

Dernière mise-à-jour : 2023/02/14 09:38

LCF208 - Gestion de la Journalisation

Contenu du Module

- **LCF208 - Gestion de la Journalisation**

- Contenu du Module
- Présentation
- La Commande dmesg
- Surveillance Sécuritaire
 - La Commande last
 - La Commande lastlog
 - La Commande lastb
 - Le Fichier /var/log/secure
- Le fichier /var/log/audit/audit.log
 - Gestion des événements audit
 - auditd
 - auditctl
 - audispd
 - La consultation des événements audit
 - La Commande aureport
 - La Commande ausearch
- Le fichier /var/log/messages
- Applications
- rsyslog
 - Priorités
 - Sous-systèmes applicatifs
 - /etc/rsyslog.conf
 - Modules
 - Directives Globales

- Règles
 - Sous-système applicatif.Priorité
 - Sous-système applicatif!Priorité
 - Sous-système applicatif=Priorité
 - L'utilisation du caractère spécial *
 - n Sous-systèmes avec la même priorité
 - n Sélecteurs avec la même Action
- La Commande logger
- La Commande logrotate
- La Journalisation avec journald
 - Consultation des Journaux
 - Consultation des Journaux d'une Application Spécifique
 - Consultation des Journaux depuis le Dernier Démarrage
 - Consultation des Journaux d'une Priorité Spécifique
 - Consultation des Journaux d'une Plage de Dates ou d'Heures
 - Consultation des Journaux en Live
 - Consultation des Journaux avec des Mots Clefs

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 `/bin/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@centos7 ~]# dmesg | more
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Initializing cgroup subsys cpuacct
[    0.000000] Linux version 3.10.0-229.4.2.el7.x86_64 (builder@kbuilder.dev.centos.org) (gcc version 4.8.2
20140120 (Red Hat 4.8.2-16) (GCC) ) #1 SMP
Wed May 13 10:06:09 UTC 2015
[    0.000000] Command line: BOOT_IMAGE=/vmlinuz-3.10.0-229.4.2.el7.x86_64 root=UUID=b35de665-5ec8-4226-
a533-58alb567ac91 ro vconsole.keymap=fr crashk
ernel=auto vconsole.font=latarcyrheb-sun16 rhgb quiet
[    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 0x0000000000100000-0x00000000005ffeffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000005fff0000-0x00000000005fffffff] 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] No AGP bridge found
[    0.000000] e820: last_pfn = 0x5ffff0 max_arch_pfn = 0x400000000
[    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] found SMP MP-table at [mem 0x0009fff0-0x0009ffff] mapped at [ffff88000009fff0]
[ 0.000000] Base memory trampoline at [ffff880000099000] 99000 size 24576
[ 0.000000] init_memory_mapping: [mem 0x00000000-0x000fffff]
[ 0.000000] [mem 0x00000000-0x000fffff] page 4k
--More--
```

Options de la Commande

Les option de cette commande sont :

```
[root@centos7 ~]# 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
-d, --show-delta	show time delta between printed messages
-e, --reltime	show local time and time delta in readable format
-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	colorize messages
-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

```
-T, --ctime      show human readable timestamp (could be
                  inaccurate if you have used SUSPEND/RESUME)
-t, --notime     don't print messages timestamp
-u, --userspace  display userspace messages
-w, --follow     wait for new messages
-x, --decode     decode facility and level to readable string

-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(q)`.

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@centos7 ~]# last
trainee pts/0      :0                Wed Oct 28 09:42  still logged in
trainee :0          :0                Wed Oct 28 09:41  still logged in
(unknown :0        :0                Wed Oct 28 09:41 - 09:41 (00:00)
reboot  system boot 3.10.0-229.4.2.e Wed Oct 28 09:40 - 09:49 (00:09)
trainee pts/1      :0                Tue Oct 27 17:58 - 17:58 (00:00)
trainee pts/2      :0                Tue Oct 27 17:58 - 17:58 (00:00)
trainee pts/1      :0                Tue Oct 27 17:58 - 17:58 (00:00)
trainee pts/1      :0                Tue Oct 27 16:33 - 16:33 (00:00)
trainee pts/0      :0                Tue Oct 27 16:17 - crash (17:22)
trainee :0          :0                Tue Oct 27 16:17 - crash (17:22)
(unknown :0        :0                Tue Oct 27 16:07 - 16:17 (00:10)
reboot  system boot 3.10.0-229.4.2.e Tue Oct 27 16:06 - 09:49 (17:42)
trainee pts/1      :0                Tue Oct 27 11:47 - crash (04:19)
trainee pts/0      :0                Sat Oct 24 16:18 - crash (3+00:48)
trainee :0          :0                Sat Oct 24 16:17 - crash (3+00:48)
(unknown :0        :0                Sat Oct 24 16:17 - 16:17 (00:00)
reboot  system boot 3.10.0-229.4.2.e Sat Oct 24 16:16 - 09:49 (3+18:32)
trainee pts/0      :0                Thu Oct 15 13:07 - crash (9+03:09)
trainee :0          :0                Thu Oct 15 13:06 - crash (9+03:10)
(unknown :0        :0                Thu Oct 15 13:05 - 13:06 (00:00)
reboot  system boot 3.10.0-229.4.2.e Thu Oct 15 13:04 - 09:49 (12+21:44)
trainee pts/0      :0                Thu Oct 8 21:42 - crash (6+15:22)
trainee :0          :0                Thu Oct 8 21:41 - crash (6+15:22)
(unknown :0        :0                Thu Oct 8 21:28 - 21:41 (00:12)
reboot  system boot 3.10.0-229.4.2.e Thu Oct 8 21:28 - 09:49 (19+13:21)
```

trainee	pts/0	:0	Thu Oct 8 12:27	- 12:27	(00:00)
trainee	:0	:0	Thu Oct 8 12:25	- crash	(09:02)
(unknown	:0	:0	Thu Oct 8 12:25	- 12:25	(00:00)
reboot	system boot	3.10.0-229.4.2.e	Thu Oct 8 12:24	- 09:49	(19+22:25)
trainee	:0	:0	Sat Jun 6 09:44	- crash	(124+02:39)
(unknown	:0	:0	Sat Jun 6 09:43	- 09:44	(00:00)
reboot	system boot	3.10.0-229.4.2.e	Sat Jun 6 09:43	- 09:49	(144+01:06)
(unknown	:0	:0	Fri Jun 5 17:22	- crash	(16:20)
reboot	system boot	3.10.0-229.4.2.e	Fri Jun 5 17:22	- 09:49	(144+17:27)
trainee	pts/0	:0	Fri Jun 5 16:09	- 17:21	(01:12)
trainee	pts/2	:0	Thu Jun 4 16:05	- 16:05	(00:00)
trainee	pts/1	:0	Thu Jun 4 16:05	- 16:05	(00:00)
trainee	pts/1	:0	Thu Jun 4 16:05	- 16:05	(00:00)
trainee	pts/0	:0	Thu Jun 4 15:38	- 16:08	(1+00:30)
trainee	:0	:0	Thu Jun 4 15:36	- 17:21	(1+01:45)
(unknown	:0	:0	Thu Jun 4 15:36	- 15:36	(00:00)
reboot	system boot	3.10.0-229.4.2.e	Thu Jun 4 15:35	- 17:21	(1+01:46)
trainee	pts/1	:0	Thu Jun 4 15:31	- 15:33	(00:02)
trainee	pts/0	:0	Thu Jun 4 15:23	- 15:35	(00:11)
trainee	:0	:0	Thu Jun 4 15:00	- 15:35	(00:34)
(unknown	:0	:0	Thu Jun 4 14:59	- 15:00	(00:00)
reboot	system boot	3.10.0-229.4.2.e	Thu Jun 4 14:59	- 15:35	(00:36)
trainee	pts/1	:0	Thu Jun 4 09:50	- 09:53	(00:03)
trainee	pts/1	:0	Thu Jun 4 09:41	- 09:42	(00:00)
trainee	pts/1	:0	Thu Jun 4 09:38	- 09:39	(00:00)
trainee	pts/0	:0	Thu Jun 4 09:37	- 10:36	(00:58)
trainee	pts/0	:0	Thu Jun 4 09:36	- 09:37	(00:00)
trainee	:0	:0	Thu Jun 4 09:35	- 10:36	(01:00)
(unknown	:0	:0	Mon Jun 1 17:31	- 09:35	(2+16:04)
reboot	system boot	3.10.0-123.el7.x	Mon Jun 1 17:30	- 10:36	(2+17:05)
trainee	pts/0	:0	Mon Jun 1 17:19	- 17:31	(00:11)
trainee	:0	:0	Mon Jun 1 15:43	- 17:31	(01:47)
(unknown	:0	:0	Mon Jun 1 15:42	- 15:43	(00:01)
reboot	system boot	3.10.0-123.el7.x	Mon Jun 1 15:41	- 17:31	(01:49)

```
trainee pts/0      :0          Sun Mar  8 14:36 - crash (85+00:05)
trainee :0          :0          Sun Mar  8 14:35 - crash (85+00:05)
(unknown :0        :0          Sun Mar  8 14:32 - 14:35 (00:03)
reboot  system boot 3.10.0-123.el7.x Sun Mar  8 14:31 - 17:31 (85+01:59)
trainee :0          :0          Sun Mar  8 14:25 - crash (00:06)
(unknown :0        :0          Sun Mar  8 14:24 - 14:25 (00:00)
reboot  system boot 3.10.0-123.el7.x Sun Mar  8 14:23 - 17:31 (85+02:07)
```

```
wtmp begins Sun Mar  8 14:23:23 2015
```

Options de la Commande

Les option de cette commande sont :

```
[root@centos7 ~]# 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@centos7 ~]# lastlog
Username      Port      From      Latest
root          pts/0     10.0.2.15  Wed Oct 28 09:48:43 +0100 2015
bin
daemon
adm
lp
sync
shutdown
**Never logged in**
```

halt		**Never logged in**
mail		**Never logged in**
operator		**Never logged in**
games		**Never logged in**
ftp		**Never logged in**
nobody		**Never logged in**
dbus		**Never logged in**
polkitd		**Never logged in**
unbound		**Never logged in**
colord		**Never logged in**
usbmuxd		**Never logged in**
avahi		**Never logged in**
avahi-autoipd		**Never logged in**
saslauth		**Never logged in**
qemu		**Never logged in**
libstoragemgmt		**Never logged in**
rpc		**Never logged in**
rpcuser		**Never logged in**
nfsnobody		**Never logged in**
rtkit		**Never logged in**
radvd		**Never logged in**
ntp		**Never logged in**
chrony		**Never logged in**
abrt		**Never logged in**
pulse		**Never logged in**
gdm	:0	Wed Oct 28 09:41:03 +0100 2015
gnome-initial-setup		**Never logged in**
postfix		**Never logged in**
sshd		**Never logged in**
tcpdump		**Never logged in**
trainee	:0	Wed Oct 28 09:41:31 +0100 2015
vboxadd		**Never logged in**
tss		**Never logged in**

Options de la Commande

Les option de cette commande sont :

```
[root@centos7 ~]# 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 infructueuses des utilisateurs à partir du contenu du fichier **/var/log/btmp** :

```
[root@centos7 ~]# lastb
trainee :0          :0          Tue Jan 19 07:19 - 07:19 (00:00)
trainee :0          :0          Tue Jan 19 07:19 - 07:19 (00:00)
root    pts/0       Thu Oct 22 12:36 - 12:36 (00:00)
trainee :0          :0          Thu Oct 15 15:01 - 15:01 (00:00)

btmp begins Thu Oct 15 15:01:57 2015
```

Options de la Commande

Les options de cette commande sont :

```
[root@centos7 ~]# lastb --help
lastb: invalid option -- '-'
Usage: lastb [-num | -n num] [-f file] [-t YYYYMMDDHHMMSS] [-R] [-adioxFw] [username..] [tty..]
```

Le Fichier /var/log/secure

Sous RHEL/CentOS ce fichier contient la journalisation des opérations de gestion des authentifications :

```
[root@centos7 ~]# tail -n 15 /var/log/secure
Oct 27 17:31:02 centos7 polkitd[625]: <no filename>:0: uncaught exception: Terminating runaway script
Oct 27 17:31:02 centos7 polkitd[625]: Error evaluating authorization rules
Oct 27 17:48:27 centos7 gdm-password]: gkr-pam: unlocked login keyring
Oct 28 09:40:43 centos7 polkitd[586]: Loading rules from directory /etc/polkit-1/rules.d
Oct 28 09:40:43 centos7 polkitd[586]: Loading rules from directory /usr/share/polkit-1/rules.d
Oct 28 09:40:44 centos7 polkitd[586]: Finished loading, compiling and executing 5 rules
Oct 28 09:40:44 centos7 polkitd[586]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Oct 28 09:40:55 centos7 sshd[1217]: Server listening on 0.0.0.0 port 22.
Oct 28 09:40:55 centos7 sshd[1217]: Server listening on :: port 22.
Oct 28 09:41:03 centos7 gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session opened for
user gdm by (uid=0)
Oct 28 09:41:18 centos7 polkitd[586]: Registered Authentication Agent for unix-session:c1 (system bus name :1.34
[gnome-shell --mode=gdm], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Oct 28 09:41:31 centos7 gdm-password]: pam_unix(gdm-password:session): session opened for user trainee by
(unknown)(uid=0)
Oct 28 09:41:32 centos7 polkitd[586]: Unregistered Authentication Agent for unix-session:c1 (system bus name
:1.34, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Oct 28 09:41:43 centos7 polkitd[586]: Registered Authentication Agent for unix-session:2 (system bus name :1.73
[/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.utf8)
Oct 28 09:48:43 centos7 su: pam_unix(su-l:session): session opened for user root by trainee(uid=1000)
```

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

Ce fichier contient les messages du système d'audit, appelés des **événements**. 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.

Consultez maintenant le fichier `/var/log/audit.log` :

```
[root@centos7 ~]# tail -n 15 /var/log/audit/audit.log
type=CRED_ACQ msg=audit(1443519601.478:401): pid=3596 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_unix acct="root"
exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1443519601.488:402): pid=3596 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-
auid=4294967295 auid=0 old-ses=4294967295 ses=3 res=1
type=USER_START msg=audit(1443519601.563:403): pid=3596 uid=0 auid=0 ses=3 subj=system_u:system_r:crond_t:s0-
s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root"
exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_REFR msg=audit(1443519601.568:404): pid=3596 uid=0 auid=0 ses=3 subj=system_u:system_r:crond_t:s0-
s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_unix acct="root" exe="/usr/sbin/crond" hostname=? addr=?
terminal=cron res=success'
type=CRED_DISP msg=audit(1443519601.646:405): pid=3596 uid=0 auid=0 ses=3 subj=system_u:system_r:crond_t:s0-
s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_unix acct="root" exe="/usr/sbin/crond" hostname=? addr=?
terminal=cron res=success'
type=USER_END msg=audit(1443519601.654:406): pid=3596 uid=0 auid=0 ses=3 subj=system_u:system_r:crond_t:s0-
s0:c0.c1023 msg='op=PAM:session_close grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root"
exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=SERVICE_START msg=audit(1443519610.092:407): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg=' comm="systemd-tmpfiles-clean" exe="/usr/lib/systemd/systemd" hostname=?
addr=? terminal=? res=success'
type=SERVICE_STOP msg=audit(1443519610.092:408): pid=1 uid=0 auid=4294967295 ses=4294967295
```

```
subj=system_u:system_r:init_t:s0 msg=' comm="systemd-tmpfiles-clean" exe="/usr/lib/systemd/systemd" hostname=?  
addr=? terminal=? res=success'  
type=SERVICE_START msg=audit(1443519737.774:409): pid=1 uid=0 auid=4294967295 ses=4294967295  
subj=system_u:system_r:init_t:s0 msg=' comm="fprintd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?  
res=success'  
type=USER_AUTH msg=audit(1443519740.732:410): pid=3718 uid=1000 auid=1000 ses=1  
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix  
acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'  
type=USER_ACCT msg=audit(1443519740.754:411): pid=3718 uid=1000 auid=1000 ses=1  
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser  
acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'  
type=CRED_ACQ msg=audit(1443519740.754:412): pid=3718 uid=1000 auid=1000 ses=1  
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root"  
exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'  
type=USER_START msg=audit(1443519740.886:413): pid=3718 uid=1000 auid=1000 ses=1  
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open  
grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_xauth acct="root" exe="/usr/bin/su"  
hostname=? addr=? terminal=pts/0 res=success'  
type=SERVICE_STOP msg=audit(1443519767.698:414): pid=1 uid=0 auid=4294967295 ses=4294967295  
subj=system_u:system_r:init_t:s0 msg=' comm="fprintd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?  
res=success'  
type=SERVICE_STOP msg=audit(1443519851.018:415): pid=1 uid=0 auid=4294967295 ses=4294967295  
subj=system_u:system_r:init_t:s0 msg=' comm="systemd-hostnamed" exe="/usr/lib/systemd/systemd" hostname=? addr=?  
terminal=? 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@centos7 ~]# 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@centos7 ~]# 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@centos7 ~]# cat /etc/audit/audit.rules
## This file is automatically generated from /etc/audit/rules.d
-D
-b 320
```

Options de la Commande

Les options de cette commande sont :

```
[root@centos7 ~]# 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
--backlog_wait_time   Set the kernel backlog_wait_time
```

audispd

Cet exécutable est responsable de la distribution des événements 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 événements, les applications placent un fichier de configuration dans le répertoire **/etc/audisp/plugins.d** :

```
[root@centos7 ~]# ls /etc/audisp/plugins.d
af_unix.conf  sedispatch.conf  syslog.conf
```

Le contenu de ces fichiers suit un format précis :

```
[root@centos7 ~]# 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 événements audit

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

La Commande aureport

Cette commande est utilisée pour générer des rapports :

```
[root@centos7 ~]# aureport
```

Summary Report

```
=====
```

```
Range of time in logs: 03/08/2015 14:23:34.354 - 09/29/2015 11:44:11.018
```

```
Selected time for report: 03/08/2015 14:23:34 - 09/29/2015 11:44:11.018
```

```
Number of changes in configuration: 5309
```

```
Number of changes to accounts, groups, or roles: 30
```

```
Number of logins: 14
```

```
Number of failed logins: 1
```

```
Number of authentications: 61
```

```
Number of failed authentications: 1
```

```
Number of users: 3
```

```
Number of terminals: 7
```

```
Number of host names: 1
```

```
Number of executables: 17
```

```
Number of commands: 84
```

```
Number of files: 1
```

```
Number of AVC's: 1
```

```
Number of MAC events: 15
```

```
Number of failed syscalls: 0
```

```
Number of anomaly events: 1
```

```
Number of responses to anomaly events: 0
```

```
Number of crypto events: 28
```

```
Number of integrity events: 0
```

```
Number of virt events: 0
```

```
Number of keys: 0
```

```
Number of process IDs: 1414
```

```
Number of events: 8610
```

Options de la Commande

Les options de cette commande sont :

```
[root@centos7 ~]# aureport --help
usage: aureport [options]
  -a,--avc                Avc report
  -au,--auth              Authentication report
  --comm                  Commands run 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
  --integrity             Integrity event report
  -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
--virt                Virtualization report
-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 événements. Par exemple, pour rechercher les événements liés à un utilisateur représenté par son UID :

```
[root@centos7 ~]# ausearch -ui 1000 | more
----
time->Sun Mar  8 14:26:43 2015
type=ANOM_ABEND msg=audit(1425821203.409:383): auid=1000 uid=1000 gid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 pid=11897
comm="yelp" reason="memory violation" sig=6
----
time->Sun Mar  8 14:36:33 2015
type=USER_AUTH msg=audit(1425821793.757:383): pid=3200 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM
:authentication acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'
----
time->Sun Mar  8 14:36:33 2015
type=USER_ACCT msg=audit(1425821793.765:384): pid=3200 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM
:accounting acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'
----
time->Sun Mar  8 14:36:33 2015
```

```
type=CRED_ACQ msg=audit(1425821793.765:385): pid=3200 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:
setcred acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'
----
time->Sun Mar  8 14:36:33 2015
type=USER_START msg=audit(1425821793.920:386): pid=3200 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PA
M:session_open acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'
----
time->Mon Jun  1 17:20:11 2015
type=USER_AUTH msg=audit(1433172011.329:505): pid=466 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:
authentication acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'
----
time->Mon Jun  1 17:20:11 2015
type=USER_ACCT msg=audit(1433172011.330:506): pid=466 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:
accounting acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=success'
----
--More--
```

Options de la Commande

Les options de cette commande sont :

```
[root@centos7 ~]# 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@centos7 ~]# tail -n 15 /var/log/messages
Sep 29 11:40:01 centos7 systemd: Created slice user-0.slice.
Sep 29 11:40:01 centos7 systemd: Starting Session 3 of user root.
Sep 29 11:40:01 centos7 systemd: Started Session 3 of user root.
Sep 29 11:40:09 centos7 systemd: Starting Cleanup of Temporary Directories...
Sep 29 11:40:10 centos7 systemd: Started Cleanup of Temporary Directories.
Sep 29 11:42:17 centos7 dbus-daemon: dbus[526]: [system] Activating via systemd: service
name='net.reactivated.Fprint' unit='fprintd.service'
Sep 29 11:42:17 centos7 dbus[526]: [system] Activating via systemd: service name='net.reactivated.Fprint'
unit='fprintd.service'
Sep 29 11:42:17 centos7 systemd: Starting Fingerprint Authentication Daemon...
Sep 29 11:42:17 centos7 dbus-daemon: dbus[526]: [system] Successfully activated service 'net.reactivated.Fprint'
Sep 29 11:42:17 centos7 dbus[526]: [system] Successfully activated service 'net.reactivated.Fprint'
Sep 29 11:42:17 centos7 systemd: Started Fingerprint Authentication Daemon.
```

```
Sep 29 11:42:17 centos7 fprintd: Launching FprintObject
Sep 29 11:42:17 centos7 fprintd: ** Message: D-Bus service launched with name: net.reactivated.Fprint
Sep 29 11:42:17 centos7 fprintd: ** Message: entering main loop
Sep 29 11:42:20 centos7 su: (to root) trainee on pts/0
```

Applications

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

- cups,
- httpd,
- samba,
- ...

```
[root@centos7 ~]# ls -l /var/log
total 1332
drwxr-xr-x. 2 root root 4096 Mar  8 2015 anaconda
drwxr-x---. 2 root root  22 Mar  5 2015 audit
-rw-r--r--. 1 root root 12098 Sep 29 11:25 boot.log
-rw-----. 1 root utmp      0 Jun  4 09:54 btmp
drwxr-xr-x. 2 chrony chrony  6 Jun 18 2014 chrony
-rw-r--r--. 1 root root  2094 Sep 29 11:50 cron
-rw-r--r--. 1 root root  1828 Jun 10 11:38 cron-20150610.gz
-rw-r--r--. 1 root root 10593 Sep 28 15:41 cron-20150928
drwxr-xr-x. 2 lp sys 4096 Sep 28 15:41 cups
-rw-r--r--. 1 root root 33323 Sep 29 11:25 dmesg
-rw-r--r--. 1 root root 33322 Sep 28 14:46 dmesg.old
drwx--x--x. 2 root gdm  79 Sep 29 11:25 gdm
drwxr-xr-x. 2 root root  6 Mar  6 2015 glusterfs
-rw-----. 1 root root  1340 Jun  4 10:00 grubby
-rw-r--r--. 1 root root 292292 Sep 29 11:42 lastlog
drwx-----. 3 root root  17 Jun  4 10:11 libvirt
```

```

-rw-----. 1 root root      194 Sep 29 11:25 maillog
-rw-----. 1 root root      815 Jun 10 10:06 maillog-20150610.gz
-rw-----. 1 root root      582 Sep 28 14:46 maillog-20150928
-rw-----. 1 root root    98378 Sep 29 11:50 messages
-rw-----. 1 root root   252331 Jun 10 11:30 messages-20150610.gz
-rw-----. 1 root root   274071 Sep 28 15:40 messages-20150928
drwxr-xr-x. 3 root root      17 Mar  8 2015 pluto
-rw-r--r--. 1 root root       0 Sep 29 11:26 pm-powersave.log
drwx-----. 2 root root       6 Jun 10 2014 ppp
drwxr-xr-x. 2 root root       6 Mar  6 2015 qemu-ga
drwxr-xr-x. 2 root root    4096 Sep 29 11:25 sa
drwx-----. 3 root root      16 May 12 22:19 samba
-rw-----. 1 root root    1597 Sep 29 11:42 secure
-rw-----. 1 root root    2698 Jun 10 10:07 secure-20150610.gz
-rw-----. 1 root root    5500 Sep 28 14:48 secure-20150928
drwx-----. 2 root root       6 Jun 10 2014 speech-dispatcher
-rw-----. 1 root root       0 Mar  8 2015 spooler
-rw-----. 1 root root       0 Mar  8 2015 tallylog
drwxr-xr-x. 2 root root      22 Mar  6 2015 tuned
-rw-r--r--. 1 root root   209481 Jun  4 15:33 vboxadd-install.log
-rw-r--r--. 1 root root      73 Jun  4 15:33 vboxadd-install-x11.log
-rw-r--r--. 1 root root     148 Jun  4 15:33 VBoxGuestAdditions.log
-rw-r--r--. 1 root root     210 Jun  4 15:31 VBoxGuestAdditions-uninstall.log
-rw-rw-r--. 1 root utmp    50304 Sep 29 11:42 wtmp
-rw-r--r--. 1 root root    20240 Sep 29 11:25 Xorg.0.log
-rw-r--r--. 1 root root    20240 Sep 28 14:46 Xorg.0.log.old
-rw-r--r--. 1 root root   18540 Jun  4 14:59 Xorg.9.log
-rw-r--r--. 1 root root    56231 Mar  8 2015 Xorg.9.log.old
-rw-----. 1 root root   31581 Sep 28 14:52 yum.log

```

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 RHEL/CentOS, le daemon rsyslog est configuré par l'édition du fichier **/etc/sysconfig/rsyslog** :

```
[root@centos7 ~]# cat /etc/sysconfig/rsyslog
# Options for rsyslogd
# Syslogd options are deprecated since rsyslog v3.
# If you want to use them, switch to compatibility mode 2 by "-c 2"
# See rsyslogd(8) for more details
SYSLOGD_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

Directive	Version
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
cron	Message de cron ou at
daemon	Message d'un daemon
kern	Message du noyau
lpr	Message du système d'impression

Fonction	Description
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@centos7 ~]# cat /etc/rsyslog.conf
# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark # provides --MARK-- message capability

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

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

GLOBAL DIRECTIVES

```
# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog
```

```
# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
```

```
# File syncing capability is disabled by default. This feature is usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on
```

```
# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf
```

```
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on
```

```
# File to store the position in the journal
$IMJournalStateFile imjournal.state
```

RULES

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console
```

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

```
# The authpriv file has restricted access.
```

```
authpriv.*                                /var/log/secure

# Log all the mail messages in one place.
mail.*                                    -/var/log/maillog

# Log cron stuff
cron.*                                    /var/log/cron

# Everybody gets emergency messages
*.emerg                                  :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                           /var/log/spooler

# Save boot messages also to boot.log
local7.*                                  /var/log/boot.log


# ### 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.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$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 ###
```

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 \$.

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/spool/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 où 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@centos7 ~]# logger -p user.info Linux est super
```

Consultez la fin de votre syslog :

```
[root@centos7 ~]# tail /var/log/messages
Sep 29 11:42:17 centos7 fprintd: ** Message: entering main loop
Sep 29 11:42:20 centos7 su: (to root) trainee on pts/0
Sep 29 11:42:47 centos7 fprintd: ** Message: No devices in use, exit
Sep 29 11:49:39 centos7 pulseaudio[2833]: [alsa-sink] alsa-sink.c: ALSA woke us up to write new data to the
device, but there was actually nothing to write!
Sep 29 11:49:39 centos7 pulseaudio[2833]: [alsa-sink] alsa-sink.c: Most likely this is a bug in the ALSA driver
'snd_intel8x0'. Please report this issue to the ALSA developers.
Sep 29 11:49:39 centos7 pulseaudio[2833]: [alsa-sink] alsa-sink.c: We were woken up with POLLOUT set -- however a
subsequent snd_pcm_avail() returned 0 or another value < min_avail.
Sep 29 11:50:01 centos7 systemd: Created slice user-0.slice.
Sep 29 11:50:01 centos7 systemd: Starting Session 4 of user root.
Sep 29 11:50:01 centos7 systemd: Started Session 4 of user root.
Sep 29 11:55:57 centos7 trainee: Linux est super
```

Options de la commande

Les options de la commande logger sont :

```
[root@centos7 ~]# 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
  -h, --help          display this help text and exit
  -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
-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
-V, --version           output version information and exit
```

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@centos7 ~]# 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

# use date as a suffix of the rotated file
dateext

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

# RPM packages drop log rotation information into this directory
```

```
include /etc/logrotate.d

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

/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 1
}

# system-specific logs may be also 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
- compresser 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@centos7 ~]# 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 `/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
```

La Journalisation avec journald

Sous RHEL/CentOS 7, 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@centos7 ~]# ls -l /run/log/journal/
total 0
drwxr-sr-x. 2 root systemd-journal 60 Sep 29 14:41 a2feb9eb09b1488da0f23b99a66350f8
```

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

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

```
[root@centos7 ~]# mkdir /var/log/journal
[root@centos7 ~]# ls -l /var/log/journal/
total 0
[root@centos7 ~]# systemctl restart systemd-journald
[root@centos7 ~]# ls -l /run/log/journal/
ls: cannot access /run/log/journal/: No such file or directory
[root@centos7 ~]# ls -l /var/log/journal/
total 0
drwxr-sr-x. 2 root systemd-journal 73 Sep 29 15:30 a2feb9eb09b1488da0f23b99a66350f8
[root@centos7 ~]#
```



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@centos7 ~]# journalctl
-- Logs begin at Tue 2015-09-29 11:25:10 CEST, end at Tue 2015-09-29 18:10:01 CEST. --
Sep 29 11:25:10 centos7.fenestros.loc systemd-journal[82]: Runtime journal is using 8.0M (max 74.8M, leaving 112.3M of free 740.8M, current limit 74.8
Sep 29 11:25:10 centos7.fenestros.loc systemd-journal[82]: Runtime journal is using 8.0M (max 74.8M, leaving 112.3M of free 740.8M, current limit 74.8
Sep 29 11:25:10 centos7.fenestros.loc kernel: Initializing cgroup subsys cpuset
Sep 29 11:25:10 centos7.fenestros.loc kernel: Initializing cgroup subsys cpu
Sep 29 11:25:10 centos7.fenestros.loc kernel: Initializing cgroup subsys cpuacct
Sep 29 11:25:10 centos7.fenestros.loc kernel: Linux version 3.10.0-229.4.2.el7.x86_64
```

```
(builder@kbuilder.dev.centos.org) (gcc version 4.8.2 20140120 (R
Sep 29 11:25:10 centos7.fenestros.loc kernel: Command line: BOOT_IMAGE=/vmlinuz-3.10.0-229.4.2.el7.x86_64
root=UUID=b35de665-5ec8-4226-a533-58alb567ac
Sep 29 11:25:10 centos7.fenestros.loc kernel: e820: BIOS-provided physical RAM map:
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000005fffff] usable
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x00000000005fff0000-0x00000000005fffffff] ACPI data
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffffffff] reserved
Sep 29 11:25:10 centos7.fenestros.loc kernel: NX (Execute Disable) protection: active
Sep 29 11:25:10 centos7.fenestros.loc kernel: SMBIOS 2.5 present.
Sep 29 11:25:10 centos7.fenestros.loc kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 29 11:25:10 centos7.fenestros.loc kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 29 11:25:10 centos7.fenestros.loc kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 29 11:25:10 centos7.fenestros.loc kernel: No AGP bridge found
Sep 29 11:25:10 centos7.fenestros.loc kernel: e820: last_pfn = 0x5fff0 max_arch_pfn = 0x400000000
Sep 29 11:25:10 centos7.fenestros.loc kernel: MTRR default type: uncachable
Sep 29 11:25:10 centos7.fenestros.loc kernel: MTRR variable ranges disabled:
Sep 29 11:25:10 centos7.fenestros.loc kernel: x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
Sep 29 11:25:10 centos7.fenestros.loc kernel: CPU MTRRs all blank - virtualized system.
Sep 29 11:25:10 centos7.fenestros.loc kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff] mapped at
[ffff88000009fff0]
Sep 29 11:25:10 centos7.fenestros.loc kernel: Base memory trampoline at [ffff880000099000] 99000 size 24576
Sep 29 11:25:10 centos7.fenestros.loc kernel: init_memory_mapping: [mem 0x00000000-0x000fffff]
lines 1-29
```



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@centos7 ~]# journalctl /sbin/anacron
-- Logs begin at Tue 2015-09-29 11:25:10 CEST, end at Tue 2015-09-29 18:20:01 CEST. --
Sep 29 12:01:01 centos7.fenestros.loc anacron[4100]: Anacron started on 2015-09-29
Sep 29 12:01:01 centos7.fenestros.loc anacron[4100]: Will run job `cron.daily' in 38 min.
Sep 29 12:01:01 centos7.fenestros.loc anacron[4100]: Jobs will be executed sequentially
Sep 29 13:45:00 centos7.fenestros.loc anacron[4100]: Job `cron.daily' started
```



Important : Rappelez-vous que sous RHEL/CentOS 7 le répertoire **/sbin** est un lien symbolique vers **/usr/sbin**.

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@centos7 ~]# journalctl -b | more
-- Logs begin at Tue 2015-09-29 11:25:10 CEST, end at Tue 2015-09-29 18:28:56 CEST. --
Sep 29 11:25:10 centos7.fenestros.loc systemd-journal[82]: Runtime journal is using 8.0M (max 74.8M, leaving
112.3M of free 740.8M, current limit 74.8
M).
Sep 29 11:25:10 centos7.fenestros.loc systemd-journal[82]: Runtime journal is using 8.0M (max 74.8M, leaving
112.3M of free 740.8M, current limit 74.8
M).
Sep 29 11:25:10 centos7.fenestros.loc kernel: Initializing cgroup subsys cpuset
Sep 29 11:25:10 centos7.fenestros.loc kernel: Initializing cgroup subsys cpu
Sep 29 11:25:10 centos7.fenestros.loc kernel: Initializing cgroup subsys cpuacct
```

```
Sep 29 11:25:10 centos7.fenestros.loc kernel: Linux version 3.10.0-229.4.2.el7.x86_64
(builder@kbuilder.dev.centos.org) (gcc version 4.8.2 20140120 (R
ed Hat 4.8.2-16) (GCC) ) #1 SMP Wed May 13 10:06:09 UTC 2015
Sep 29 11:25:10 centos7.fenestros.loc kernel: Command line: BOOT_IMAGE=/vmlinuz-3.10.0-229.4.2.el7.x86_64
root=UUID=b35de665-5ec8-4226-a533-58a1b567ac
91 ro vconsole.keymap=fr crashkernel=auto vconsole.font=latacyrheb-sun16 rhgb quiet
Sep 29 11:25:10 centos7.fenestros.loc kernel: e820: BIOS-provided physical RAM map:
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000005fffff] usable
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x00000000005fff0000-0x00000000005fffffff] ACPI data
Sep 29 11:25:10 centos7.fenestros.loc kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffffffff] reserved
Sep 29 11:25:10 centos7.fenestros.loc kernel: NX (Execute Disable) protection: active
Sep 29 11:25:10 centos7.fenestros.loc kernel: SMBIOS 2.5 present.
Sep 29 11:25:10 centos7.fenestros.loc kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Sep 29 11:25:10 centos7.fenestros.loc kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 29 11:25:10 centos7.fenestros.loc kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 29 11:25:10 centos7.fenestros.loc kernel: No AGP bridge found
Sep 29 11:25:10 centos7.fenestros.loc kernel: e820: last_pfn = 0x5fff0 max_arch_pfn = 0x400000000
Sep 29 11:25:10 centos7.fenestros.loc kernel: MTRR default type: uncachable
Sep 29 11:25:10 centos7.fenestros.loc kernel: MTRR variable ranges disabled:
Sep 29 11:25:10 centos7.fenestros.loc kernel: x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
--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@centos7 ~]# journalctl -p warning
-- Logs begin at Tue 2015-09-29 11:25:10 CEST, end at Tue 2015-09-29 18:30:02 CEST. --
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: RSDP 000000000000e000 00024 (v02 VBOX )
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: XSDT 000000005fff0030 0003C (v01 VBOX VBOXXSDT 00000001 ASL
00000061)
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: FACP 000000005fff00f0 000F4 (v04 VBOX VBOXFACP 00000001 ASL
00000061)
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: DSDT 000000005fff0470 01BF1 (v01 VBOX VBOXBIOS 00000002
INTL 20100528)
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: FACS 000000005fff0200 00040
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: APIC 000000005fff0240 00054 (v02 VBOX VBOXAPIC 00000001 ASL
00000061)
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: SSDT 000000005fff02a0 001CC (v01 VBOX VBOXCPUPT 00000002
INTL 20100528)
Sep 29 11:25:10 centos7.fenestros.loc kernel: kexec: crashkernel=auto resulted in zero bytes of reserved memory.
Sep 29 11:25:10 centos7.fenestros.loc kernel: Zone ranges:
Sep 29 11:25:10 centos7.fenestros.loc kernel: DMA [mem 0x00001000-0x00ffffff]
Sep 29 11:25:10 centos7.fenestros.loc kernel: DMA32 [mem 0x01000000-0xffffffff]
Sep 29 11:25:10 centos7.fenestros.loc kernel: Normal empty
Sep 29 11:25:10 centos7.fenestros.loc kernel: Movable zone start for each node
Sep 29 11:25:10 centos7.fenestros.loc kernel: Early memory node ranges
Sep 29 11:25:10 centos7.fenestros.loc kernel: node 0: [mem 0x00001000-0x0009efff]
Sep 29 11:25:10 centos7.fenestros.loc kernel: node 0: [mem 0x00100000-0x5ffeffff]
Sep 29 11:25:10 centos7.fenestros.loc kernel: Built 1 zonelists in Node order, mobility grouping on. Total
pages: 386937
Sep 29 11:25:10 centos7.fenestros.loc kernel: Policy zone: DMA32
Sep 29 11:25:10 centos7.fenestros.loc kernel: tsc: Fast TSC calibration failed
Sep 29 11:25:10 centos7.fenestros.loc kernel: tsc: Unable to calibrate against PIT
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: All ACPI Tables successfully acquired
Sep 29 11:25:10 centos7.fenestros.loc kernel: NMI watchdog: disabled (cpu0): hardware events not enabled
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI: Executed 1 blocks of module-level executable AML code
```

```
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S1_] (20130517/hwxface-571)
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S2_] (20130517/hwxface-571)
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S3_] (20130517/hwxface-571)
Sep 29 11:25:10 centos7.fenestros.loc kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S4_] (20130517/hwxface-571)
Sep 29 11:25:10 centos7.fenestros.loc kernel: acpi PNP0A03:00: fail to add MMCONFIG information, can't access extended PCI configuration space under t
lines 1-29
```

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@centos7 ~]# journalctl --since 18:00 --until now
-- Logs begin at Tue 2015-09-29 11:25:10 CEST, end at Tue 2015-09-29 18:30:02 CEST. --
Sep 29 18:05:50 centos7.fenestros.loc systemd[1]: Time has been changed
Sep 29 18:06:23 centos7.fenestros.loc dbus-daemon[526]: dbus[526]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprint
Sep 29 18:06:23 centos7.fenestros.loc dbus[526]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service'
Sep 29 18:06:23 centos7.fenestros.loc systemd[1]: Starting Fingerprint Authentication Daemon...
Sep 29 18:06:23 centos7.fenestros.loc dbus-daemon[526]: dbus[526]: [system] Successfully activated service 'net.reactivated.Fprint'
Sep 29 18:06:23 centos7.fenestros.loc dbus[526]: [system] Successfully activated service 'net.reactivated.Fprint'
Sep 29 18:06:23 centos7.fenestros.loc systemd[1]: Started Fingerprint Authentication Daemon.
Sep 29 18:06:23 centos7.fenestros.loc fprintd[7642]: Launching FprintObject
Sep 29 18:06:23 centos7.fenestros.loc fprintd[7642]: ** Message: D-Bus service launched with name: net.reactivated.Fprint
Sep 29 18:06:23 centos7.fenestros.loc fprintd[7642]: ** Message: entering main loop
Sep 29 18:06:27 centos7.fenestros.loc gdm-password[7646]: gkr-pam: unlocked login keyring
```

```
Sep 29 18:06:27 centos7.fenestros.loc dbus-daemon[526]: dbus[526]: [system] Activating via systemd: service
name='org.freedesktop.hostname1' unit='dbu
Sep 29 18:06:27 centos7.fenestros.loc dbus[526]: [system] Activating via systemd: service
name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.
Sep 29 18:06:27 centos7.fenestros.loc systemd[1]: Starting Hostname Service...
Sep 29 18:06:27 centos7.fenestros.loc dbus-daemon[526]: dbus[526]: [system] Successfully activated service
'org.freedesktop.hostname1'
Sep 29 18:06:27 centos7.fenestros.loc dbus[526]: [system] Successfully activated service
'org.freedesktop.hostname1'
Sep 29 18:06:27 centos7.fenestros.loc systemd[1]: Started Hostname Service.
Sep 29 18:06:53 centos7.fenestros.loc fprintf[7642]: ** Message: No devices in use, exit
Sep 29 18:09:27 centos7.fenestros.loc systemd[1]: Stopping Journal Service...
Sep 29 18:09:27 centos7.fenestros.loc systemd-journal[362]: Journal stopped
Sep 29 18:09:27 centos7.fenestros.loc systemd-journal[7694]: Permanent journal is using 8.0M (max 699.0M, leaving
1.0G of free 2.5G, current limit 699
Sep 29 18:09:27 centos7.fenestros.loc systemd-journal[7694]: Permanent journal is using 8.0M (max 699.0M, leaving
1.0G of free 2.5G, current limit 699
Sep 29 18:09:27 centos7.fenestros.loc systemd-journal[7694]: Time spent on flushing to /var is 52.802ms for 1492
entries.
Sep 29 18:09:27 centos7.fenestros.loc systemd-journald[362]: Received SIGTERM
Sep 29 18:09:27 centos7.fenestros.loc systemd-journal[7694]: Journal started
Sep 29 18:09:27 centos7.fenestros.loc systemd[1]: Starting Trigger Flushing of Journal to Persistent Storage...
Sep 29 18:09:27 centos7.fenestros.loc systemd[1]: Started Trigger Flushing of Journal to Persistent Storage.
Sep 29 18:10:01 centos7.fenestros.loc systemd[1]: Created slice user-0.slice.
lines 1-29
```



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@centos7 ~]# journalctl -f
-- Logs begin at Tue 2015-09-29 11:25:10 CEST. --
Sep 29 18:28:56 centos7.fenestros.loc gdm-password[8599]: gkr-pam: unlocked login keyring
Sep 29 18:29:24 centos7.fenestros.loc fprintd[8595]: ** Message: No devices in use, exit
Sep 29 18:30:01 centos7.fenestros.loc systemd[1]: Created slice user-0.slice.
Sep 29 18:30:02 centos7.fenestros.loc systemd[1]: Starting Session 33 of user root.
Sep 29 18:30:02 centos7.fenestros.loc systemd[1]: Started Session 33 of user root.
Sep 29 18:30:02 centos7.fenestros.loc CROND[8670]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Sep 29 18:40:01 centos7.fenestros.loc systemd[1]: Created slice user-0.slice.
Sep 29 18:40:01 centos7.fenestros.loc systemd[1]: Starting Session 34 of user root.
Sep 29 18:40:01 centos7.fenestros.loc systemd[1]: Started Session 34 of user root.
Sep 29 18:40:01 centos7.fenestros.loc CROND[8809]: (root) CMD (/usr/lib64/sa/sa1 1 1)
```

Ouvrez un deuxième terminal et saisissez la commande suivante :

```
[trainee@centos7 ~]$ logger -p user.info Linux est super
```

Retournez consulter le premier terminal :

```
[root@centos7 ~]# journalctl -f
-- Logs begin at Tue 2015-09-29 11:25:10 CEST. --
Sep 29 18:28:56 centos7.fenestros.loc gdm-password[8599]: gkr-pam: unlocked login keyring
Sep 29 18:29:24 centos7.fenestros.loc fprintd[8595]: ** Message: No devices in use, exit
Sep 29 18:30:01 centos7.fenestros.loc systemd[1]: Created slice user-0.slice.
Sep 29 18:30:02 centos7.fenestros.loc systemd[1]: Starting Session 33 of user root.
Sep 29 18:30:02 centos7.fenestros.loc systemd[1]: Started Session 33 of user root.
Sep 29 18:30:02 centos7.fenestros.loc CROND[8670]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Sep 29 18:40:01 centos7.fenestros.loc systemd[1]: Created slice user-0.slice.
Sep 29 18:40:01 centos7.fenestros.loc systemd[1]: Starting Session 34 of user root.
```

```
Sep 29 18:40:01 centos7.fenestros.loc systemd[1]: Started Session 34 of user root.
Sep 29 18:40:01 centos7.fenestros.loc CROND[8809]: (root) CMD (/usr/lib64/sa/sa1 1 1)
Sep 29 18:43:00 centos7.fenestros.loc trainee[8930]: 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@centos7 ~]# 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@centos7 ~]# journalctl _UID=
```

```
0      1000  172   32   42   70   81   994   997   999
[root@centos7 ~]# journalctl _COMM=
abrtd                avahi-daemon        dracut-cmdline      kdumpctl            NetworkManager      rtkit-daemon        su
vboxadd-service
accounts-daemon      bluetoothd          fprintd             libvirt             nm-dispatcher        run-parts            systemd
vmtoolsd
alsactl              chronyd             gdm-session-wor     logger              polkitd              sal                  systemd-
fsck
anacron              colord              gnome-session       master              postlog              sh                   systemd-
journal
audispd              crond               goa-daemon          ModemManager        pulseaudio           smartd               systemd-
logind
auditd              dbus-daemon         goa-identity-se     netcf-transacti     rngd                  sm-notify            udisksd
augenrules           dhclient            irqbalance          network             rpcbind              sshd                  vboxadd
[root@centos7 ~]# journalctl _COMM=
```