Gestión de logs

Un aspecto fundamental a la hora de administrar un sistema operativo son los logs. Los logs llevan registro de las acciones ejecutadas por los procesos que utilizan algún tipo de control de registro de actividad.

Systemd permite gestionar este aspecto de forma nativa, manteniendo control, registro y seguimiento de las actividades de log del sistema. Incluye también herramientas para visualizar y gestionar los logs

Comando journalctl

Este es el comando para consultar los logs gestionados por systemd. Admite muchas e interesantes opciones, veamos algunas de ellas

- **-b**: muestra los mensajes solamente desde el último inicio
    - **-n**: siendo, n un número natural (1,2,3...), acompañando al parámetro -b: muestra información de ?n? inicio atrás. Para poder utilizar esta opción es necesario que esté activada la persistencia del journal. Para ello editamos el archivo **/etc/systemd/journald.conf** y establecemos la directiva **Storage=persistent**.
- **-n número**: indica las n últimas líneas del log, (similar al -n del comando tail)
- **-u**: permite especificar un unit para ver solamente los logs asociados a esa unit
- **-k:** muestra los mensajes del kernel
- **-p**: permite filtrar logs nivel de severidad (emerg, alert, crit, err, warning, notice, info, debug)
- **-f**: muestra logs ?en vivo? (similar al tail -f)
- **-o**: indica el tipo de formato para la información de salida (json, json-pretty, cat, export...)

Otra opción interesante permite filtrar por marcas de tiempo

- **--since**: indica el instante inicial desde el que se muestran los logs
- **--until**: indica el instante final hasta el que se muestran los logs

También se pueden ver los logs de un ejecutable, indicando su path en la ruta:

```
journalctl /usr/bin/bash
```

mostraría los logs correspondientes al ejecutable bash

Veamos algún otro ejemplo

```
journalctl --since yesterday -u nginx.service
```

muestra las líneas de log correspondientes al unit nginx.service desde ayer

```
journalctl -b -k
```

mostraría las líneas de mensajes de log del kernel desde el último inicio

```
journalctl -f -u nginx.service
```

mostraría las líneas de log del unit nginx.service en vivo

```
journalctl -k -10
```

mostraría las 10 últimas líneas del journal relativas a mensajes enviados por el kernel

```
journalctl -b 2 -k
```

mostraría los mensajes del kernel de 2 inicios antes del sistema. Este comando funcionaría solo en caso de que estuviera habilitada la persistencia de mensajes del journal

Volver

JavierFP 17:44 11 dec 2017 (CET)