Version : **2024.01**

Dernière mise-à-jour : 2024/10/01 08:03

LCF602 - 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 /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@centos8 ~]# dmesg | more
[    0.000000] Linux version 4.18.0-240.22.1.el8_3.x86_64 (mockbuild@kbuilder.bsys.centos.org) (gcc version 8.3.1
20191121 (Red Hat 8.3.1-5) (G
CC)) #1 SMP Thu Apr 8 19:01:30 UTC 2021
[    0.000000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-4.18.0-240.22.1.el8_3.x86_64
root=UUID=4c0cc28c-0d59-45be-bd73-d292b80be33c ro cra
shkernel=auto resume=UUID=c8bb3f47-d67f-4b21-b781-766899dc83d4 rhgb quiet
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
[    0.000000] 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 0x0000000000100000-0x00000000dffeffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
[    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
[    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] Hypervisor detected: KVM
--More--
```

Les option de cette commande sont :

```
[root@centos8 ~]# dmesg --help

Usage:
 dmesg [options]

Display or control the kernel ring buffer.

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)
                               colors are enabled by default
 -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
 -p, --force-prefix          force timestamp output on each line of multi-line messages
 -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 (may be inaccurate!)
 -t, --notime                don't show any timestamp with messages
```

```
     --time-format <format>  show timestamp using the given format:
                               [delta|reltime|ctime|notime|iso]
Suspending/resume will make ctime and iso timestamps inaccurate.

 -h, --help                  display this help
 -V, --version               display version

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).
```

LAB #1 - Surveillance Sécuritaire

1.1 - La Commande last

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

```
[root@centos8 ~]# last
trainee  pts/0        10.0.2.2         Thu Jun  3 09:01   still logged in
reboot   system boot  4.18.0-240.22.1. Thu Jun  3 09:01   still running
trainee  pts/0        10.0.2.2         Wed Jun  2 12:07 - crash  (20:54)
trainee  pts/0        10.0.2.2         Wed Jun  2 11:16 - 12:06  (00:50)
reboot   system boot  4.18.0-240.22.1. Wed Jun  2 11:12   still running
trainee  pts/0        10.0.2.2         Wed Jun  2 11:13 - 11:14  (00:01)
reboot   system boot  4.18.0-240.22.1. Wed Jun  2 11:10 - 11:14  (00:04)
trainee  pts/0        10.0.2.2         Wed Jun  2 11:08 - 11:12  (00:04)
reboot   system boot  4.18.0-240.22.1. Wed Jun  2 11:04 - 11:12  (00:07)
trainee  pts/0        10.0.2.2         Wed Jun  2 06:40 - 11:06  (04:26)
trainee  pts/0        10.0.2.2         Wed Jun  2 06:39 - 06:39  (00:00)
reboot   system boot  4.18.0-240.22.1. Wed Jun  2 06:07 - 11:07  (04:59)
trainee  pts/1        10.0.2.2         Wed May 26 16:51 - crash (6+13:15)
trainee  pts/0        10.0.2.2         Wed May 26 10:37 - 18:50  (08:13)
trainee  pts/0        10.0.2.2         Wed May 26 08:48 - 10:36  (01:48)
trainee  tty1                          Wed May 26 08:47 - crash (6+21:19)
reboot   system boot  4.18.0-240.22.1. Wed May 26 08:44 - 11:07 (7+02:22)
trainee  pts/0        10.0.2.2         Wed Apr 21 07:23 - 19:14  (11:51)
trainee  pts/0        10.0.2.2         Tue Apr 20 23:13 - 07:22  (08:08)
trainee  pts/1                         Tue Apr 20 10:59 - 11:00  (00:00)
trainee  pts/0        10.0.2.2         Tue Apr 20 09:59 - 23:13  (13:13)
trainee  pts/1        10.0.2.2         Tue Apr 20 04:10 - 04:29  (00:19)
trainee  pts/0        10.0.2.2         Tue Apr 20 02:21 - 09:57  (07:36)
trainee  tty1                          Tue Apr 20 02:17 - crash (36+06:26)
trainee  pts/0        10.0.2.2         Mon Apr 19 13:55 - 02:17  (12:22)
trainee  pts/0        10.0.2.2         Mon Apr 19 12:05 - 13:47  (01:42)
reboot   system boot  4.18.0-240.22.1. Mon Apr 19 12:05 - 11:07 (43+23:01)
trainee  pts/0        10.0.2.2         Mon Apr 19 11:40 - crash  (00:24)
```

```
reboot   system boot  4.18.0-147.8.1.e Mon Apr 19 11:37 - 11:07 (43+23:29)
trainee  pts/0        10.0.2.2         Tue Sep  1 09:59 - 11:10  (01:10)
reboot   system boot  4.18.0-147.8.1.e Tue Sep  1 09:58 - 11:10  (01:11)
reboot   system boot  4.18.0-147.8.1.e Fri May  8 08:13 - 11:10 (116+02:56)

wtmp begins Fri May  8 08:13:49 2020
```

Les option de cette commande sont :

```
[root@centos8 ~]# last --help

Usage:
 last [options] [<username>...] [<tty>...]

Show a listing of last logged in users.

Options:
 -<number>            how many lines to show
 -a, --hostlast       display hostnames in the last column
 -d, --dns            translate the IP number back into a hostname
 -f, --file <file>    use a specific file instead of /var/log/wtmp
 -F, --fulltimes      print full login and logout times and dates
 -i, --ip             display IP numbers in numbers-and-dots notation
 -n, --limit <number> how many lines to show
 -R, --nohostname     don't display the hostname field
 -s, --since <time>   display the lines since the specified time
 -t, --until <time>   display the lines until the specified time
 -p, --present <time> display who were present at the specified time
 -w, --fullnames      display full user and domain names
 -x, --system         display system shutdown entries and run level changes
     --time-format <format>  show timestamps in the specified <format>:
                               notime|short|full|iso

 -h, --help           display this help
```

```
 -V, --version        display version

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

1.2 - La Commande lastlog

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

```
[root@centos8 ~]# lastlog
Username         Port     From             Latest
root             pts/0                     Thu Jun  3 09:01:46 -0400 2021
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
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**
systemd-coredump                           **Never logged in**
systemd-resolve                            **Never logged in**
tss                                        **Never logged in**
polkitd                                    **Never logged in**
unbound                                    **Never logged in**
libstoragemgmt                             **Never logged in**
cockpit-ws                                 **Never logged in**
sssd                                       **Never logged in**
setroubleshoot                             **Never logged in**
```

```
sshd                                           **Never logged in**
chrony                                         **Never logged in**
tcpdump                                        **Never logged in**
trainee          pts/0    10.0.2.2             Thu Jun  3 09:01:39 -0400 2021
cockpit-wsinstance                               **Never logged in**
rngd                                           **Never logged in**
gluster                                        **Never logged in**
qemu                                           **Never logged in**
rpc                                            **Never logged in**
rpcuser                                        **Never logged in**
saslauth                                       **Never logged in**
radvd                                          **Never logged in**
dnsmasq                                        **Never logged in**
fenestros2       pts/0                         Tue Apr 20 15:20:26 -0400 2021
fenestros1                                     **Never logged in**
apache                                         **Never logged in**
```

Les option de cette commande sont :

```
[root@centos8 ~]# lastlog --help
Usage: lastlog [options]

Options:
  -b, --before DAYS             print only lastlog records older than DAYS
  -C, --clear                   clear lastlog record of an user (usable only with -u)
  -h, --help                    display this help message and exit
  -R, --root CHROOT_DIR         directory to chroot into
  -S, --set                     set lastlog record to current time (usable only with -u)
  -t, --time DAYS               print only lastlog records more recent than DAYS
  -u, --user LOGIN              print lastlog record of the specified LOGIN
```

1.3 - 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@centos8 ~]# lastb
trainee  tty1                         Thu Jun  3 09:51 - 09:51  (00:00)
trainee  tty1                         Thu Jun  3 09:51 - 09:51  (00:00)
trqinee  tty1                         Thu Jun  3 09:51 - 09:51  (00:00)

btmp begins Thu Jun  3 09:51:07 2021
```

Les options de cette commande sont :

```
[root@centos8 ~]# lastb --help

Usage:
 lastb [options] [<username>...] [<tty>...]

Show a listing of last logged in users.

Options:
 -<number>            how many lines to show
 -a, --hostlast       display hostnames in the last column
 -d, --dns            translate the IP number back into a hostname
 -f, --file <file>    use a specific file instead of /var/log/btmp
 -F, --fulltimes      print full login and logout times and dates
 -i, --ip             display IP numbers in numbers-and-dots notation
 -n, --limit <number> how many lines to show
 -R, --nohostname     don't display the hostname field
 -s, --since <time>   display the lines since the specified time
 -t, --until <time>   display the lines until the specified time
 -p, --present <time> display who were present at the specified time
 -w, --fullnames      display full user and domain names
```

```
 -x, --system         display system shutdown entries and run level changes
     --time-format <format>  show timestamps in the specified <format>:
                               notime|short|full|iso

 -h, --help           display this help
 -V, --version        display version

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

1.4 - Le Fichier /var/log/secure

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

```
[root@centos8 ~]# tail -n 15 /var/log/secure
Jun  3 09:01:20 centos8 sshd[905]: Server listening on :: port 22.
Jun  3 09:01:39 centos8 sshd[1585]: Accepted password for trainee from 10.0.2.2 port 52734 ssh2
Jun  3 09:01:39 centos8 systemd[1590]: pam_unix(systemd-user:session): session opened for user trainee by (uid=0)
Jun  3 09:01:39 centos8 sshd[1585]: pam_unix(sshd:session): session opened for user trainee by (uid=0)
Jun  3 09:01:46 centos8 su[1627]: pam_systemd(su-l:session): Cannot create session: Already running in a session
or user slice
Jun  3 09:01:46 centos8 su[1627]: pam_unix(su-l:session): session opened for user root by trainee(uid=1000)
Jun  3 09:51:05 centos8 login[1158]: pam_unix(login:auth): check pass; user unknown
Jun  3 09:51:05 centos8 login[1158]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0
tty=tty1 ruser= rhost=
Jun  3 09:51:07 centos8 login[1158]: FAILED LOGIN 1 FROM tty1 FOR trqinee, Authentication failure
Jun  3 09:51:18 centos8 unix_chkpwd[2400]: password check failed for user (trainee)
Jun  3 09:51:18 centos8 login[1158]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0
tty=tty1 ruser= rhost=  user=trainee
Jun  3 09:51:20 centos8 login[1158]: FAILED LOGIN 2 FROM tty1 FOR trainee, Authentication failure
Jun  3 09:51:45 centos8 login[1158]: pam_unix(login:auth): check pass; user unknown
Jun  3 09:51:45 centos8 login[1158]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0
tty=tty1 ruser= rhost=
```

```
Jun  3 09:51:47 centos8 login[1158]: FAILED LOGIN SESSION FROM tty1 FOR trainee  , Authentication failure
```

1.5 - Gestion des Evénements audit

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@centos8 ~]# tail -n 15 /var/log/audit/audit.log
type=PROCTITLE msg=audit(1622728321.894:455): proctitle=2F7573722F7362696E2F63726F6E64002D6E
type=USER_START msg=audit(1622728321.901:456): pid=2420 uid=0 auid=1000 ses=53 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="trainee"
exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'UID="root" AUID="trainee"
type=CRED_REFR msg=audit(1622728321.902:457): pid=2420 uid=0 auid=1000 ses=53 subj=system_u:system_r:crond_t:s0-
s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_localuser,pam_unix acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'UID="root" AUID="trainee"
type=CRED_DISP msg=audit(1622728321.908:458): pid=2420 uid=0 auid=1000 ses=53 subj=system_u:system_r:crond_t:s0-
s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_localuser,pam_unix acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'UID="root" AUID="trainee"
type=USER_END msg=audit(1622728321.910:459): pid=2420 uid=0 auid=1000 ses=53 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="trainee"
exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'UID="root" AUID="trainee"
type=SERVICE_STOP msg=audit(1622728330.965:460): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=?
addr=? terminal=? res=success'UID="root" AUID="unset"
```

```
type=USER_ACCT msg=audit(1622728381.954:461): pid=2439 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_access,pam_unix,pam_localuser
acct="trainee" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'UID="root" AUID="unset"
type=CRED_ACQ msg=audit(1622728381.954:462): pid=2439 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_localuser,pam_unix
acct="trainee" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'UID="root" AUID="unset"
type=LOGIN msg=audit(1622728381.954:463): pid=2439 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-
auid=4294967295 auid=1000 tty=(none) old-ses=4294967295 ses=54 res=1UID="root" OLD-AUID="unset" AUID="trainee"
type=SYSCALL msg=audit(1622728381.954:463): arch=c000003e syscall=1 success=yes exit=4 a0=7 a1=7ffdcd7a6d50 a2=4
a3=0 items=0 ppid=1126 pid=2439 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=54 comm="crond" exe="/usr/sbin/crond" subj=system_u:system_r:crond_t:s0-s0:c0.c1023 key=(null)ARCH=x86_64
SYSCALL=write AUID="trainee" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root"
FSGID="root"
type=PROCTITLE msg=audit(1622728381.954:463): proctitle=2F7573722F7362696E2F63726F6E64002D6E
type=USER_START msg=audit(1622728381.960:464): pid=2439 uid=0 auid=1000 ses=54 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="trainee"
exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'UID="root" AUID="trainee"
type=CRED_REFR msg=audit(1622728381.962:465): pid=2439 uid=0 auid=1000 ses=54 subj=system_u:system_r:crond_t:s0-
s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_localuser,pam_unix acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'UID="root" AUID="trainee"
type=CRED_DISP msg=audit(1622728381.966:466): pid=2439 uid=0 auid=1000 ses=54 subj=system_u:system_r:crond_t:s0-
s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_localuser,pam_unix acct="trainee" exe="/usr/sbin/crond"
hostname=? addr=? terminal=cron res=success'UID="root" AUID="trainee"
type=USER_END msg=audit(1622728381.968:467): pid=2439 uid=0 auid=1000 ses=54 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="trainee"
exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'UID="root" AUID="trainee"
```

La gestion des événements 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@centos8 ~]# cat /etc/audit/auditd.conf
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
transport = TCP
krb5_principal = auditd
```

```
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
q_depth = 400
overflow_action = SYSLOG
max_restarts = 10
plugin_dir = /etc/audit/plugins.d
```

Les option de cette commande sont :

```
[root@centos8 ~]# auditd --help
auditd: unrecognized option '--help'
Usage: auditd [-f] [-l] [-n] [-s disable|enable|nochange] [-c <config_file>]
```

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@centos8 ~]# cat /etc/audit/audit.rules
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1
--backlog_wait_time 60000
```

Les options de cette commande sont :

```
[root@centos8 ~]# 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
    --reset-lost         Reset the lost record counter
```

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@centos8 ~]# aureport

Summary Report
======================
Range of time in logs: 05/08/2020 08:13:52.320 - 06/03/2021 10:20:02.028
Selected time for report: 05/08/2020 08:13:52 - 06/03/2021 10:20:02.028
Number of changes in configuration: 46
Number of changes to accounts, groups, or roles: 56
Number of logins: 21
Number of failed logins: 5
Number of authentications: 50
Number of failed authentications: 8
Number of users: 3
Number of terminals: 10
Number of host names: 4
Number of executables: 22
Number of commands: 11
Number of files: 0
Number of AVC's: 0
Number of MAC events: 35
Number of failed syscalls: 0
Number of anomaly events: 7
Number of responses to anomaly events: 0
Number of crypto events: 287
```

```
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 616
Number of events: 6030
```

Les options de cette commande sont :

```
[root@centos8 ~]# 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@centos8 ~]# ausearch -ui 1000 | more
----
time->Tue Sep  1 11:05:28 2020
type=USER_AUTH msg=audit(1598972728.209:77): pid=1633 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=localhost.locald
omain addr=? terminal=pts/0 res=success'
----
time->Tue Sep  1 11:05:28 2020
type=USER_ACCT msg=audit(1598972728.214:78): pid=1633 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=localh
ost.localdomain addr=? terminal=pts/0 res=success'
----
time->Tue Sep  1 11:05:28 2020
```

```
type=CRED_ACQ msg=audit(1598972728.218:79): pid=1633 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=localhost.localdomain ad
dr=? terminal=pts/0 res=success'
----
time->Tue Sep  1 11:05:28 2020
type=USER_START msg=audit(1598972728.223:80): pid=1633 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_umask
,pam_xauth acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/0 res=success'
----
time->Tue Sep  1 11:10:13 2020
type=USER_END msg=audit(1598973013.687:87): pid=1633 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_close
grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,
pam_xauth acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/0 res=success'
----
time->Tue Sep  1 11:10:13 2020
type=CRED_DISP msg=audit(1598973013.687:88): pid=1633 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=localhost.localdomain a
ddr=? terminal=pts/0 res=success'
----
time->Mon Apr 19 11:48:01 2021
type=USER_AUTH msg=audit(1618847281.847:77): pid=1768 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=centos8.ittraini
ng.loc addr=? terminal=pts/0 res=success'
----
time->Mon Apr 19 11:48:01 2021
type=USER_ACCT msg=audit(1618847281.847:78): pid=1768 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=centos
8.ittraining.loc addr=? terminal=pts/0 res=success'
```

```
----
time->Mon Apr 19 11:48:01 2021
type=CRED_ACQ msg=audit(1618847281.847:79): pid=1768 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=centos8.ittraining.loc a
ddr=? terminal=pts/0 res=success'
----
time->Mon Apr 19 11:48:01 2021
type=USER_START msg=audit(1618847281.883:80): pid=1768 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_umask
,pam_xauth acct="root" exe="/usr/bin/su" hostname=centos8.ittraining.loc addr=? terminal=pts/0 res=success'
----
time->Mon Apr 19 12:04:39 2021
type=USER_END msg=audit(1618848279.544:541): pid=1768 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_close
grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask
,pam_xauth acct="root" exe="/usr/bin/su" hostname=centos8.ittraining.loc addr=? terminal=pts/0 res=success'
----
time->Mon Apr 19 12:04:39 2021
type=CRED_DISP msg=audit(1618848279.544:542): pid=1768 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=centos8.ittraining.loc
 addr=? terminal=pts/0 res=success'
----
time->Mon Apr 19 12:05:57 2021
type=USER_AUTH msg=audit(1618848357.204:69): pid=4892 uid=1000 auid=1000 ses=1
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=? acct="root"
exe="/usr/bin/su" hostname=centos8.ittraining.loc
addr=? terminal=pts/0 res=failed'
----
time->Mon Apr 19 12:06:03 2021
type=USER_AUTH msg=audit(1618848363.134:70): pid=4901 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=centos8.ittraini
ng.loc addr=? terminal=pts/0 res=success'
----
--More--
```

Les options de cette commande sont :

```
[root@centos8 ~]# 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
    --format [raw|default|interpret|csv|text] results format options
    -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@centos8 ~]# tail -n 15 /var/log/messages
Jun  3 10:15:01 centos8 systemd[1]: session-76.scope: Succeeded.
Jun  3 10:16:01 centos8 systemd[1]: Started Session 77 of user trainee.
Jun  3 10:16:01 centos8 systemd[1]: session-77.scope: Succeeded.
Jun  3 10:17:01 centos8 systemd[1]: Started Session 78 of user trainee.
Jun  3 10:17:01 centos8 systemd[1]: session-78.scope: Succeeded.
Jun  3 10:18:01 centos8 systemd[1]: Started Session 79 of user trainee.
Jun  3 10:18:01 centos8 systemd[1]: session-79.scope: Succeeded.
Jun  3 10:19:01 centos8 systemd[1]: Started Session 80 of user trainee.
Jun  3 10:19:01 centos8 systemd[1]: session-80.scope: Succeeded.
Jun  3 10:20:02 centos8 systemd[1]: Started Session 81 of user trainee.
Jun  3 10:20:02 centos8 systemd[1]: session-81.scope: Succeeded.
Jun  3 10:21:01 centos8 systemd[1]: Started Session 82 of user trainee.
Jun  3 10:21:01 centos8 systemd[1]: session-82.scope: Succeeded.
Jun  3 10:22:01 centos8 systemd[1]: Started Session 83 of user trainee.
Jun  3 10:22:01 centos8 systemd[1]: session-83.scope: Succeeded.
```

Applications

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

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

```
[root@centos8 ~]# ls -l /var/log
total 2448
drwxr-xr-x. 2 root   root      280 May  8  2020 anaconda
drwx------. 2 root   root       23 Apr 23  2020 audit
```

```
-rw-------. 1 root   root        0 Jun  3 10:16 boot.log
-rw-------. 1 root   root    19710 Apr 19 13:44 boot.log-20210419
-rw-------. 1 root   root     9548 May 26 09:35 boot.log-20210526
-rw-------. 1 root   root     9491 Jun  2 07:40 boot.log-20210602
-rw-------. 1 root   root    38555 Jun  3 10:16 boot.log-20210603
-rw-rw----. 1 root   utmp     1152 Jun  3 09:51 btmp
-rw-rw----. 1 root   utmp      384 May 26 10:37 btmp-20210602
drwxr-xr-x. 2 chrony chrony      6 Nov 19  2019 chrony
-rw-------. 1 root   root    35397 Jun  3 10:22 cron
-rw-------. 1 root   root     5652 Apr 19 13:01 cron-20210419
-rw-------. 1 root   root    16279 May 26 09:01 cron-20210526
-rw-------. 1 root   root     5117 Jun  2 07:01 cron-20210602
-rw-------. 1 root   root    13577 Jun  3 10:12 dnf.librepo.log
-rw-r--r--. 1 root   root    43871 Apr 19 13:15 dnf.librepo.log-20210419
-rw-------. 1 root   root    89109 May 26 08:54 dnf.librepo.log-20210526
-rw-------. 1 root   root    17737 Jun  2 07:18 dnf.librepo.log-20210602
-rw-r--r--. 1 root   root   749350 Jun  3 10:12 dnf.log
-rw-r--r--. 1 root   root   138497 Jun  3 10:12 dnf.rpm.log
-rw-r-----. 1 root   root     3808 Jun  3 09:01 firewalld
drwxr-xr-x. 2 root   root        6 Nov  3  2020 glusterfs
-rw-------. 1 root   root      510 Jun  3 09:58 hawkey.log
-rw-r--r--. 1 root   root      561 Apr 19 12:13 hawkey.log-20210419
-rw-------. 1 root   root     3927 May 26 08:54 hawkey.log-20210526
-rw-------. 1 root   root      306 Jun  2 06:17 hawkey.log-20210602
-rw-rw-r--. 1 root   utmp   293168 Jun  3 09:01 lastlog
drwx------. 3 root   root       18 Apr 19 12:07 libvirt
-rw-------. 1 root   root        0 Jun  2 07:40 maillog
-rw-------. 1 root   root        0 May  8  2020 maillog-20210419
-rw-------. 1 root   root        0 Apr 19 13:44 maillog-20210526
-rw-------. 1 root   root        0 May 26 09:35 maillog-20210602
-rw-------. 1 root   root   452404 Jun  3 10:22 messages
-rw-------. 1 root   root   397916 Apr 19 13:15 messages-20210419
-rw-------. 1 root   root   173289 May 26 09:19 messages-20210526
-rw-------. 1 root   root   123100 Jun  2 07:38 messages-20210602
```

```
drwx------. 2 root   root        6 May  8  2020 private
drwx------. 3 root   root       17 Aug 17  2020 samba
-rw-------. 1 root   root     6554 Jun  3 09:51 secure
-rw-------. 1 root   root    10835 Apr 19 12:07 secure-20210419
-rw-------. 1 root   root    11884 May 26 08:49 secure-20210526
-rw-------. 1 root   root     3633 Jun  2 06:40 secure-20210602
-rw-------. 1 root   root        0 Jun  2 07:40 spooler
-rw-------. 1 root   root        0 May  8  2020 spooler-20210419
-rw-------. 1 root   root        0 Apr 19 13:44 spooler-20210526
-rw-------. 1 root   root        0 May 26 09:35 spooler-20210602
drwxr-x---. 2 sssd   sssd      270 Jun  3 10:16 sssd
drwxr-xr-x. 3 root   root       21 Apr 19 12:07 swtpm
drwxr-xr-x. 2 root   root       23 Jan  4 11:24 tuned
-rw-rw-r--. 1 root   utmp    34176 Jun  3 09:51 wtmp
```

LAB #2 - 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@centos8 ~]# 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
SYSLOGD_OPTIONS="-c 0"	syslogd

2.1 - 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

Niveau	Priorité	Description
7	debug	Condition normale - message de débogage

2.2 - 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
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

2.3 - /etc/rsyslog.conf

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

```
[root@centos8 ~]# cat /etc/rsyslog.conf
# rsyslog configuration file

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

#### MODULES ####
```

```
module(load="imuxsock"      # provides support for local system logging (e.g. via logger command)
       SysSock.Use="off") # Turn off message reception via local log socket;
              # local messages are retrieved through imjournal now.
module(load="imjournal"       # provides access to the systemd journal
       StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
#module(load="imudp") # needs to be done just once
#input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
#module(load="imtcp") # needs to be done just once
#input(type="imtcp" port="514")

#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")

# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")

# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")

#### 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


# ### sample forwarding rule ###
#action(type="omfwd"
# 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.
#queue.filename="fwdRule1"       # unique name prefix for spool files
#queue.maxdiskspace="1g"         # 1gb space limit (use as much as possible)
#queue.saveonshutdown="on"       # save messages to disk on shutdown
#queue.type="LinkedList"         # run asynchronously
#action.resumeRetryCount="-1"    # infinite retries if host is down
# Remote Logging (we use TCP for reliable delivery)
```

```
# remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")
```

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 **module**.

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**
module(load=“imuxsock” SysSock.Use=“off”)	Active la trace des messages locaux, per exemple de la commande **logger**
module(load=“imjournal” StateFile=“imjournal.state”)	Fournit un accès au journal **systemd**
module(load=“imklog”)	Active la trace de messages du **noyau**
module(load=“immark”)	Active la trace des messages de type **mark**
module(load=“imudp”)	Active la réception de messages en utilisant le protocole **UDP**
module(load=“imtcp”)	Active la réception de messages en utilisant le protocole **TCP**

Dans le fichier **/etc/rsyslog.conf** nous pouvons constater que les inputs **module(load=“imuxsock” SysSock.Use=“off”)** et **module(load=“imjournal” StateFile=“imjournal.state”)** sont activés :

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

```
module(load="imuxsock"      # provides support for local system logging (e.g. via logger command)
       SysSock.Use="off") # Turn off message reception via local log socket;
              # local messages are retrieved through imjournal now.
module(load="imjournal"       # provides access to the systemd journal
       StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
#module(load="imudp") # needs to be done just once
#input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
#module(load="imtcp") # needs to be done just once
#input(type="imtcp" port="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 :

```
...
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
...
```

Important : Les deux directives **module(load=“imudp”)** et **input(type=“imudp” port=“514”)** crée un **Écouteur** sur le port UDP/514 tandis que les deux directives **module(load=“imtcp”)** et **input(type=“imtcp” port=“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 numéro du port.

Pour envoyer l'ensemble des traces de journalisation vers un serveur rsyslog distant, il convient de décommenter et modifier une ligne dans la section suivante du fichier **/etc/rsyslog.conf** :

```
...
# ### sample forwarding rule ###
#action(type="omfwd"
# 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.
#queue.filename="fwdRule1"       # unique name prefix for spool files
#queue.maxdiskspace="1g"         # 1gb space limit (use as much as possible)
#queue.saveonshutdown="on"       # save messages to disk on shutdown
#queue.type="LinkedList"         # run asynchronously
#action.resumeRetryCount="-1"    # infinite retries if host is down
# Remote Logging (we use TCP for reliable delivery)
# remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
Target="remote_host" Port="514" Protocol="tcp")
...
```

Important : Ces directives utilisent le protocole TCP. Le serveur distant doit donc être configuré pour ce mode de communication. La directive **Target=“remote_host” Port=“514” Protocol=“tcp”)** 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 :

```
module(load="builtin:omfile" Template="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.

LAB #3 - 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@centos8 ~]# logger -p user.info Linux est super
```

Consultez la fin de votre syslog :

```
[root@centos8 ~]# tail /var/log/messages
Jun  3 12:55:01 centos8 systemd[1]: session-237.scope: Succeeded.
Jun  3 12:56:01 centos8 systemd[1]: Started Session 238 of user trainee.
Jun  3 12:56:01 centos8 systemd[1]: session-238.scope: Succeeded.
Jun  3 12:57:01 centos8 systemd[1]: Started Session 239 of user trainee.
Jun  3 12:57:01 centos8 systemd[1]: session-239.scope: Succeeded.
Jun  3 12:58:01 centos8 systemd[1]: Started Session 240 of user trainee.
Jun  3 12:58:01 centos8 systemd[1]: session-240.scope: Succeeded.
Jun  3 12:58:55 centos8 trainee[5139]: Linux est super
Jun  3 12:59:01 centos8 systemd[1]: Started Session 241 of user trainee.
Jun  3 12:59:01 centos8 systemd[1]: session-241.scope: Succeeded.
```

Les options de la commande logger sont :

```
[root@centos8 ~]# logger --help

Usage:
 logger [options] [<message>]

Enter messages into the system log.

Options:
 -i                        log the logger command's PID
     --id[=<id>]           log the given <id>, or otherwise the PID
 -f, --file <file>         log the contents of this file
```

```
 -e, --skip-empty         do not log empty lines when processing files
     --no-act             do everything except the write the log
 -p, --priority <prio>    mark given message with this priority
     --octet-count        use rfc6587 octet counting
     --prio-prefix        look for a prefix on every line read from stdin
 -s, --stderr             output message to standard error as well
 -S, --size <size>        maximum size for a single message
 -t, --tag <tag>          mark every line with this tag
 -n, --server <name>      write to this remote syslog server
 -P, --port <port>        use this port for UDP or TCP connection
 -T, --tcp                use TCP only
 -d, --udp                use UDP only
     --rfc3164            use the obsolete BSD syslog protocol
     --rfc5424[=<snip>]   use the syslog protocol (the default for remote);
                            <snip> can be notime, or notq, and/or nohost
     --sd-id <id>         rfc5424 structured data ID
     --sd-param <data>    rfc5424 structured data name=value
     --msgid <msgid>      set rfc5424 message id field
 -u, --socket <socket>    write to this Unix socket
     --socket-errors[=<on|off|auto>]
                          print connection errors when using Unix sockets
     --journald[=<file>]  write journald entry

 -h, --help               display this help
 -V, --version            display version

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

LAB #4 - 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@centos8 ~]# 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

# 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
- 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.

Les options de la commande logrotate sont :

```
[root@centos8 ~]# logrotate --help
Usage: logrotate [OPTION...] <configfile>
  -d, --debug               Don't do anything, just test and print debug
                            messages
  -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
  -l, --log=logfile         Log file or 'syslog' to log to syslog
      --version             Display version information

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

LAB #5 - La Journalisation avec journald

Sous RHEL/CentOS 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@centos8 ~]# ls -l /run/log/journal/
```

```
total 0
drwxr-s---+ 2 root systemd-journal 60 Jun  3 09:01 de79af4f226d480fa7d3fec4cabbf97a
```

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

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

```
[root@centos8 ~]# mkdir /var/log/journal
[root@centos8 ~]# ls -l /var/log/journal/
total 0
[root@centos8 ~]# systemctl restart systemd-journald
[root@centos8 ~]# ls -l /run/log/journal/
ls: cannot access '/run/log/journal/': No such file or directory
[root@centos8 ~]# ls -l /var/log/journal/
total 0
drwxr-xr-x. 2 root root 28 Jun  3 13:03 de79af4f226d480fa7d3fec4cabbf97a
```

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 :

```
[root@centos8 ~]# cat /etc/systemd/journald.conf
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See journald.conf(5) for details.
```

```
[Journal]
#Storage=auto
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
#RateLimitIntervalSec=30s
#RateLimitBurst=10000
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize=
#SystemMaxFiles=100
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#RuntimeMaxFiles=100
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=no
ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
#LineMax=48K
```

5.1 - Consultation des Journaux

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

```
[root@centos8 ~]# journalctl
-- Logs begin at Thu 2021-06-03 09:01:10 EDT, end at Thu 2021-06-03 13:08:01 EDT. --
Jun 03 09:01:10 centos8.ittraining.loc kernel: Linux version 4.18.0-240.22.1.el8_3.x86_64
(mockbuild@kbuilder.bsys.centos.org) (gcc version 8.3.1 20191121 (Red Hat 8.3.1-5) (GCC)) #1 SMP Thu Apr 8
19:01:30 UTC 2021
Jun 03 09:01:10 centos8.ittraining.loc kernel: Command line:
BOOT_IMAGE=(hd0,msdos1)/vmlinuz-4.18.0-240.22.1.el8_3.x86_64 root=UUID=4c0cc28c-0d59-45be-bd73-d292b80be33c ro
crashkernel=auto resume=UUID=c8bb3f47-d67f-4b21-b781-766899dc83d4>
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
registers'
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes,
using 'standard' format.
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-provided physical RAM map:
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Jun 03 09:01:10 centos8.ittraining.loc kernel: NX (Execute Disable) protection: active
Jun 03 09:01:10 centos8.ittraining.loc kernel: SMBIOS 2.5 present.
Jun 03 09:01:10 centos8.ittraining.loc kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox
12/01/2006
```

```
Jun 03 09:01:10 centos8.ittraining.loc kernel: Hypervisor detected: KVM
Jun 03 09:01:10 centos8.ittraining.loc kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jun 03 09:01:10 centos8.ittraining.loc kernel: kvm-clock: cpu 0, msr 114801001, primary cpu clock
Jun 03 09:01:10 centos8.ittraining.loc kernel: kvm-clock: using sched offset of 5675771878 cycles
Jun 03 09:01:10 centos8.ittraining.loc kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles:
0x1cd42e4dffb, max_idle_ns: 881590591483 ns
Jun 03 09:01:10 centos8.ittraining.loc kernel: tsc: Detected 1190.400 MHz processor
Jun 03 09:01:10 centos8.ittraining.loc kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Jun 03 09:01:10 centos8.ittraining.loc kernel: last_pfn = 0x120000 max_arch_pfn = 0x400000000
Jun 03 09:01:10 centos8.ittraining.loc kernel: MTRR default type: uncachable
Jun 03 09:01:10 centos8.ittraining.loc kernel: MTRR variable ranges disabled:
Jun 03 09:01:10 centos8.ittraining.loc kernel: Disabled
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/PAT: MTRRs disabled, skipping PAT initialization too.
Jun 03 09:01:10 centos8.ittraining.loc kernel: CPU MTRRs all blank - virtualized system.
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/PAT: Configuration [0-7]: WB  WT  UC- UC  WB  WT  UC- UC
Jun 03 09:01:10 centos8.ittraining.loc kernel: last_pfn = 0xdfff0 max_arch_pfn = 0x400000000
Jun 03 09:01:10 centos8.ittraining.loc kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
Jun 03 09:01:10 centos8.ittraining.loc kernel: kexec: Reserving the low 1M of memory for crashkernel
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a01000, 0x114a01fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a02000, 0x114a02fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a03000, 0x114a03fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a04000, 0x114a04fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a05000, 0x114a05fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a06000, 0x114a06fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a07000, 0x114a07fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a08000, 0x114a08fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: BRK [0x114a09000, 0x114a09fff] PGTABLE
Jun 03 09:01:10 centos8.ittraining.loc kernel: RAMDISK: [mem 0x34e00000-0x366f7fff]
Jun 03 09:01:10 centos8.ittraining.loc kernel: ACPI: Early table checksum verification disabled
Jun 03 09:01:10 centos8.ittraining.loc kernel: ACPI: RSDP 0x00000000000E0000 000024 (v02 VBOX  )
Jun 03 09:01:10 centos8.ittraining.loc kernel: ACPI: XSDT 0x00000000DFFF0030 00003C (v01 VBOX   VBOXXSDT 00000001
ASL  00000061)
Jun 03 09:01:10 centos8.ittraining.loc kernel: ACPI: FACP 0x00000000DFFF00F0 0000F4 (v04 VBOX   VBOXFACP 00000001
```

```
ASL  00000061)
Jun 03 09:01:10 centos8.ittraining.loc kernel: ACPI: DSDT 0x00000000DFFF0480 002325 (v02 VBOX   VBOXBIOS 00000002
INTL 20190509)
Jun 03 09:01:10 centos8.ittraining.loc kernel: ACPI: FACS 0x00000000DFFF0200 000040
Jun 03 09:01:10 centos8.ittraining.loc kernel: ACPI: FACS 0x00000000DFFF0200 000040
Jun 03 09:01:10 centos8.ittraining.loc kernel: ACPI: APIC 0x00000000DFFF0240 00006C (v02 VBOX   VBOXAPIC 00000001
ASL  00000061)
lines 1-57
```

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.

5.2 - 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@centos8 ~]# journalctl /sbin/anacron
-- Logs begin at Thu 2021-06-03 09:01:10 EDT, end at Thu 2021-06-03 13:10:01 EDT. --
Jun 03 10:01:01 centos8.ittraining.loc anacron[2575]: Anacron started on 2021-06-03
Jun 03 10:01:01 centos8.ittraining.loc anacron[2575]: Will run job `cron.daily' in 15 min.
Jun 03 10:01:01 centos8.ittraining.loc anacron[2575]: Jobs will be executed sequentially
Jun 03 10:16:01 centos8.ittraining.loc anacron[2575]: Job `cron.daily' started
Jun 03 10:16:01 centos8.ittraining.loc anacron[2575]: Job `cron.daily' terminated
Jun 03 10:16:01 centos8.ittraining.loc anacron[2575]: Normal exit (1 job run)
```

Important : Rappelez-vous que sous RHEL/CentOS 8 le répertoire **/sbin** est un lien symbolique vers **/usr/sbin**.

5.3 - 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@centos8 ~]# journalctl -b | more
-- Logs begin at Thu 2021-06-03 09:01:10 EDT, end at Thu 2021-06-03 13:11:01 EDT. --
Jun 03 09:01:10 centos8.ittraining.loc kernel: Linux version 4.18.0-240.22.1.el8_3.x86_64
(mockbuild@kbuilder.bsys.centos.org) (gcc version
 8.3.1 20191121 (Red Hat 8.3.1-5) (GCC)) #1 SMP Thu Apr 8 19:01:30 UTC 2021
Jun 03 09:01:10 centos8.ittraining.loc kernel: Command line:
BOOT_IMAGE=(hd0,msdos1)/vmlinuz-4.18.0-240.22.1.el8_3.x86_64 root=UUID=4c0cc28
c-0d59-45be-bd73-d292b80be33c ro crashkernel=auto resume=UUID=c8bb3f47-d67f-4b21-b781-766899dc83d4 rhgb quiet
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
registers'
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Jun 03 09:01:10 centos8.ittraining.loc kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes,
using 'standard' format.
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-provided physical RAM map:
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Jun 03 09:01:10 centos8.ittraining.loc kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Jun 03 09:01:10 centos8.ittraining.loc kernel: NX (Execute Disable) protection: active
Jun 03 09:01:10 centos8.ittraining.loc kernel: SMBIOS 2.5 present.
Jun 03 09:01:10 centos8.ittraining.loc kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox
12/01/2006
```

```
Jun 03 09:01:10 centos8.ittraining.loc kernel: Hypervisor detected: KVM
Jun 03 09:01:10 centos8.ittraining.loc kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Jun 03 09:01:10 centos8.ittraining.loc kernel: kvm-clock: cpu 0, msr 114801001, primary cpu clock
Jun 03 09:01:10 centos8.ittraining.loc kernel: kvm-clock: using sched offset of 5675771878 cycles
Jun 03 09:01:10 centos8.ittraining.loc kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles:
0x1cd42e4dffb, max_idle_ns: 881
590591483 ns
Jun 03 09:01:10 centos8.ittraining.loc kernel: tsc: Detected 1190.400 MHz processor
Jun 03 09:01:10 centos8.ittraining.loc kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
--More--
```

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

5.4 - 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@centos8 ~]# journalctl -p warning
-- Logs begin at Thu 2021-06-03 09:01:10 EDT, end at Thu 2021-06-03 13:12:01 EDT. --
Jun 03 09:01:10 centos8.ittraining.loc kernel:  #2
Jun 03 09:01:10 centos8.ittraining.loc kernel:  #3
Jun 03 09:01:10 centos8.ittraining.loc kernel: acpi PNP0A03:00: fail to add MMCONFIG information, can't access
extended PCI configuration >
Jun 03 09:01:12 centos8.ittraining.loc kernel: e1000: E1000 MODULE IS NOT SUPPORTED
Jun 03 09:01:12 centos8.ittraining.loc kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log
message.
Jun 03 09:01:12 centos8.ittraining.loc kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log
message.
```

```
Jun 03 09:01:18 centos8.ittraining.loc kernel: printk: systemd: 19 output lines suppressed due to ratelimiting
Jun 03 09:01:20 centos8.ittraining.loc firewalld[874]: WARNING: AllowZoneDrifting is enabled. This is considered
an insecure configuration>
Jun 03 09:01:21 centos8.ittraining.loc systemd[1]: iscsi.service: Unit cannot be reloaded because it is inactive.
Jun 03 09:01:24 centos8.ittraining.loc systemd[1]: iscsi.service: Unit cannot be reloaded because it is inactive.
Jun 03 09:01:24 centos8.ittraining.loc systemd[1]: iscsi.service: Unit cannot be reloaded because it is inactive.
Jun 03 09:01:26 centos8.ittraining.loc chronyd[850]: System clock wrong by 1.753498 seconds, adjustment started
Jun 03 09:01:28 centos8.ittraining.loc chronyd[850]: System clock was stepped by 1.753498 seconds
Jun 03 12:46:31 centos8.ittraining.loc chronyd[850]: System clock wrong by 47255.336542 seconds, adjustment
started
lines 1-15/15 (END)
```

Les priorités reconnues par Journald sont :

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

5.5 - 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@centos8 ~]# journalctl --since 12:00 --until now
-- Logs begin at Thu 2021-06-03 09:01:10 EDT, end at Thu 2021-06-03 13:14:01 EDT. --
Jun 03 12:00:01 centos8.ittraining.loc systemd[1]: Started Session 181 of user trainee.
Jun 03 12:00:01 centos8.ittraining.loc CROND[4238]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:00:01 centos8.ittraining.loc systemd[1]: session-181.scope: Succeeded.
```

```
Jun 03 12:01:01 centos8.ittraining.loc CROND[4251]: (root) CMD (run-parts /etc/cron.hourly)
Jun 03 12:01:01 centos8.ittraining.loc systemd[1]: Started Session 182 of user trainee.
Jun 03 12:01:01 centos8.ittraining.loc run-parts[4255]: (/etc/cron.hourly) starting 0anacron
Jun 03 12:01:01 centos8.ittraining.loc CROND[4260]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:01:01 centos8.ittraining.loc run-parts[4262]: (/etc/cron.hourly) finished 0anacron
Jun 03 12:01:01 centos8.ittraining.loc systemd[1]: session-182.scope: Succeeded.
Jun 03 12:02:01 centos8.ittraining.loc systemd[1]: Started Session 183 of user trainee.
Jun 03 12:02:01 centos8.ittraining.loc CROND[4275]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:02:01 centos8.ittraining.loc systemd[1]: session-183.scope: Succeeded.
Jun 03 12:03:01 centos8.ittraining.loc systemd[1]: Started Session 184 of user trainee.
Jun 03 12:03:01 centos8.ittraining.loc CROND[4289]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:03:01 centos8.ittraining.loc systemd[1]: session-184.scope: Succeeded.
Jun 03 12:04:01 centos8.ittraining.loc systemd[1]: Started Session 185 of user trainee.
Jun 03 12:04:01 centos8.ittraining.loc CROND[4303]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:04:01 centos8.ittraining.loc systemd[1]: session-185.scope: Succeeded.
Jun 03 12:05:01 centos8.ittraining.loc systemd[1]: Started Session 186 of user trainee.
Jun 03 12:05:01 centos8.ittraining.loc CROND[4319]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:05:01 centos8.ittraining.loc systemd[1]: session-186.scope: Succeeded.
Jun 03 12:06:02 centos8.ittraining.loc systemd[1]: Started Session 187 of user trainee.
Jun 03 12:06:02 centos8.ittraining.loc CROND[4332]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:06:02 centos8.ittraining.loc systemd[1]: session-187.scope: Succeeded.
Jun 03 12:07:01 centos8.ittraining.loc systemd[1]: Started Session 188 of user trainee.
Jun 03 12:07:01 centos8.ittraining.loc CROND[4346]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:07:01 centos8.ittraining.loc systemd[1]: session-188.scope: Succeeded.
Jun 03 12:08:01 centos8.ittraining.loc systemd[1]: Started Session 189 of user trainee.
Jun 03 12:08:01 centos8.ittraining.loc CROND[4360]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 12:08:01 centos8.ittraining.loc systemd[1]: session-189.scope: Succeeded.
lines 1-31
```

Important : Il est possible d'utiliser des mots clefs : **yesterday**, **today**, **tomorrow**, **now**.

5.6 - Consultation des Journaux en Live

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

```
[root@centos8 ~]# journalctl -f
-- Logs begin at Thu 2021-06-03 09:01:10 EDT. --
Jun 03 13:13:08 centos8.ittraining.loc systemd[1]: Started dnf makecache.
Jun 03 13:14:01 centos8.ittraining.loc systemd[1]: Started Session 256 of user trainee.
Jun 03 13:14:01 centos8.ittraining.loc CROND[5391]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 13:14:01 centos8.ittraining.loc systemd[1]: session-256.scope: Succeeded.
Jun 03 13:15:01 centos8.ittraining.loc systemd[1]: Started Session 257 of user trainee.
Jun 03 13:15:01 centos8.ittraining.loc CROND[5407]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 13:15:01 centos8.ittraining.loc systemd[1]: session-257.scope: Succeeded.
Jun 03 13:16:02 centos8.ittraining.loc systemd[1]: Started Session 258 of user trainee.
Jun 03 13:16:02 centos8.ittraining.loc CROND[5420]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 13:16:02 centos8.ittraining.loc systemd[1]: session-258.scope: Succeeded.
^C
```

Ouvrez un deuxième terminal et saisissez la commande suivante :

```
[trainee@centos8 ~]$ logger -p user.info Linux est super
```

Retournez consulter le premier terminal :

```
[root@centos8 ~]# journalctl -f
-- Logs begin at Thu 2021-06-03 09:01:10 EDT. --
Jun 03 13:13:08 centos8.ittraining.loc systemd[1]: Started dnf makecache.
Jun 03 13:14:01 centos8.ittraining.loc systemd[1]: Started Session 256 of user trainee.
Jun 03 13:14:01 centos8.ittraining.loc CROND[5391]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 13:14:01 centos8.ittraining.loc systemd[1]: session-256.scope: Succeeded.
Jun 03 13:15:01 centos8.ittraining.loc systemd[1]: Started Session 257 of user trainee.
Jun 03 13:15:01 centos8.ittraining.loc CROND[5407]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 13:15:01 centos8.ittraining.loc systemd[1]: session-257.scope: Succeeded.
```

```
Jun 03 13:16:02 centos8.ittraining.loc systemd[1]: Started Session 258 of user trainee.
Jun 03 13:16:02 centos8.ittraining.loc CROND[5420]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 13:16:02 centos8.ittraining.loc systemd[1]: session-258.scope: Succeeded.
Jun 03 13:17:01 centos8.ittraining.loc systemd[1]: Started Session 259 of user trainee.
Jun 03 13:17:01 centos8.ittraining.loc CROND[5436]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 13:17:01 centos8.ittraining.loc systemd[1]: session-259.scope: Succeeded.
Jun 03 13:17:19 centos8.ittraining.loc sshd[5439]: Accepted password for trainee from 10.0.2.2 port 39906 ssh2
Jun 03 13:17:19 centos8.ittraining.loc systemd-logind[880]: New session 260 of user trainee.
Jun 03 13:17:19 centos8.ittraining.loc systemd[1]: Started Session 260 of user trainee.
Jun 03 13:17:19 centos8.ittraining.loc sshd[5439]: pam_unix(sshd:session): session opened for user trainee by
(uid=0)
Jun 03 13:17:34 centos8.ittraining.loc trainee[5470]: Linux est super
Jun 03 13:17:34 centos8.ittraining.loc rsyslogd[1113]: imjournal: journal files changed, reloading...
[v8.1911.0-6.el8 try https://www.rsyslog.com/e/0 ]
Jun 03 13:18:01 centos8.ittraining.loc systemd[1]: Started Session 261 of user trainee.
Jun 03 13:18:01 centos8.ittraining.loc CROND[5481]: (trainee) CMD (/bin/pwd > pwd.txt)
Jun 03 13:18:01 centos8.ittraining.loc systemd[1]: session-261.scope: Succeeded.
^C
```

Important : Notez la présence de la ligne **Jun 03 13:17:34 centos8.ittraining.loc trainee[5470]: Linux est super**.

5.7 - Consultation des Journaux avec des Mots Clefs

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

```
[root@centos8 ~]# journalctl [tab] [tab]
_AUDIT_LOGINUID=              _HOSTNAME=                    NM_DEVICE=                    _SYSTEMD_SESSION=
_AUDIT_SESSION=               INITRD_USEC=                  NM_LOG_DOMAINS=               _SYSTEMD_SLICE=
AVAILABLE=                    INVOCATION_ID=                NM_LOG_LEVEL=                 _SYSTEMD_UNIT=
```

```
AVAILABLE_PRETTY=          JOB_ID=                    N_RESTARTS=                _SYSTEMD_USER_SLICE=
_BOOT_ID=                  JOB_RESULT=                _PID=                      _SYSTEMD_USER_UNIT=
_CAP_EFFECTIVE=            JOB_TYPE=                  PRIORITY=                  TIMESTAMP_BOOTTIME=
_CMDLINE=                  JOURNAL_NAME=              SEAT_ID=                   TIMESTAMP_MONOTONIC=
CODE_FILE=                 JOURNAL_PATH=              _SELINUX_CONTEXT=          _TRANSPORT=
CODE_FUNC=                 _KERNEL_DEVICE=            SESSION_ID=                _UDEV_DEVNODE=
CODE_LINE=                 _KERNEL_SUBSYSTEM=         _SOURCE_MONOTONIC_TIMESTAMP= _UDEV_SYSNAME=
_COMM=                     KERNEL_USEC=               _SOURCE_REALTIME_TIMESTAMP= _UID=
CURRENT_USE=               LEADER=                    SSSD_DOMAIN=               UNIT=
CURRENT_USE_PRETTY=        LIMIT=                     _STREAM_ID=                USER_ID=
DISK_AVAILABLE=            LIMIT_PRETTY=              SYSLOG_FACILITY=           USER_INVOCATION_ID=
DISK_AVAILABLE_PRETTY=     _MACHINE_ID=               SYSLOG_IDENTIFIER=         USERSPACE_USEC=
DISK_KEEP_FREE=            MAX_USE=                   SYSLOG_PID=                USER_UNIT=
DISK_KEEP_FREE_PRETTY=     MAX_USE_PRETTY=            _SYSTEMD_CGROUP=
_EXE=                      MESSAGE=                   _SYSTEMD_INVOCATION_ID=
_GID=                      MESSAGE_ID=                _SYSTEMD_OWNER_UID=
```

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@centos8 ~]# journalctl _UID=
0     1000  81    983   990   992   998
[root@centos8 ~]# journalctl _COMM=
anacron          dbus-daemon      kdumpctl         NetworkManager   smartd           sssd_nss         systemd-
hiberna
auditd           dnf              logger           polkitd          sm-notify        su               systemd-
journal
augenrules       dnsmasq          login            rngd             sshd             (systemd)        systemd-
logind
chronyd          dracut-cmdline   lvm              rsyslogd         sssd             systemd          systemd-
udevd
crond            firewalld        netcf-transacti  sh               sssd_be          systemd-fsck
```