Dernière mise-à-jour : 2024/10/14 13:14

LDF208 - Gestion de la Journalisation

Contenu du Module

Présentation

La majorité des journaux du système et des applications se trouve dans le répertoire **/var/log**.

> **Important** : Il est conseillé de déplacer le point de montage du répertoire **/var/log** sur une partition physique ou un volume logique à part. De cette façon, en cas de journalisation rapide trop bavarde la limite de la taille de ce répertoire est celle de la taille de la partition physique ou du volume logique. Si vous laissez ce répertoire dans la racine du système, il existe un risque à ce que les journaux grossissent si vite qu'ils occupent toute l'espace disque libre, créant ainsi un crash système.

La Commande dmesg

Cette commande retourne les messages du noyau (***Kernel Ring Buffer***) stockés dans le fichier **/var/log/dmesg** lors du dernier démarrage du système :

```
root@debian8:~# dmesg | more
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Initializing cgroup subsys cpuacct
[    0.000000] Linux version 3.16.0-4-686-pae (debian-kernel@lists.debian.org) (gcc version 4.8.4 (De
bian 4.8.4-1) ) #1 SMP Debian 3.16.7-ckt11-1+deb8u5 (2015-10-09)
[    0.000000] e820: BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
[    0.000000] BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] SMBIOS 2.5 present.
[    0.000000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[    0.000000] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.000000] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.000000] e820: last_pfn = 0x3fff0 max_arch_pfn = 0x1000000
[    0.000000] MTRR default type: uncachable
[    0.000000] MTRR variable ranges disabled:
[    0.000000] x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
[    0.000000] CPU MTRRs all blank - virtualized system.
[    0.000000] initial memory mapped: [mem 0x00000000-0x01bfffff]
--More--
```

Options de la Commande

Les option de cette commande sont :

```
root@debian8:~# dmesg --help

Usage:
 dmesg [options]

Options:
 -C, --clear                 clear the kernel ring buffer
 -c, --read-clear            read and clear all messages
 -D, --console-off           disable printing messages to console
 -E, --console-on            enable printing messages to console
 -F, --file <file>           use the file instead of the kernel log buffer
 -f, --facility <list>       restrict output to defined facilities
 -H, --human                 human readable output
 -k, --kernel                display kernel messages
 -L, --color[=<when>]        colorize messages (auto, always or never)
 -l, --level <list>          restrict output to defined levels
 -n, --console-level <level> set level of messages printed to console
 -P, --nopager               do not pipe output into a pager
 -r, --raw                   print the raw message buffer
 -S, --syslog                force to use syslog(2) rather than /dev/kmsg
 -s, --buffer-size <size>    buffer size to query the kernel ring buffer
 -u, --userspace             display userspace messages
 -w, --follow                wait for new messages
 -x, --decode                decode facility and level to readable string
 -d, --show-delta            show time delta between printed messages
 -e, --reltime               show local time and time delta in readable format
 -T, --ctime                 show human readable timestamp
 -t, --notime                don't print messages timestamp
     --time-format <format>  show time stamp using format:
```

```
                                  [delta|reltime|ctime|notime|iso]
Suspending/resume will make ctime and iso timestamps inaccurate.

 -h, --help     display this help and exit
 -V, --version  output version information and exit

Supported log facilities:
    kern - kernel messages
    user - random user-level messages
    mail - mail system
  daemon - system daemons
    auth - security/authorization messages
  syslog - messages generated internally by syslogd
     lpr - line printer subsystem
    news - network news subsystem

Supported log levels (priorities):
   emerg - system is unusable
   alert - action must be taken immediately
    crit - critical conditions
     err - error conditions
    warn - warning conditions
  notice - normal but significant condition
    info - informational
   debug - debug-level messages


For more details see dmesg(1).
```

Surveillance Sécuritaire

La Commande last

Cette commande indique les dates et heures des connexions des utilisateurs à partir du contenu du fichier **/var/log/wtmp** :

```
root@debian8:~# last
trainee  pts/0        :0               Mon Oct 26 14:21   still logged in
trainee  pts/0        :0               Mon Oct 26 14:15 - 14:19  (00:04)
trainee  :0           :0               Mon Oct 26 13:52   still logged in
reboot   system boot  3.16.0-4-686-pae Mon Oct 26 13:51 - 14:28 (2+00:36)
trainee  pts/0        :0               Mon Oct 26 13:10 - crash  (00:40)
trainee  :0           :0               Mon Oct 26 11:22 - crash  (02:28)
reboot   system boot  3.16.0-4-686-pae Mon Oct 26 11:22 - 14:28 (2+03:05)
trainee  pts/0        :0               Fri Oct 23 17:00 - crash (2+19:21)
trainee  :0           :0               Fri Oct 23 17:00 - crash (2+19:21)
reboot   system boot  3.16.0-4-686-pae Fri Oct 23 16:59 - 14:28 (4+22:28)
trainee  pts/0        :0               Fri Oct 23 16:51 - 16:59  (00:08)
trainee  :0           :0               Fri Oct 23 16:50 - 16:59  (00:09)
reboot   system boot  3.16.0-4-686-pae Fri Oct 23 16:50 - 16:59  (00:09)
reboot   system boot  3.16.0-4-686-pae Fri Oct 23 16:47 - 16:59  (00:12)

wtmp begins Fri Oct 23 16:47:17 2015
```

Options de la Commande

Les option de cette commande sont :

```
root@debian8:~# last --help
last: invalid option -- '-'
Usage: last [-num | -n num] [-f file] [-t YYYYMMDDHHMMSS] [-R] [-adioxFw] [username..] [tty..]
```

La Commande lastlog

Cette commande indique les dates et heures de la connexion au système la plus récente des utilisateurs :

```
root@debian8:~# lastlog
Username         Port     From             Latest
root                                       **Never logged in**
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
nobody                                     **Never logged in**
systemd-timesync                           **Never logged in**
systemd-network                            **Never logged in**
systemd-resolve                            **Never logged in**
systemd-bus-proxy                           **Never logged in**
messagebus                                 **Never logged in**
pulse                                      **Never logged in**
avahi                                      **Never logged in**
uuidd                                      **Never logged in**
Debian-exim                                **Never logged in**
```

```
statd                                          **Never logged in**
avahi-autoipd                                  **Never logged in**
colord                                         **Never logged in**
dnsmasq                                        **Never logged in**
geoclue                                        **Never logged in**
speech-dispatcher                               **Never logged in**
sshd                                           **Never logged in**
rtkit                                          **Never logged in**
saned                                          **Never logged in**
usbmux                                         **Never logged in**
hplip                                          **Never logged in**
lightdm                                        **Never logged in**
trainee                                        **Never logged in**
vboxadd                                        **Never logged in**
```

Options de la Commande

Les option de cette commande sont :

```
root@debian8:~# lastlog --help
Usage: lastlog [options]

Options:
  -b, --before DAYS             print only lastlog records older than DAYS
  -h, --help                    display this help message and exit
  -R, --root CHROOT_DIR         directory to chroot into
  -t, --time DAYS               print only lastlog records more recent than DAYS
  -u, --user LOGIN              print lastlog record of the specified LOGIN
```

La Commande lastb

Cette commande indique les dates et heures des connexions infructueueses des utilisateurs à partir du contenu du fichier **/var/log/btmp** :

```
root@debian8:~# lastb
trainee  :0           :0               Wed Oct 28 15:01 - 15:01  (00:00)
trainee  :0           :0               Wed Oct 28 15:01 - 15:01  (00:00)
trainee  :0           :0               Wed Oct 28 15:01 - 15:01  (00:00)
trainee  :0           :0               Wed Oct 28 15:01 - 15:01  (00:00)
trainee  :0           :0               Wed Oct 28 15:01 - 15:01  (00:00)
trainee  :0           :0               Wed Oct 28 15:01 - 15:01  (00:00)
trainee  :0           :0               Wed Oct 28 15:01 - 15:01  (00:00)

btmp begins Wed Oct 28 15:01:05 2015
```

Options de la Commande

Les options de cette commande sont :

```
root@debian8:~# lastb --help
lastb: invalid option -- '-'
Usage: lastb [-num | -n num] [-f file] [-t YYYYMMDDHHMMSS] [-R] [-adioxFw] [username..] [tty..]
```

Le fichier /var/log/auth.log

Sous Debian, ces mêmes informations se trouvent dans le fichier **/var/log/auth.log** :

```
root@debian8:~# tail -n 15 /var/log/auth.log
Oct 28 14:29:01 debian8 CRON[4497]: pam_unix(cron:session): session closed for user trainee
Oct 28 14:30:01 debian8 CRON[4504]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 14:30:01 debian8 CRON[4504]: pam_unix(cron:session): session closed for user trainee
Oct 28 14:31:01 debian8 CRON[4508]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 14:31:01 debian8 CRON[4508]: pam_unix(cron:session): session closed for user trainee
```

```
Oct 28 14:31:30 debian8 su[1558]: pam_unix(su:session): session closed for user root
Oct 28 14:31:36 debian8 su[4513]: pam_unix(su:auth): authentication failure; logname=trainee uid=1000 euid=0
tty=/dev/pts/0 ruser=trainee rhost=  user=root
Oct 28 14:31:38 debian8 su[4513]: pam_authenticate: Authentication failure
Oct 28 14:31:38 debian8 su[4513]: FAILED su for root by trainee
Oct 28 14:31:38 debian8 su[4513]: - /dev/pts/0 trainee:root
Oct 28 14:31:46 debian8 su[4514]: Successful su for root by trainee
Oct 28 14:31:46 debian8 su[4514]: + /dev/pts/0 trainee:root
Oct 28 14:31:46 debian8 su[4514]: pam_unix(su:session): session opened for user root by trainee(uid=1000)
Oct 28 14:32:01 debian8 CRON[4522]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 14:32:01 debian8 CRON[4522]: pam_unix(cron:session): session closed for user trainee
```

Le fichier /var/log/audit/audit.log

Ce fichier contient les messages du système d'audit, appelés des **évènements**. Le système audit est installé par défaut dans RHEL/CentOS par le paquet **audit**. Le système audit collectionne des informations telles :

- des appels système,
- des accès aux fichiers,
- des informations en provenance de SELinux.

Le système d'audit n'est pas installé par défaut sous Debian. Pour l'installer, utilisez la commande apt-get :

```
root@debian8:~# apt-get install auditd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libauparse0
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
```

```
  auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 262 kB of archives.
After this operation, 712 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.fr.debian.org/debian/ jessie/main libauparse0 i386 1:2.4-1+b1 [48.7 kB]
Get:2 http://ftp.fr.debian.org/debian/ jessie/main auditd i386 1:2.4-1+b1 [213 kB]
Fetched 262 kB in 1s (168 kB/s)
Selecting previously unselected package libauparse0:i386.
(Reading database ... 167450 files and directories currently installed.)
Preparing to unpack .../libauparse0_1%3a2.4-1+b1_i386.deb ...
Unpacking libauparse0:i386 (1:2.4-1+b1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a2.4-1+b1_i386.deb ...
Unpacking auditd (1:2.4-1+b1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Processing triggers for systemd (215-17+deb8u2) ...
Setting up libauparse0:i386 (1:2.4-1+b1) ...
Setting up auditd (1:2.4-1+b1) ...
update-rc.d: warning: start and stop actions are no longer supported; falling back to defaults
Processing triggers for libc-bin (2.19-18+deb8u1) ...
Processing triggers for systemd (215-17+deb8u2) ...
```

A l'issu de quelques minutes, consultez le fichier **/var/log/audit.log** :

```
root@debian8:~# tail -n 15 /var/log/audit/audit.log
type=USER_START msg=audit(1446039481.860:899): pid=4559 uid=0 auid=1000 ses=443 msg='op=PAM:session_open
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1446039481.864:900): pid=4559 uid=0 auid=1000 ses=443 msg='op=PAM:setcred acct="trainee"
exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1446039481.864:901): pid=4559 uid=0 auid=1000 ses=443 msg='op=PAM:session_close
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=USER_ACCT msg=audit(1446039541.874:902): pid=4567 uid=0 auid=4294967295 ses=4294967295
msg='op=PAM:accounting acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
```

```
type=CRED_ACQ msg=audit(1446039541.874:903): pid=4567 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1446039541.874:904): pid=4567 uid=0 old-auid=4294967295 auid=1000 old-ses=4294967295 ses=444
res=1
type=USER_START msg=audit(1446039541.874:905): pid=4567 uid=0 auid=1000 ses=444 msg='op=PAM:session_open
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1446039541.878:906): pid=4567 uid=0 auid=1000 ses=444 msg='op=PAM:setcred acct="trainee"
exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1446039541.878:907): pid=4567 uid=0 auid=1000 ses=444 msg='op=PAM:session_close
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=USER_ACCT msg=audit(1446039601.888:908): pid=4571 uid=0 auid=4294967295 ses=4294967295
msg='op=PAM:accounting acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1446039601.888:909): pid=4571 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1446039601.888:910): pid=4571 uid=0 old-auid=4294967295 auid=1000 old-ses=4294967295 ses=445
res=1
type=USER_START msg=audit(1446039601.888:911): pid=4571 uid=0 auid=1000 ses=445 msg='op=PAM:session_open
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1446039601.896:912): pid=4571 uid=0 auid=1000 ses=445 msg='op=PAM:setcred acct="trainee"
exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1446039601.896:913): pid=4571 uid=0 auid=1000 ses=445 msg='op=PAM:session_close
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
```

Gestion des évènements audit

La gestion des évènements audit se repose sur trois exécutables :

auditd

Cet exécutable est le daemon du système audit. Il est responsable de l’écriture des enregistrements audit sur disque. Son fichier de configuration est le **/etc/audit/auditd.conf** :

```
root@debian8:~# cat /etc/audit/auditd.conf
#
# This file controls the configuration of the audit daemon
#

log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 5
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 6
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
```

Options de la Commande

Les option de cette commande sont :

```
root@debian8:~# auditd --help
auditd: invalid option -- '-'
Usage: auditd [-f] [-l] [-n] [-s disable|enable|nochange]
```

auditctl

Cet exécutable est utilisé pour configurer les règles du système audit. Au démarrage, auditctl lit et applique les règles contunues dans le fichier **/etc/audit/audit.rules** :

```
root@debian8:~# cat /etc/audit/audit.rules
# This file contains the auditctl rules that are loaded
# whenever the audit daemon is started via the initscripts.
# The rules are simply the parameters that would be passed
# to auditctl.

# First rule - delete all
-D

# Increase the buffers to survive stress events.
# Make this bigger for busy systems
-b 320

# Feel free to add below this line. See auditctl man pag
```

Options de la Commande

Les options de cette commande sont :

```
root@debian8:~# auditctl --help
usage: auditctl [options]
    -a <l,a>            Append rule to end of <l>ist with <a>ction
    -A <l,a>            Add rule at beginning of <l>ist with <a>ction
    -b <backlog>        Set max number of outstanding audit buffers
                        allowed Default=64
    -c                  Continue through errors in rules
    -C f=f              Compare collected fields if available:
                        Field name, operator(=,!=), field name
    -d <l,a>            Delete rule from <l>ist with <a>ction
                        l=task,exit,user,exclude
                        a=never,always
    -D                  Delete all rules and watches
    -e [0..2]           Set enabled flag
    -f [0..2]           Set failure flag
                        0=silent 1=printk 2=panic
    -F f=v              Build rule: field name, operator(=,!=,<,>,<=,
                        >=,&,&=) value
    -h                  Help
    -i                  Ignore errors when reading rules from file
    -k <key>            Set filter key on audit rule
    -l                  List rules
    -m text             Send a user-space message
    -p [r|w|x|a]        Set permissions filter on watch
                        r=read, w=write, x=execute, a=attribute
    -q <mount,subtree>  make subtree part of mount point's dir watches
    -r <rate>           Set limit in messages/sec (0=none)
    -R <file>           read rules from file
    -s                  Report status
    -S syscall          Build rule: syscall name or number
    -t                  Trim directory watches
    -v                  Version
    -w <path>           Insert watch at <path>
    -W <path>           Remove watch at <path>
```

```
    --loginuid-immutable   Make loginuids unchangeable once set
```

audispd

Cet exécutable est responsable de la distribution des évènements audit à des applications tierces. Le démarrage et l'arrêt de cet exécutable est contrôlé par **auditd**. Afin d'informer **audispd** de la façon dont elles veulent recevoir les informations concernant les évènements, les applications placent un fichier de configuration dans le répertoire **/etc/audisp/plugins.d** :

```
root@debian8:~# ls /etc/audisp/plugins.d
af_unix.conf  syslog.conf
```

Le contenu de ces fichiers suit un format précis :

```
root@debian8:~# cat /etc/audisp/plugins.d/syslog.conf
# This file controls the configuration of the syslog plugin.
# It simply takes events and writes them to syslog. The
# arguments provided can be the default priority that you
# want the events written with. And optionally, you can give
# a second argument indicating the facility that you want events
# logged to. Valid options are LOG_LOCAL0 through 7.

active = no
direction = out
path = builtin_syslog
type = builtin
args = LOG_INFO
format = string
```

La consultation des évènements audit

La consultation des évènements audit se fait en utilisant les commandes **ausearch** et **aureport** :

La Commande aureport

Cette commande est utilisée pour générer des rapports :

```
root@debian8:~# aureport

Summary Report
======================
Range of time in logs: 10/28/2015 06:37:21.563 - 10/28/2015 14:48:01.088
Selected time for report: 10/28/2015 06:37:21 - 10/28/2015 14:48:01.088
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 1
Number of failed authentications: 1
Number of users: 3
Number of terminals: 3
Number of host names: 1
Number of executables: 3
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 0
Number of process IDs: 163
Number of events: 959
```

Les options de cette commande sont :

```
root@debian8:~# aureport --help
usage: aureport [options]
    -a,--avc            Avc report
    -au,--auth            Authentication report
    -c,--config            Config change report
    -cr,--crypto            Crypto report
    -e,--event            Event report
    -f,--file            File name report
    --failed            only failed events in report
    -h,--host            Remote Host name report
    --help                help
    -i,--interpret            Interpretive mode
    -if,--input <Input File name>    use this file as input
    --input-logs            Use the logs even if stdin is a pipe
    -l,--login            Login report
    -k,--key            Key report
    -m,--mods            Modification to accounts report
    -ma,--mac            Mandatory Access Control (MAC) report
    -n,--anomaly            aNomaly report
    -nc,--no-config            Don't include config events
    --node <node name>        Only events from a specific node
    -p,--pid            Pid report
    -r,--response            Response to anomaly report
    -s,--syscall            Syscall report
    --success            only success events in report
    --summary            sorted totals for main object in report
    -t,--log            Log time range report
    -te,--end [end date] [end time]    ending date & time for reports
    -tm,--terminal            TerMinal name report
    -ts,--start [start date] [start time]    starting data & time for reports
    --tty                Report about tty keystrokes
    -u,--user            User name report
    -v,--version            Version
    -x,--executable            eXecutable name report
```

```
    If no report is given, the summary report will be displayed
```

La Commande ausearch

Cette commande est utilisée pour rechercher des évènements. Par exemple, pour rechercher les évènements liés à un utilisateur représenté par son UID :

```
root@debian8:~# ausearch -ui 1000 | more
----
time->Wed Oct 28 14:31:30 2015
type=USER_END msg=audit(1446039090.595:853): pid=1558 uid=1000 auid=1000 ses=2 msg='op=PAM:session_cl
ose acct="root" exe="/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'
----
time->Wed Oct 28 14:31:30 2015
type=CRED_DISP msg=audit(1446039090.595:854): pid=1558 uid=1000 auid=1000 ses=2 msg='op=PAM:setcred a
cct="root" exe="/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'
----
time->Wed Oct 28 14:31:38 2015
type=USER_AUTH msg=audit(1446039098.083:855): pid=4513 uid=1000 auid=1000 ses=2 msg='op=PAM:authentic
ation acct="root" exe="/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=failed'
----
time->Wed Oct 28 14:31:46 2015
type=USER_AUTH msg=audit(1446039106.663:856): pid=4514 uid=1000 auid=1000 ses=2 msg='op=PAM:authentic
ation acct="root" exe="/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'
----
time->Wed Oct 28 14:31:46 2015
type=USER_ACCT msg=audit(1446039106.663:857): pid=4514 uid=1000 auid=1000 ses=2 msg='op=PAM:accountin
g acct="root" exe="/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'
----
time->Wed Oct 28 14:31:46 2015
type=CRED_ACQ msg=audit(1446039106.663:858): pid=4514 uid=1000 auid=1000 ses=2 msg='op=PAM:setcred ac
--More--
```

Options de la Commande

Les options de cette commande sont :

```
root@debian8:~# ausearch --help
usage: ausearch [options]
    -a,--event <Audit event id>    search based on audit event id
    --arch <CPU>            search based on the CPU architecture
    -c,--comm  <Comm name>        search based on command line name
    --checkpoint <checkpoint file>    search from last complete event
    --debug            Write malformed events that are skipped to stderr
    -e,--exit  <Exit code or errno>    search based on syscall exit code
    -f,--file  <File name>        search based on file name
    -ga,--gid-all <all Group id>    search based on All group ids
    -ge,--gid-effective <effective Group id>  search based on Effective
                    group id
    -gi,--gid <Group Id>        search based on group id
    -h,--help            help
    -hn,--host <Host Name>        search based on remote host name
    -i,--interpret            Interpret results to be human readable
    -if,--input <Input File name>    use this file instead of current logs
    --input-logs            Use the logs even if stdin is a pipe
    --just-one            Emit just one event
    -k,--key  <key string>        search based on key field
    -l, --line-buffered        Flush output on every line
    -m,--message  <Message type>    search based on message type
    -n,--node  <Node name>        search based on machine's name
    -o,--object  <SE Linux Object context> search based on context of object
    -p,--pid  <Process id>        search based on process id
    -pp,--ppid <Parent Process id>    search based on parent process id
    -r,--raw            output is completely unformatted
    -sc,--syscall <SysCall name>    search based on syscall name or number
    -se,--context <SE Linux context> search based on either subject or
```

```
                  object
    --session <login session id>    search based on login session id
    -su,--subject <SE Linux context> search based on context of the Subject
    -sv,--success <Success Value>    search based on syscall or event
                  success value
    -te,--end [end date] [end time]    ending date & time for search
    -ts,--start [start date] [start time]    starting data & time for search
    -tm,--terminal <TerMinal>    search based on terminal
    -ua,--uid-all <all User id>    search based on All user id's
    -ue,--uid-effective <effective User id>  search based on Effective
                  user id
    -ui,--uid <User Id>        search based on user id
    -ul,--loginuid <login id>    search based on the User's Login id
    -uu,--uuid <guest UUID>        search for events related to the virtual
                  machine with the given UUID.
    -v,--version            version
    -vm,--vm-name <guest name>    search for events related to the virtual
                  machine with the name.
    -w,--word            string matches are whole word
    -x,--executable <executable name>  search based on executable name
```

Important : Pour plus d'information concernant le système audit, consultez les manuels de **auditd**, **auditctl**, **audispd**, **aureport** et **ausearch**.

Le fichier /var/log/messages

Ce fichier contient la plupart des messages du système :

```
root@debian8:~# tail -n 15 /var/log/messages
```

```
Oct 28 06:37:21 debian8 kernel: [17310.156006] audit: type=1305 audit(1446010641.567:2): audit_pid=3789 old=0
auid=4294967295 ses=4294967295 res=1
Oct 28 06:54:50 debian8 kernel: [18358.844152] usb 1-1: USB disconnect, device number 4
Oct 28 06:54:50 debian8 kernel: [18359.429167] usb 1-1: new full-speed USB device number 5 using ohci-pci
Oct 28 06:54:51 debian8 kernel: [18359.707784] usb 1-1: New USB device found, idVendor=80ee, idProduct=0021
Oct 28 06:54:51 debian8 kernel: [18359.707791] usb 1-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
Oct 28 06:54:51 debian8 kernel: [18359.707794] usb 1-1: Product: USB Tablet
Oct 28 06:54:51 debian8 kernel: [18359.707797] usb 1-1: Manufacturer: VirtualBox
Oct 28 06:54:51 debian8 kernel: [18359.717328] input: VirtualBox USB Tablet as
/devices/pci0000:00/0000:00:06.0/usb1/1-1/1-1:1.0/0003:80EE:0021.0004/input/input11
Oct 28 06:54:51 debian8 mtp-probe: checking bus 1, device 5: "/sys/devices/pci0000:00/0000:00:06.0/usb1/1-1"
Oct 28 06:54:51 debian8 mtp-probe: bus: 1, device: 5 was not an MTP device
Oct 28 06:54:51 debian8 kernel: [18359.717846] hid-generic 0003:80EE:0021.0004: input,hidraw0: USB HID v1.10
Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
Oct 28 06:54:51 debian8 kernel: [18359.798364] e1000: eth0 NIC Link is Down
Oct 28 12:30:24 debian8 kernel: [18365.868629] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
Oct 28 12:30:24 debian8 kernel: [18365.869262] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Oct 28 14:11:01 debian8 rsyslogd-2007: action 'action 17' suspended, next retry is Wed Oct 28 14:11:31 2015 [try
http://www.rsyslog.com/e/2007 ]
```

Applications

Certaines applications consignent leurs journaux dans des répertoires spécifiques. Par exemple :

- cups,
- samba,
- ...

```
root@debian8:~# ls -l /var/log
total 1388
-rw-r--r-- 1 root              root    718 Oct 23 17:09 alternatives.log
drwxr-xr-x 2 root              root   4096 Oct 23 16:37 apt
```

```
drwxr-x--- 2 root              root   4096 Oct 28 06:37 audit
-rw-r----- 1 root              adm   96160 Oct 28 14:52 auth.log
-rw-r----- 1 root              adm    8318 Oct 26 11:22 auth.log.1
-rw-r--r-- 1 root              root      0 Jun  6 17:19 bootstrap.log
-rw------- 1 root              utmp      0 Jun  6 17:19 btmp
drwxr-xr-x 2 root              root   4096 Oct 26 11:27 cups
-rw-r----- 1 root              adm   45007 Oct 28 12:30 daemon.log
-rw-r----- 1 root              adm   77008 Oct 26 11:22 daemon.log.1
-rw-r----- 1 root              adm    9127 Oct 28 06:37 debug
-rw-r----- 1 root              adm   35138 Oct 26 11:22 debug.1
-rw-r----- 1 root              adm       0 Jun  6 17:19 dmesg
-rw-r--r-- 1 root              root 130612 Oct 28 06:37 dpkg.log
drwxr-s--- 2 Debian-exim       adm    4096 Oct 26 11:27 exim4
-rw-r--r-- 1 root              root  24024 Oct 23 16:59 faillog
-rw-r--r-- 1 root              root      0 Jun  6 17:19 fontconfig.log
drwxr-xr-x 2 root              root   4096 Oct 23 16:37 fsck
drwxr-xr-x 3 root              root   4096 Oct 23 16:37 hp
drwxr-xr-x 3 root              root   4096 Oct 23 16:45 installer
-rw-r----- 1 root              adm   48698 Oct 28 12:30 kern.log
-rw-r----- 1 root              adm  180412 Oct 26 11:22 kern.log.1
-rw-rw-r-- 1 root              utmp 292292 Oct 23 16:59 lastlog
drwx--x--x 2 root              root   4096 Oct 26 13:52 lightdm
-rw-r----- 1 root              adm   42656 Oct 28 14:11 messages
-rw-r----- 1 root              adm  155184 Oct 26 11:27 messages.1
drwx------ 2 speech-dispatcher root   4096 Dec  5  2014 speech-dispatcher
-rw-r----- 1 root              adm  131678 Oct 28 14:52 syslog
-rw-r----- 1 root              adm  269816 Oct 26 11:27 syslog.1
-rw-r----- 1 root              adm    2391 Oct 28 06:54 user.log
-rw-r----- 1 root              adm   10169 Oct 26 11:23 user.log.1
-rw-r--r-- 1 root              root   1195 Oct 23 16:59 vboxadd-install.log
-rw-r--r-- 1 root              root     73 Oct 23 16:59 vboxadd-install-x11.log
-rw-r--r-- 1 root              root     75 Oct 23 16:59 VBoxGuestAdditions.log
-rw-rw-r-- 1 root              utmp  13440 Oct 26 14:21 wtmp
-rw-r--r-- 1 root              root  29935 Oct 28 06:54 Xorg.0.log
```

```
-rw-r--r-- 1 root              root  22097 Oct 26 11:22 Xorg.0.log.old
```

rsyslog

rsyslog, le successeur de syslog, centralise les journaux du système grâce au daemon **rsyslog**.

rsyslog apporte des améliorations par rapport à syslogd :

- l'addition du protocole **TCP** pour la communication,
- la haute disponibilité,
- l'utilisation des bases de données au format MySQL et PostgreSQL pour stocker des journaux.

Les messages de journalisation envoyés à rsyslog sont marqués avec un **Sous-système applicatif** et une **Priorité**. Le binôme Sous-système applicatif/Priorité s'appelle un **Sélecteur**.

rsyslog décide ensuite de l'**action** à entreprendre concernant les informations transmises :

- ignorer les informations,
- envoyer les informations à un rsyslog sur une autre machine (par exemple, **@machine2**),
- inscrire les informations dans un fichier sur disque (par exemple, **/var/log/messages**),
- transmettre les informations à un utilisateur (par exemple **root**),
- transmettre les informations à tous les utilisateurs (par exemple *),
- transmettre les informations à une application liée à rsyslog via un tube (par exemple, **|logrotate**).

Sous Debian, le daemon rsyslog est configuré par l'édition du fichier **/etc/default/rsyslog** :

```
root@debian8:~# cat /etc/default/rsyslog
# Options for rsyslogd
# -x disables DNS lookups for remote messages
# See rsyslogd(8) for more details
RSYSLOGD_OPTIONS=""
```

L'option **-c** de la directive **SYSLOGD_OPTIONS** spécifie le niveau de compatibilité avec les anciennes versions de rsyslog ainsi qu'avec son

prédécesseur syslogd :

Directive	Version
SYSLOGD_OPTIONS="-c 4"	Mode natif - aucune compatibilité
SYSLOGD_OPTIONS="-c 2"	rsyslog V2 - mode compatibilité
SYSLOGD_OPTIONS="-c 0"	syslogd

Important : Notez que l'emplacement du fichier **rsyslog** n'est pas le même.

Priorités

La **Priorité** permet d'indiquer à rsyslog l'importance des informations :

Niveau	Priorité	Description
0	emerg/panic	Système inutilisable
1	alert	Action immédiate requise
2	crit	Condition critique atteinte
3	err/error	Erreurs rencontrées
4	warning/warn	Avertissements présentés
5	notice	Condition normale - message important
6	info	Condition normale - message simple
7	debug	Condition normale - message de débogage

Sous-systèmes applicatifs

Le **Sous-système applicatif**, aussi appelé **facility**, permet d'indiquer à rsyslog le type de programme qui envoie les informations :

Fonction	Description
auth/auth-priv	Message de sécurité / autorisation

Fonction	Description
cron	Message de cron ou at
daemon	Message d'un daemon
kern	Message du noyau
lpr	Message du système d'impression
mail	Message du système de mail
news	Message du système de news
syslog	Message interne de rsyslogd
user	Message utilisateur
uucp	Message du système UUCP
local0 - local7	Réservés pour des utilisations locales

/etc/rsyslog.conf

rsyslog est configuré par le fichier **/etc/rsyslog.conf** :

```
root@debian8:~# cat /etc/rsyslog.conf
#  /etc/rsyslog.conf    Configuration file for rsyslog.
#
#           For more information see
#           /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html


#################
#### MODULES ####
#################

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
```

```
#$ModLoad imudp
#$UDPServerRun 514

# provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514



###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

#
# Set the default permissions for all log files.
#
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
```

```
#
$IncludeConfig /etc/rsyslog.d/*.conf


###############
#### RULES ####
###############

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*         /var/log/auth.log
*.*;auth,authpriv.none      -/var/log/syslog
#cron.*             /var/log/cron.log
daemon.*            -/var/log/daemon.log
kern.*              -/var/log/kern.log
lpr.*               -/var/log/lpr.log
mail.*              -/var/log/mail.log
user.*              -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info           -/var/log/mail.info
mail.warn           -/var/log/mail.warn
mail.err            /var/log/mail.err

#
# Logging for INN news system.
#
news.crit           /var/log/news/news.crit
news.err            /var/log/news/news.err
news.notice         -/var/log/news/news.notice
```

```
#
# Some "catch-all" log files.
#
*.=debug;\
    auth,authpriv.none;\
    news.none;mail.none    -/var/log/debug
*.=info;*.=notice;*.=warn;\
    auth,authpriv.none;\
    cron,daemon.none;\
    mail,news.none        -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg             :omusrmsg:*

#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
#daemon,mail.*;\
#   news.=crit;news.=err;news.=notice;\
#   *.=debug;*.=info;\
#   *.=notice;*.=warn    /dev/tty8

# The named pipe /dev/xconsole is for the `xconsole' utility.  To use it,
# you must invoke `xconsole' with the `-file' option:
#
#    $ xconsole -file /dev/xconsole [...]
#
# NOTE: adjust the list below, or you'll go crazy if you have a reasonably
#      busy site..
#
daemon.*;mail.*;\
```

```
    news.err;\
    *.=debug;*.=info;\
    *.=notice;*.=warn    |/dev/xconsole
```

Ce fichier est divisé en 3 parties :

- **Modules**,
  - Section traitant le chargement des modules offrant des fonctionnalités étendues à rsyslog,
- **Directives Globales** (*Global Directives*),
  - Section traitant les options de comportement global du service rsyslog,
- **Règles** (*Rules*),
  - Section traitant les règles de configuration des journaux. Les règles au format syslogd gardent le même format. Les nouvelles règles, compatibles seulement avec rsyslog commencent par **$**.

Important : Notez que les versions du fichier **/etc/rsyslog.conf** diffèrent entre RHEL/CentOS et Debian.

Modules

Depuis la version 3 de rsyslog, la réception des données par ce dernier appelée les **inputs** est gérée par l'utilisation de modules. Parmi les modules les plus fréquemment utilisés, on trouve :

Module	**Fonction**
$ModLoad imuxsock.so	Active la trace des messages locaux, per exemple de la commande **logger**
$ModLoad imklog.so	Active la trace de messages du **noyau**
$ModLoad immark.so	Active la trace des messages de type **mark**
$ModLoad imudp.so	Active la réception de messages en utilisant le protocole **UDP**
$ModLoad imtcp.so	Active la réception de messages en utilisant le protocole **TCP**

Dans le fichier **/etc/rsyslog.conf** nous pouvons constater que les inputs **$ModLoad imuxsock.so** et **$ModLoad imklog.so** sont activés :

```
...
  * **#### MODULES ####

$ModLoad imuxsock.so    # provides support for local system logging (e.g. via logger command)
$ModLoad imklog.so  # provides kernel logging support (previously done by rklogd)
#$ModLoad immark.so # provides --MARK-- message capability

# Provides UDP syslog reception
#$ModLoad imudp.so
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp.so
#$InputTCPServerRun 514
...
```

Pour activer la réception de messages à partir de serveurs rsyslog distants en utilisant le protocole **UDP**, il convient de décommenter les directives de chargement de modules dans le fichier **/etc/rsyslog.conf** et de re-démarrer le service :

```
...
  * **#### MODULES ####

$ModLoad imuxsock.so    # provides support for local system logging (e.g. via logger command)
$ModLoad imklog.so  # provides kernel logging support (previously done by rklogd)
#$ModLoad immark.so # provides --MARK-- message capability

# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp.so
$InputTCPServerRun 514
```

```
...
```

Important : Les deux directives **$ModLoad imudp.so** et **$UDPServerRun 514** crée un **Écouteur** sur le port UDP/514 tandis que les deux directives **$ModLoad imtcp.so** et **$InputTCPServerRun 514** crée un Écouteur sur le port TCP/514. Le port 514 est le port standard pour les Écouteurs de rsyslog. Cependant il est possible de modifier le port utilisé en modifiant la valeur dans la directive **$UDPServerRun** ou **$InputTCPServerRun**. Par exemple : **$InputTCPServerRun 1514**.

Pour envoyer l'ensemble des traces de journalisation vers un serveur rsyslog distant, il convient de décommenter ou d'ajouter les lignes dans la section suivante du fichier **/etc/rsyslog.conf** :

```
...
# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
$WorkDirectory /var/spppl/rsyslog # where to place spool files
$ActionQueueFileName fwdRule1 # unique name prefix for spool files
$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
$ActionQueueType LinkedList   # run asynchronously
$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.* @@remote-host:514
# ### end of the forwarding rule ###
...
```

Important : Ces directives utilisent le protocole TCP. Le serveur distant doit donc être configuré pour ce mode de communication.La directive ***.* @@remote-host:514** doit être modifiée pour indiquer l'adresse IP du serveur rsyslog distant.

Directives Globales

Les directives dans cette section servent à configurer le comportement de rsyslog. Par exemple, nous pouvons constater la présence de la directive suivante :

```
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
```

Cette directive stipule que le format des entrées dans les fichiers de journalisation **ne doit pas** être au format d'horodatage étendu de rsyslog qui offre plus de précision que le format de syslog classique.

Règles

Chaque règle prend la forme suivante :

```
Sélecteur[; ...]  [-] Action
```

Un Sélecteur est défini d'une des façons suivantes :

Sous-système applicatif.Priorité

Dans ce cas on ne tient compte que des messages de priorité égale ou supérieure à la Priorité indiquée.

Sous-système applicatif!Priorité

Dans ce cas on ne tient compte que des messages de priorité inférieure à la Priorité indiquée.

Sous-système applicatif=Priorité

Dans ce cas on ne tient compte que des messages de priorité égale à la Priorité indiquée.

L'utilisation du caractère spécial *

La valeur du Sous-système applicatif et/ou de la Priorité peut également être *. Dans ce cas, toutes les valeurs possibles du **Sous-système applicatif** et/ou de la **Priorité** sont concernées, par exemple : **cron.***.

n Sous-systèmes avec la même priorité

Plusieurs Sous-systèmes applicatifs peuvent être stipulés pour la même Priorité en les séparant avec un **virgule**. Par exemple : **uucp,news.crit**.

n Sélecteurs avec la même Action

Une Action peut s'appliquer à plusieurs Sélecteurs en les séparant par le caractère **;**, par exemple : ***.info;mail.none;authpriv.none;cron.none**.

> **Important** : Une Action précédée par le signe **-** est entreprise d'une manière **asynchrone**. Dans le cas ou l'action est entreprise d'une manière **synchrone**, la pertinence des journaux est garantie mais au prix d'un ralentissement du système.

La Commande logger

La commande **/usr/bin/logger** permet d'intégrer des informations dans rsyslog. Ceci peut s'avérer utile dans des scripts bash.

La syntaxe de la commande est :

```
logger -p Sous-système applicatif.Priorité message
```

Par exemple saisissez la commande suivante :

```
root@debian8:~# logger -p user.info Linux est super
```

Consultez la fin de votre syslog :

```
root@debian8:~# tail /var/log/messages
Oct 28 15:01:50 debian8 pulseaudio[1278]: Disabling timer-based scheduling because running inside a VM.
Oct 28 15:01:50 debian8 pulseaudio[1278]: Disabling timer-based scheduling because running inside a VM.
Oct 28 15:01:52 debian8 org.gnome.OnlineAccounts[1245]: goa-daemon-Message: goa-daemon version 3.14.2 starting
Oct 28 15:01:53 debian8 org.gnome.OnlineAccounts[1245]: (goa-daemon:1318): goa-daemon-CRITICAL **: Error
preparing AM: The name org.freedesktop.Telepathy.AccountManager was not provided by any .service files
Oct 28 15:01:53 debian8 org.gtk.Private.AfcVolumeMonitor[1245]: Volume monitor alive
Oct 28 15:01:57 debian8 vmusr[1368]: [ warning] [vmusr] Error creating backup of old config file.
Oct 28 15:01:57 debian8 vmusr[1368]: [ warning] [vmtoolsd] The vmusr service needs to run inside a virtual
machine.
Oct 28 15:01:59 debian8 org.gnome.zeitgeist.Engine[1245]: ** (zeitgeist-datahub:1421): WARNING **: zeitgeist-
datahub.vala:226: Unable to get name "org.gnome.zeitgeist.datahub" on the bus!
Oct 28 15:08:21 debian8 kernel: [  778.981705] hrtimer: interrupt took 3109967 ns
Oct 28 15:49:23 debian8 trainee: Linux est super
```

Options de la commande

Les options de la commande logger sont :

```
root@debian8:~# logger --help

Usage:
 logger [options] [<message>]

Options:
 -T, --tcp             use TCP only
 -d, --udp             use UDP only
 -i, --id              log the process ID too
 -f, --file <file>     log the contents of this file
 -n, --server <name>   write to this remote syslog server
 -P, --port <number>   use this UDP port
 -p, --priority <prio> mark given message with this priority
     --prio-prefix     look for a prefix on every line read from stdin
 -s, --stderr          output message to standard error as well
 -t, --tag <tag>       mark every line with this tag
 -u, --socket <socket> write to this Unix socket
     --journald[=<file>]  write journald entry

 -h, --help     display this help and exit
 -V, --version  output version information and exit

For more details see logger(1).
```

La Commande logrotate

Les fichiers journaux grossissent régulièrement. Le programme **/usr/sbin/logrotate** est utilisé pour effectuer des rotations de ces fichiers selon la configuration contenue dans le fichier **/etc/logrotate.conf**.

Visualisez le fichier **/etc/logrotate.conf** :

```
root@debian8:~# cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

# system-specific logs may be configured here
```

Dans la première partie de ce fichier on trouve des directives pour :

- remplacer les fichiers journaux chaque semaine
- garder 4 archives des fichiers journaux
- créer un nouveau fichier log une fois le précédent archivé
- comprimer les archives créées.

La directive **include /etc/logrotate.d** indique que les configurations incluent dans le répertoire cité doivent être incorporées dans le fichier de configuration de logrotate.

La deuxième partie du fichier concerne des configurations spécifiques pour certains fichiers journaux.

Important : Notez que la compression des fichiers de journalisation n'est pas activée par défaut.

Options de la commande

Les options de la commande logrotate sont :

```
root@debian8:~# logrotate --help
Usage: logrotate [OPTION...] <configfile>
  -d, --debug               Don't do anything, just test (implies -v)
  -f, --force               Force file rotation
  -m, --mail=command        Command to send mail (instead of `/usr/bin/mail')
  -s, --state=statefile     Path of state file
  -v, --verbose             Display messages during rotation
      --version             Display version information

Help options:
  -?, --help                Show this help message
      --usage               Display brief usage message
```

LAB #1 - La Journalisation avec journald

Sous Debian 8, les fichiers de Syslog sont gardés pour une question de compatibilité. Cependant, tous les journaux sont d'abord collectés par **Journald** pour ensuite être redistribués vers les fichiers classiques se trouvant dans le répertoire /var/log. Les journaux de journald sont stockés dans un seul et unique fichier dynamique dans le répertoire **/run/log/journal** :

```
root@debian8:~# ls -l /run/log/journal/
total 0
drwxr-s--- 2 root systemd-journal 60 Oct 28 14:55 951001cfea0b40279f6ad23a29c19005
```

A l'extinction de la machine les journaux sont **effacés**.

Pour rendre les journaux permenants, il faut créer le répertoire **/var/log/journal** :

```
root@debian8:~# mkdir /var/log/journal
root@debian8:~# ls -l /var/log/journal
total 0
root@debian8:~# systemctl restart systemd-journald
root@debian8:~# ls -l /var/run/journal
ls: cannot access /var/run/journal: No such file or directory
root@debian8:~# ls -l /var/log/journal
total 4
drwxr-xr-x 2 root root 4096 Oct 28 15:59 951001cfea0b40279f6ad23a29c19005
root@debian8:~#
```

> **Important** : Journald ne peut pas envoyer les traces à un autre ordinateur. Pour utiliser un serveur de journalisation distant il faut donc inclure la directive **ForwardToSyslog=yes** dans le fichier de configuration de journald, **/etc/systemd/journald.conf**, puis configurer Rsyslog à envoyer les traces au serveur distant.

Consultation des Journaux

L'utilisation de la commande **journalctl** permet la consultation des journaux :

```
root@debian8:~# journalctl
-- Logs begin at Wed 2015-10-28 14:55:29 CET, end at Wed 2015-10-28 16:01:01 CET. --
Oct 28 14:55:29 debian8 systemd-journal[147]: Runtime journal is using 4.0M (max allowed 20.1M, trying to leave
30.2M free of 197.3M available → curre
Oct 28 14:55:29 debian8 systemd-journal[147]: Runtime journal is using 4.0M (max allowed 20.1M, trying to leave
30.2M free of 197.3M available → curre
Oct 28 14:55:29 debian8 kernel: Initializing cgroup subsys cpuset
Oct 28 14:55:29 debian8 kernel: Initializing cgroup subsys cpu
Oct 28 14:55:29 debian8 kernel: Initializing cgroup subsys cpuacct
Oct 28 14:55:29 debian8 kernel: Linux version 3.16.0-4-686-pae (debian-kernel@lists.debian.org) (gcc version
4.8.4 (Debian 4.8.4-1) ) #1 SMP Debian 3.
Oct 28 14:55:29 debian8 kernel: e820: BIOS-provided physical RAM map:
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 28 14:55:29 debian8 kernel: NX (Execute Disable) protection: active
Oct 28 14:55:29 debian8 kernel: SMBIOS 2.5 present.
Oct 28 14:55:29 debian8 kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 28 14:55:29 debian8 kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 28 14:55:29 debian8 kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 28 14:55:29 debian8 kernel: e820: last_pfn = 0x3fff0 max_arch_pfn = 0x1000000
Oct 28 14:55:29 debian8 kernel: MTRR default type: uncachable
Oct 28 14:55:29 debian8 kernel: MTRR variable ranges disabled:
Oct 28 14:55:29 debian8 kernel: x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
Oct 28 14:55:29 debian8 kernel: CPU MTRRs all blank - virtualized system.
Oct 28 14:55:29 debian8 kernel: initial memory mapped: [mem 0x00000000-0x01bfffff]
```

```
Oct 28 14:55:29 debian8 kernel: Base memory trampoline at [c009b000] 9b000 size 16384
Oct 28 14:55:29 debian8 kernel: init_memory_mapping: [mem 0x00000000-0x000fffff]
Oct 28 14:55:29 debian8 kernel:  [mem 0x00000000-0x000fffff] page 4k
Oct 28 14:55:29 debian8 kernel: init_memory_mapping: [mem 0x37200000-0x373fffff]
Oct 28 14:55:29 debian8 kernel:  [mem 0x37200000-0x373fffff] page 2M
Oct 28 14:55:29 debian8 kernel: init_memory_mapping: [mem 0x34000000-0x371fffff]
lines 1-31
```

Important : Notez que les messages importants sont en gras, par exemple les messages de niveaux **notice** ou **warning** et que les messages graves sont en rouge.

Consultation des Journaux d'une Application Spécifique

Pour consulter les entrées concernant une application spécifique, il suffit de passer l'exécutable, y compris son chemin complet, en argument à la commande journalctl :

```
root@debian8:~# journalctl /usr/sbin/anacron
-- Logs begin at Wed 2015-10-28 14:55:29 CET, end at Wed 2015-10-28 16:03:01 CET. --
Oct 28 14:55:36 debian8 anacron[441]: Anacron 2.3 started on 2015-10-28
Oct 28 14:55:36 debian8 anacron[441]: Will run job `cron.daily' in 5 min.
Oct 28 14:55:36 debian8 anacron[441]: Jobs will be executed sequentially
Oct 28 15:00:36 debian8 anacron[441]: Job `cron.daily' started
Oct 28 15:00:36 debian8 anacron[972]: Updated timestamp for job `cron.daily' to 2015-10-28
```

Important : Rappelez-vous que sous RHEL/CentOS 7 le répertoire **/sbin** est un line symbolique vers **/usr/sbin**. Ceci n'est pas le cas sous Debian 8.

Consultation des Journaux depuis le Dernier Démarrage

Pour consulter les entrées depuis le dernier démarrage, il suffit d'utiliser l'option **-b** de la commande journalctl :

```
root@debian8:~# journalctl -b | more
-- Logs begin at Wed 2015-10-28 14:55:29 CET, end at Wed 2015-10-28 16:06:01 CET. --
Oct 28 14:55:29 debian8 systemd-journal[147]: Runtime journal is using 4.0M (max allowed 20.1M, trying to leave
30.2M free of 197.3M available → curre
nt limit 20.1M).
Oct 28 14:55:29 debian8 systemd-journal[147]: Runtime journal is using 4.0M (max allowed 20.1M, trying to leave
30.2M free of 197.3M available → curre
nt limit 20.1M).
Oct 28 14:55:29 debian8 kernel: Initializing cgroup subsys cpuset
Oct 28 14:55:29 debian8 kernel: Initializing cgroup subsys cpu
Oct 28 14:55:29 debian8 kernel: Initializing cgroup subsys cpuacct
Oct 28 14:55:29 debian8 kernel: Linux version 3.16.0-4-686-pae (debian-kernel@lists.debian.org) (gcc version
4.8.4 (Debian 4.8.4-1) ) #1 SMP Debian 3.
16.7-ckt11-1+deb8u5 (2015-10-09)
Oct 28 14:55:29 debian8 kernel: e820: BIOS-provided physical RAM map:
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
Oct 28 14:55:29 debian8 kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 28 14:55:29 debian8 kernel: NX (Execute Disable) protection: active
Oct 28 14:55:29 debian8 kernel: SMBIOS 2.5 present.
Oct 28 14:55:29 debian8 kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 28 14:55:29 debian8 kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 28 14:55:29 debian8 kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 28 14:55:29 debian8 kernel: e820: last_pfn = 0x3fff0 max_arch_pfn = 0x1000000
Oct 28 14:55:29 debian8 kernel: MTRR default type: uncachable
Oct 28 14:55:29 debian8 kernel: MTRR variable ranges disabled:
```

```
Oct 28 14:55:29 debian8 kernel: x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
Oct 28 14:55:29 debian8 kernel: CPU MTRRs all blank - virtualized system.
Oct 28 14:55:29 debian8 kernel: initial memory mapped: [mem 0x00000000-0x01bfffff]
Oct 28 14:55:29 debian8 kernel: Base memory trampoline at [c009b000] 9b000 size 16384
Oct 28 14:55:29 debian8 kernel: init_memory_mapping: [mem 0x00000000-0x000fffff]
Oct 28 14:55:29 debian8 kernel:  [mem 0x00000000-0x000fffff] page 4k
--More--
```

Important : Notez que vous pouvez consulter les messages des démarrages précédents, il est possible d'utiliser les options **-b 1**, **-b 2** etc.

Consultation des Journaux d'une Priorité Spécifique

Pour consulter les entrées à partir d'une priorité spécifique et supérieur, il suffit d'utiliser l'option **-p** de la commande journalctl en spécifiant la priorité concernée :

```
root@debian8:~# journalctl -p warning
-- Logs begin at Wed 2015-10-28 14:55:29 CET, end at Wed 2015-10-28 16:07:01 CET. --
Oct 28 14:55:29 debian8 kernel: ACPI: RSDP 0x000E0000 000024 (v02 VBOX  )
Oct 28 14:55:29 debian8 kernel: ACPI: XSDT 0x3FFF0030 000034 (v01 VBOX   VBOXXSDT 00000001 ASL  00000061)
Oct 28 14:55:29 debian8 kernel: ACPI: FACP 0x3FFF00F0 0000F4 (v04 VBOX   VBOXFACP 00000001 ASL  00000061)
Oct 28 14:55:29 debian8 kernel: ACPI: DSDT 0x3FFF0410 001BF1 (v01 VBOX   VBOXBIOS 00000002 INTL 20100528)
Oct 28 14:55:29 debian8 kernel: ACPI: FACS 0x3FFF0200 000040
Oct 28 14:55:29 debian8 kernel: ACPI: SSDT 0x3FFF0240 0001CC (v01 VBOX   VBOXCPUT 00000002 INTL 20100528)
Oct 28 14:55:29 debian8 kernel: Zone ranges:
Oct 28 14:55:29 debian8 kernel:   DMA      [mem 0x00001000-0x00ffffff]
Oct 28 14:55:29 debian8 kernel:   Normal   [mem 0x01000000-0x375fdfff]
Oct 28 14:55:29 debian8 kernel:   HighMem  [mem 0x375fe000-0x3ffeffff]
Oct 28 14:55:29 debian8 kernel: Movable zone start for each node
Oct 28 14:55:29 debian8 kernel: Early memory node ranges
```

```
Oct 28 14:55:29 debian8 kernel:   node   0: [mem 0x00001000-0x0009efff]
Oct 28 14:55:29 debian8 kernel:   node   0: [mem 0x00100000-0x3ffeffff]
Oct 28 14:55:29 debian8 kernel: Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 260258
Oct 28 14:55:29 debian8 kernel: Memory: 1010236K/1048120K available (4599K kernel code, 518K rwdata, 1448K
rodata, 656K init, 460K bss, 37884K reserve
Oct 28 14:55:29 debian8 kernel: Fast TSC calibration using MSR failed
Oct 28 14:55:29 debian8 kernel: tsc: Unable to calibrate against PIT
Oct 28 14:55:29 debian8 kernel: ACPI: All ACPI Tables successfully acquired
Oct 28 14:55:29 debian8 kernel: ACPI: setting ELCR to 0200 (from 0e00)
Oct 28 14:55:29 debian8 kernel: smpboot: weird, boot CPU (#0) not listed by the BIOS
Oct 28 14:55:29 debian8 kernel: NMI watchdog: disabled (cpu0): hardware events not enabled
Oct 28 14:55:29 debian8 kernel: ACPI: Executed 1 blocks of module-level executable AML code
Oct 28 14:55:29 debian8 kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S1_]
(20140424/hwxface-580)
Oct 28 14:55:29 debian8 kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S2_]
(20140424/hwxface-580)
Oct 28 14:55:29 debian8 kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S3_]
(20140424/hwxface-580)
Oct 28 14:55:29 debian8 kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S4_]
(20140424/hwxface-580)
Oct 28 14:55:29 debian8 kernel: acpi PNP0A03:00: fail to add MMCONFIG information, can't access extended PCI
configuration space under this bridge.
Oct 28 14:55:29 debian8 kernel: ACPI: Enabled 2 GPEs in block 00 to 07
Oct 28 14:55:29 debian8 kernel: ACPI: PCI Interrupt Link [LNKB] enabled at IRQ 11
lines 1-31
```

Consultation des Journaux d'une Plage de Dates ou d'Heures

Pour consulter les entrées d'une plage de dates ou d'heures, il suffit de passer cette plage en argument à la commande journalctl :

```
root@debian8:~# journalctl --since 16:00 --until now
-- Logs begin at Wed 2015-10-28 14:55:29 CET, end at Wed 2015-10-28 16:08:01 CET. --
Oct 28 16:00:01 debian8 CRON[1856]: pam_unix(cron:session): session opened for user trainee by (uid=0)
```

```
Oct 28 16:00:01 debian8 CRON[1857]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:00:01 debian8 CRON[1856]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:01:01 debian8 CRON[1861]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:01:01 debian8 CRON[1862]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:01:01 debian8 CRON[1861]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:02:01 debian8 CRON[1870]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:02:01 debian8 CRON[1871]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:02:01 debian8 CRON[1870]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:03:01 debian8 CRON[1877]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:03:01 debian8 CRON[1878]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:03:01 debian8 CRON[1877]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:04:01 debian8 CRON[1885]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:04:01 debian8 CRON[1886]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:04:01 debian8 CRON[1885]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:05:01 debian8 CRON[1888]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:05:01 debian8 CRON[1889]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:05:01 debian8 CRON[1888]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:06:01 debian8 CRON[1893]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:06:01 debian8 CRON[1894]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:06:01 debian8 CRON[1893]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:07:01 debian8 CRON[1899]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:07:01 debian8 CRON[1900]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:07:01 debian8 CRON[1899]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:08:01 debian8 CRON[1909]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:08:01 debian8 CRON[1910]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:08:01 debian8 CRON[1909]: pam_unix(cron:session): session closed for user trainee
```

Important : Le format de la date est **2015-09-29 18:38:00**. Il est possible d'utiliser des mots clefs : **yesterday**, **today**, **tomorrow**, **now**.

Consultation des Journaux en Live

Pour consulter les journaux en live, il suffit d'utiliser l'option **-f** de la commande journalctl :

```
root@debian8:~# journalctl -f
-- Logs begin at Wed 2015-10-28 14:55:29 CET. --
Oct 28 16:06:01 debian8 CRON[1893]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:07:01 debian8 CRON[1899]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:07:01 debian8 CRON[1900]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:07:01 debian8 CRON[1899]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:08:01 debian8 CRON[1909]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:08:01 debian8 CRON[1910]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:08:01 debian8 CRON[1909]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:09:01 debian8 CRON[1914]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:09:01 debian8 CRON[1915]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:09:01 debian8 CRON[1914]: pam_unix(cron:session): session closed for user trainee
```

Ouvrez un deuxième terminal et saisissez la commande suivante :

```
root@debian8:~# logger -p user.info Linux est super
```

Retournez consulter le premier terminal :

```
root@debian8:~# journalctl -f
-- Logs begin at Wed 2015-10-28 14:55:29 CET. --
Oct 28 16:06:01 debian8 CRON[1893]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:07:01 debian8 CRON[1899]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:07:01 debian8 CRON[1900]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:07:01 debian8 CRON[1899]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:08:01 debian8 CRON[1909]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:08:01 debian8 CRON[1910]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:08:01 debian8 CRON[1909]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:09:01 debian8 CRON[1914]: pam_unix(cron:session): session opened for user trainee by (uid=0)
```

```
Oct 28 16:09:01 debian8 CRON[1915]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:09:01 debian8 CRON[1914]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:10:01 debian8 CRON[1922]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:10:01 debian8 CRON[1923]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:10:01 debian8 CRON[1922]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:11:01 debian8 CRON[1927]: pam_unix(cron:session): session opened for user trainee by (uid=0)
Oct 28 16:11:01 debian8 CRON[1928]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 28 16:11:01 debian8 CRON[1927]: pam_unix(cron:session): session closed for user trainee
Oct 28 16:11:20 debian8 trainee[1936]: Linux est super
```

Important : Notez la présence de la dernière ligne.

Consultation des Journaux avec des Mots Clefs

Pour consulter les mots clefs compris par Journald, tapez la commande journalctl puis appuyer trois fois sur la touche Tab ⇆ :

```
root@debian8:~# journalctl [tab] [tab] [tab]
_AUDIT_LOGINUID=             COREDUMP_EXE=              _MACHINE_ID=
_SOURCE_REALTIME_TIMESTAMP=  _TRANSPORT=
_AUDIT_SESSION=              __CURSOR=                  MESSAGE=                   SYSLOG_FACILITY=
_UDEV_DEVLINK=
_BOOT_ID=                    ERRNO=                     MESSAGE_ID=                SYSLOG_IDENTIFIER=
_UDEV_DEVNODE=
_CMDLINE=                    _EXE=                      __MONOTONIC_TIMESTAMP=     SYSLOG_PID=
_UDEV_SYSNAME=
CODE_FILE=                   _GID=                      _PID=                      _SYSTEMD_CGROUP=
_UID=
CODE_FUNC=                   _HOSTNAME=                 PRIORITY=                  _SYSTEMD_OWNER_UID=
CODE_LINE=                   _KERNEL_DEVICE=            __REALTIME_TIMESTAMP=      _SYSTEMD_SESSION=
```

```
_COMM=                    _KERNEL_SUBSYSTEM=          _SELINUX_CONTEXT=          _SYSTEMD_UNIT=
```

Pour voir la liste des processus dont les traces sont inclus dans les journaux du mots clefs, tapez la commande journalctl suivi par le nom d'un mot clef puis appuyer deux fois sur la touche Tab ⇆ :

```
root@debian8:~# journalctl journalctl _UID=
0     1000  104   106   111   116   120
root@debian8:~# journalctl journalctl _COMM=
accounts-daemon  cinnamon-screen  exim4           logger          nfs-common       rtkit-daemon     systemd
vboxadd
anacron          colord           gdomap          minissdpd       nm-dispatcher    saned            (systemd)
vmtoolsd
audispd          console-setup    irqbalance      ModemManager    polkitd          sm-notify        systemd-
journal
auditctl         cron             kbd             mtp-probe       pulseaudio       speech-dispatch  systemd-
logind
auditd           dbus-daemon      keyboard-setup  networking      rpcbind          sshd             systemd-
modules
avahi-daemon     dhclient         lightdm         NetworkManager  rpc.statd        su               udisksd
root@debian8:~# journalctl journalctl _COMM=
```

<html>

</html>
