journalctl

Funcionamiento

El comando journalctl nos permite hacer consultas sobre los registros que el journald administra. Algunas de sus opciones las vemos a continuación:

- -b [N]: muestra los mensajes del arranque del sistema N, siendo 0 el arranque actual, 1 el anterior, ...
- -D: permite especificar la ruta del journal que se quiere consultar
- -e: muestra todos los mensajes y se va al final
- -f: permite ver los mensajes mientras se van produciendo
- -k: filtra los mensajes relacionados con el kernel
- -n [N]: muestra los N últimos mensajes
- -o: permite definir los parámetros de salida
- -p [PRI]: muestra los mensajes con prioridad igual o superior a la indicada
- -r muesrta los resultados en orden inverso
- -u [UNIT] muestra sólo mensajes relacionados con la unit indicada
- -no-pager: no pagina la salida de datos
- -since=[]: muestra los mensajes a partir de una fecha especificada
- -state: muestra las unidades que se encuentran en el estado indicado
- -vaccum-size: limita el tamaño de los ficheros en /var/log/journal
- -vaccum-time: limita la antigüedad de los ficheros en /var/log/journal
- -until=[N]: muestra los mensajes hasta una fecha
- -utc: muestra la salida del log en formato UTC

Si utilizamos la opción -o (verbose) podemos ver más campos de la entrada de journal que por defecto no se muestran. Estos campos también pueden ser utilizados para hacer búsquedas dentro de journald.

```
# journalctl -o verbose
Mon 2018-04-09 15:31:32.454210 UTC
[s=ca88f19f93c14f0a9f91159b4ae5bf11;i=ba9;b=5dc54ed59edf429a988ce2b91fc98ebe
;m=18dadcd52;t=5696c19b86e82;x=cdf91bf55028befa]
  PRIORITY=5
  _BOOT_ID=5dc54ed59edf429a988ce2b91fc98ebe
  _MACHINE_ID=ada7a6dc422f4f538eb35a9980cbc46e
  _HOSTNAME=virtual
  _SYSTEMD_SLICE=system.slice
  _TRANSPORT=syslog
  SYSLOG_IDENTIFIER=dbus
  SYSLOG_PID=394
  _PID=394
  _UID=107
  _GID=111
  _COMM=dbus-daemon
  _EXE=/usr/bin/dbus-daemon
```

```
  _CMDLINE=/usr/bin/dbus-daemon --system --address=systemd: --nofork --
nopidfile --systemd-activation
  _CAP_EFFECTIVE=20000000
  _SYSTEMD_CGROUP=/system.slice/dbus.service
  _SYSTEMD_UNIT=dbus.service
  _SYSTEMD_INVOCATION_ID=37e2eb3bff2d4fe5bccebcb7c5219c96
  SYSLOG_FACILITY=4
  MESSAGE=[system] Failed to activate service 'org.bluez': timed out
  _SOURCE_REALTIME_TIMESTAMP=1523287892454210
```

De esta manera podemos hacer búsqueda como la siguiente:

```
# journalctl _PÎD=3454
# journalctl _UID=27
...
```