arranca con el script **/etc/init.d/sysklogd**:

- **syslogd**: gestiona los logs del sistema. Distribuye los mensajes a archivos usando las indicaciones especificadas en su archivo de configuración **/etc/syslog.conf**, donde se indica qué se loguea y a dónde se envían estos logs.
- **klogd**: se encarga de los logs del kernel.

Los logs se guardan en archivos ubicados en el directorio **/var/log**,

- **/var/log/messages**: aquí se encuentran los logs que llegan con prioridad info (información), notice (notificación) o warn (aviso).
- **/var/log/kern.log**: aquí se almacenan los logs del kernel, generados por **klogd**.
- **/var/log/auth.log:** en este log se registran los login en el sistema. Los intentos fallidos se registran en líneas con información del tipo invalid password o authentication failure.
- **/var/log/dmesg:** en este archivo se almacena la información que genera el kernel durante el arranque del sistema.

```
$ tail -f /var/log/messages
```

Muestra las últimas líneas de uno o más archivos de texto (por defecto las diez últimas), pero con la opción -f, en lugar de mostrar las últimas diez líneas y terminar, tail seguirá activo y conforme se añadan nuevas líneas al fichero las imprimirá.

```
# logger -t mi_programa -f /var/log/messages "Mensaje ejemplo"
```

Permite generar logs.

```
head example.log
```

Permite ver las primeras diez líneas de un archivo

Conclusión

Los registros de Linux proporcionan una línea de tiempo de eventos para el sistema operativo Linux, las aplicaciones y el sistema, y son una herramienta valiosa para la solución de problemas cuando surgen problemas.

Bibliografías

- https://help.ubuntu.com/community/LinuxLogFiles
- https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/
- https://www.linuxadictos.com/conoce-los-ficheros-de-registro-logs-de-linux.html
- http://www.estrellateyarde.org/logs-en-linux
- https://help.ubuntu.com/community/LinuxLogFiles
- https://stackify.com/linux-logs/