Version : **2024.01**

Dernière mise-à-jour : 2024/03/08 08:41

LDF508 - Gestion de la Journalisation

Contenu du Module

- **LDF508 - Gestion de la Journalisation**
  - Contenu du Module
  - Présentation
  - La Commande dmesg
  - LAB #1 - Surveillance Sécuritaire
    - 1.1 - La Commande last
    - 1.2 - La Commande lastlog
    - 1.3 - La Commande lastb
    - 1.4 - Le fichier /var/log/auth.log
    - 1.5 - Gestion des évènements audit
      - Le fichier /var/log/audit/audit.log
      - auditd
      - auditctl
      - audispd
      - La consultation des événements audit
        - La Commande aureport
        - La Commande ausearch
  - Le fichier /var/log/messages
  - Applications
  - LAB #2 - rsyslog
    - 2.1 - Priorités
    - 2.2 - Sous-systèmes applicatifs
    - 2.3 - /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
- LAB #3 - La Commande logger
- LAB #4 - La Commande logrotate
- LAB #5 - La Journalisation avec journald
  - 5.1 - Consultation des Journaux
  - 5.2 - Consultation des Journaux d'une Application Spécifique
  - 5.3 - Consultation des Journaux depuis le Dernier Démarrage
  - 5.4 - Consultation des Journaux d'une Priorité Spécifique
  - 5.5 - Consultation des Journaux d'une Plage de Dates ou d'Heures
  - 5.6 - Consultation des Journaux en Live

Présentation

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

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

La Commande dmesg

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

```
root@debian11:~# dmesg | more
[    0.000000] Linux version 5.10.0-13-amd64 (debian-kernel@lists.debian.org) (gcc-10 (Debian 10.2.1-6) 10.2.1
20210110, GNU ld (GNU Binutils for Debian) 2
.35.2) #1 SMP Debian 5.10.106-1 (2022-03-17)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.10.0-13-amd64 root=UUID=9887a74f-a680-4bde-8f04-
db5ae9ea186e ro quiet
[    0.000000] x86/fpu: x87 FPU will use FXSAVE
[    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 0x0000000000100000-0x00000000bffd9fff] usable
[    0.000000] BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000100000000-0x000000013fffffff] usable
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] SMBIOS 2.8 present.
[    0.000000] DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org
04/01/2014
[    0.000000] Hypervisor detected: KVM
[    0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[    0.000000] kvm-clock: cpu 0, msr 5ccb8001, primary cpu clock
[    0.000000] kvm-clock: using sched offset of 10164710878 cycles
[    0.000006] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns:
881590591483 ns
[    0.000013] tsc: Detected 2399.982 MHz processor
[    0.000754] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```

```
[    0.000757] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.000761] last_pfn = 0x140000 max_arch_pfn = 0x400000000
[    0.000789] MTRR default type: write-back
[    0.000791] MTRR fixed ranges enabled:
[    0.000792]   00000-9FFFF write-back
[    0.000793]   A0000-BFFFF uncachable
[    0.000794]   C0000-FFFFF write-protect
[    0.000795] MTRR variable ranges enabled:
[    0.000796]   0 base 00C0000000 mask FFC0000000 uncachable
[    0.000797]   1 disabled
[    0.000797]   2 disabled
[    0.000798]   3 disabled
[    0.000798]   4 disabled
[    0.000799]   5 disabled
[    0.000799]   6 disabled
[    0.000800]   7 disabled
[    0.000815] x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WC  UC- UC
[    0.000826] last_pfn = 0xbffda max_arch_pfn = 0x400000000
[    0.009867] found SMP MP-table at [mem 0x000f5a80-0x000f5a8f]
[    0.010459] RAMDISK: [mem 0x3304d000-0x3581dfff]
[    0.010467] ACPI: Early table checksum verification disabled
[    0.010479] ACPI: RSDP 0x00000000000F5880 000014 (v00 BOCHS )
[    0.010487] ACPI: RSDT 0x00000000BFFE145E 000038 (v01 BOCHS  BXPCRSDT 00000001 BXPC 00000001)
[    0.010497] ACPI: FACP 0x00000000BFFE1240 000074 (v01 BOCHS  BXPCFACP 00000001 BXPC 00000001)
--More--
[q]
```

Les option de cette commande sont :

```
root@debian11:~# 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
     --noescape              don't escape unprintable character
 -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
 -W, --follow-new            wait and print only 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@debian11:~# last
```

```
trainee  pts/0        10.0.2.1         Fri Apr 29 14:17   still logged in
trainee  pts/0        10.0.2.1         Thu Apr 28 05:24 - 16:47  (11:22)
trainee  pts/0        10.0.2.1         Wed Apr 27 10:38 - 17:09  (06:31)
trainee  pts/0        10.0.2.1         Tue Apr 26 13:24 - 19:44  (06:20)
reboot   system boot  5.10.0-13-amd64  Tue Apr 26 13:08   still running
trainee  pts/0        10.0.2.1         Mon Apr 25 13:36 - 17:18  (03:41)
reboot   system boot  5.10.0-13-amd64  Mon Apr 25 07:08   still running
trainee  pts/1        10.0.2.1         Mon Apr 25 07:05 - 07:05  (00:00)
trainee  tty7         :0               Mon Apr 25 07:03 - crash  (00:05)
reboot   system boot  5.10.0-13-amd64  Mon Apr 25 07:01   still running

wtmp begins Mon Apr 25 07:01:57 2022
```

Les option de cette commande sont :

```
root@debian11:~# 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@debian11:~# lastlog
Username         Port     From             Latest
root                                       **Never logged in**
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
```

```
nobody                                           **Never logged in**
_apt                                             **Never logged in**
systemd-network                                  **Never logged in**
systemd-resolve                                  **Never logged in**
messagebus                                       **Never logged in**
systemd-timesync                                 **Never logged in**
usbmux                                           **Never logged in**
rtkit                                            **Never logged in**
dnsmasq                                          **Never logged in**
avahi                                            **Never logged in**
speech-dispatcher                                 **Never logged in**
pulse                                            **Never logged in**
saned                                            **Never logged in**
colord                                           **Never logged in**
lightdm                                          **Never logged in**
trainee          pts/0    10.0.2.1               Fri Apr 29 14:17:31 +0200 2022
systemd-coredump                                 **Never logged in**
sshd                                             **Never logged in**
```

Les option de cette commande sont :

```
root@debian11:~# 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 infructueueses des utilisateurs à partir du contenu du fichier **/var/log/btmp** :

```
root@debian11:~# lastb
trainee  ssh:notty    10.0.2.1         Fri Apr 29 14:22 - 14:22  (00:00)
trainee  ssh:notty    10.0.2.1         Fri Apr 29 14:22 - 14:22  (00:00)
trainee  ssh:notty    10.0.2.1         Fri Apr 29 14:22 - 14:22  (00:00)
trainee  ssh:notty    10.0.2.1         Fri Apr 29 14:22 - 14:22  (00:00)
trainee  ssh:notty    10.0.2.1         Fri Apr 29 14:22 - 14:22  (00:00)
trainee  ssh:notty    10.0.2.1         Fri Apr 29 14:22 - 14:22  (00:00)

btmp begins Fri Apr 29 14:22:11 2022
```

Les options de cette commande sont :

```
root@debian11:~# 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/auth.log

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

```
root@debian11:~# tail -n 15 /var/log/auth.log
Apr 29 14:22:22 debian11 sshd[45387]: Failed password for trainee from 10.0.2.1 port 55278 ssh2
Apr 29 14:22:23 debian11 sshd[45387]: Connection closed by authenticating user trainee 10.0.2.1 port 55278
[preauth]
Apr 29 14:22:23 debian11 sshd[45387]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=10.0.2.1  user=trainee
Apr 29 14:22:29 debian11 sshd[45391]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=10.0.2.1  user=trainee
Apr 29 14:22:31 debian11 sshd[45391]: Failed password for trainee from 10.0.2.1 port 55296 ssh2
Apr 29 14:22:35 debian11 sshd[45391]: Failed password for trainee from 10.0.2.1 port 55296 ssh2
Apr 29 14:22:40 debian11 sshd[45391]: Failed password for trainee from 10.0.2.1 port 55296 ssh2
Apr 29 14:22:41 debian11 sshd[45391]: Connection closed by authenticating user trainee 10.0.2.1 port 55296
[preauth]
Apr 29 14:22:41 debian11 sshd[45391]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=10.0.2.1  user=trainee
Apr 29 14:22:46 debian11 sshd[45393]: Accepted password for trainee from 10.0.2.1 port 55306 ssh2
Apr 29 14:22:46 debian11 sshd[45393]: pam_unix(sshd:session): session opened for user trainee(uid=1000) by
```

```
(uid=0)
Apr 29 14:22:46 debian11 systemd-logind[385]: New session 142 of user trainee.
Apr 29 14:22:46 debian11 systemd: pam_unix(systemd-user:session): session opened for user trainee(uid=1000) by
(uid=0)
Apr 29 14:22:52 debian11 su: (to root) trainee on pts/0
Apr 29 14:22:52 debian11 su: pam_unix(su-l:session): session opened for user root(uid=0) by trainee(uid=1000)
```

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 collectionne des informations telles :

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

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

```
root@debian11:~# apt-get -y install auditd
```

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

```
root@debian11:~# tail -n 15 /var/log/audit/audit.log
type=DAEMON_START msg=audit(1651235065.372:1869): op=start ver=3.0 format=enriched kernel=5.10.0-13-amd64
auid=4294967295 pid=45572 uid=0 ses=4294967295 subj=unconfined  res=successAUID="unset" UID="root"
type=CONFIG_CHANGE msg=audit(1651235065.384:26): op=set audit_backlog_limit=8192 old=64 auid=4294967295
ses=4294967295 subj==unconfined res=1AUID="unset"
type=CONFIG_CHANGE msg=audit(1651235065.384:27): op=set audit_failure=1 old=1 auid=4294967295 ses=4294967295
subj==unconfined res=1AUID="unset"
type=CONFIG_CHANGE msg=audit(1651235065.384:28): op=set audit_backlog_wait_time=60000 old=15000 auid=4294967295
ses=4294967295 subj==unconfined res=1AUID="unset"
```

```
type=SERVICE_START msg=audit(1651235065.388:29): pid=1 uid=0 auid=4294967295 ses=4294967295 subj==unconfined
msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?
res=success'UID="root" AUID="unset"
```

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@debian11:~# 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 = adm
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@debian11:~# 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 contenues dans le fichier **/etc/audit/audit.rules** :

```
root@debian11:~# 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@debian11:~# auditctl -h
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
    --signal <signal>                  Send the specified signal to the daemon    -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
    --reset_backlog_wait_time_actual   Reset the actual backlog wait time counter
```

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/audit/plugins.d** :

```
root@debian11:~# ls /etc/audit/plugins.d
af_unix.conf  syslog.conf
```

Le contenu de ces fichiers suit un format précis :

```
root@debian11:~# cat /etc/audit/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, LOG_AUTH,
# LOG_AUTHPRIV, LOG_DAEMON, LOG_SYSLOG, and LOG_USER.
```

```
active = no
direction = out
path = /sbin/audisp-syslog
type = always
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@debian11:~# aureport

Summary Report
======================
Range of time in logs: 04/29/2022 14:24:25.372 - 04/29/2022 14:24:25.388
Selected time for report: 04/29/2022 14:24:25 - 04/29/2022 14:24:25.388
Number of changes in configuration: 3
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 1
Number of terminals: 1
Number of host names: 1
Number of executables: 1
```

```
Number of commands: 1
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 2
Number of events: 5
```

Les options de cette commande sont :

```
root@debian11:~# 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@debian11:~# exit
logout
trainee@debian11:~$ su -
Password: fenestros
root@debian11:~# ausearch -ui 1000 | more
----
time->Fri Apr 29 14:31:05 2022
```

```
type=USER_END msg=audit(1651235465.623:36): pid=45426 uid=1000 auid=1000 ses=142 subj==unconfined
msg='op=PAM:session_close grantors=pam_keyinit,pam_env,pa
m_env,pam_mail,pam_limits,pam_permit,pam_unix,pam_systemd,pam_ecryptfs acct="root" exe="/usr/bin/su"
hostname=debian11 addr=? terminal=pts/0 res=success'
----
time->Fri Apr 29 14:31:05 2022
type=CRED_DISP msg=audit(1651235465.623:37): pid=45426 uid=1000 auid=1000 ses=142 subj==unconfined
msg='op=PAM:setcred grantors=pam_permit,pam_ecryptfs acc
t="root" exe="/usr/bin/su" hostname=debian11 addr=? terminal=pts/0 res=success'
----
time->Fri Apr 29 14:31:11 2022
type=USER_AUTH msg=audit(1651235471.067:38): pid=45693 uid=1000 auid=1000 ses=142 subj==unconfined
msg='op=PAM:authentication grantors=pam_permit,pam_ecryp
tfs acct="root" exe="/usr/bin/su" hostname=debian11 addr=? terminal=pts/0 res=success'
----
time->Fri Apr 29 14:31:11 2022
type=USER_ACCT msg=audit(1651235471.067:39): pid=45693 uid=1000 auid=1000 ses=142 subj==unconfined
msg='op=PAM:accounting grantors=pam_permit acct="root" e
xe="/usr/bin/su" hostname=debian11 addr=? terminal=pts/0 res=success'
----
time->Fri Apr 29 14:31:11 2022
type=CRED_ACQ msg=audit(1651235471.067:40): pid=45693 uid=1000 auid=1000 ses=142 subj==unconfined
msg='op=PAM:setcred grantors=pam_permit,pam_ecryptfs acct
="root" exe="/usr/bin/su" hostname=debian11 addr=? terminal=pts/0 res=success'
----
time->Fri Apr 29 14:31:11 2022
type=USER_START msg=audit(1651235471.071:41): pid=45693 uid=1000 auid=1000 ses=142 subj==unconfined
msg='op=PAM:session_open grantors=pam_keyinit,pam_env,p
am_env,pam_mail,pam_limits,pam_permit,pam_unix,pam_systemd,pam_ecryptfs acct="root" exe="/usr/bin/su"
hostname=debian11 addr=? terminal=pts/0 res=success'
```

Les options de cette commande sont :

```
root@debian11:~# 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 date & 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@debian11:~# tail -n 15 /var/log/messages
Apr 28 06:43:12 debian11 kernel: [149698.386556] Adding 262140k swap on /swap.  Priority:-3 extents:4
across:286716k FS
Apr 28 06:43:47 debian11 kernel: [149733.302599] Adding 998396k swap on /dev/sda5.  Priority:-2 extents:1
across:998396k FS
Apr 28 06:44:00 debian11 kernel: [149746.478556] Adding 262140k swap on /swap.  Priority:-3 extents:4
```

```
across:286716k FS
Apr 28 16:47:22 debian11 pipewire-media-session[34487]: error id:0 seq:158 res:-32 (Broken pipe): connection
error
Apr 29 00:00:03 debian11 kernel: [211909.512230] audit: type=1400 audit(1651183203.717:23): apparmor="DENIED"
operation="capable" profile="/usr/sbin/cupsd" pid=44753 comm="cupsd" capability=12  capname="net_admin"
Apr 29 00:00:03 debian11 kernel: [211909.537867] audit: type=1400 audit(1651183203.741:24): apparmor="DENIED"
operation="capable" profile="/usr/sbin/cups-browsed" pid=44754 comm="cups-browsed" capability=23
capname="sys_nice"
Apr 29 14:17:31 debian11 pipewire[45354]: could not set nice-level to -11: Permission denied
Apr 29 14:17:31 debian11 pipewire[45354]: could not make thread realtime: Permission denied
Apr 29 14:17:31 debian11 pipewire-media-session[45364]: could not set nice-level to -11: Permission denied
Apr 29 14:17:31 debian11 pipewire-media-session[45364]: could not make thread realtime: Permission denied
Apr 29 14:22:13 debian11 pipewire-media-session[45364]: error id:0 seq:158 res:-32 (Broken pipe): connection
error
Apr 29 14:22:47 debian11 pipewire[45411]: could not set nice-level to -11: Permission denied
Apr 29 14:22:47 debian11 pipewire[45411]: could not make thread realtime: Permission denied
Apr 29 14:22:47 debian11 pipewire-media-session[45423]: could not set nice-level to -11: Permission denied
Apr 29 14:22:47 debian11 pipewire-media-session[45423]: could not make thread realtime: Permission denied
```

Applications

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

- cups,
- samba,
- ...

```
root@debian11:~# ls -l /var/log
total 1884
-rw-r--r--  1 root              root             46300 Apr 25 17:08 alternatives.log
drwxr-xr-x  2 root              root              4096 Apr 29 14:24 apt
drwxr-x---  2 root              adm               4096 Apr 29 14:24 audit
```

```
-rw-r-----  1 root              adm              50109 Apr 29 14:31 auth.log
-rw-------  1 root              root                 0 Apr 27 00:00 boot.log
-rw-------  1 root              root             15065 Apr 27 00:00 boot.log.1
-rw-rw----  1 root              utmp              2304 Apr 29 14:22 btmp
drwxr-xr-x  2 root              root              4096 Apr 29 00:00 cups
-rw-r-----  1 root              adm             175380 Apr 29 14:24 daemon.log
-rw-r-----  1 root              adm              23560 Apr 29 14:22 debug
-rw-r--r--  1 root              root            666074 Apr 29 14:24 dpkg.log
-rw-r--r--  1 root              root             32032 Apr 25 07:04 faillog
-rw-r--r--  1 root              root              4939 Apr 25 06:54 fontconfig.log
drwxr-xr-x  3 root              root              4096 Apr 28 06:00 installer
drwxr-sr-x+ 3 root              systemd-journal   4096 Apr 25 07:01 journal
-rw-r-----  1 root              adm             186224 Apr 29 00:00 kern.log
-rw-rw-r--  1 root              utmp            292292 Apr 29 14:22 lastlog
drwx--x--x  2 root              root              4096 Apr 26 13:08 lightdm
-rw-r-----  1 root              adm             181928 Apr 29 14:22 messages
drwx------  2 root              root              4096 Apr 25 07:01 private
drwxr-xr-x  3 root              root              4096 Apr 25 07:04 runit
drwx------  2 speech-dispatcher root              4096 Sep 19  2021 speech-dispatcher
-rw-r-----  1 root              adm             411969 Apr 29 14:30 syslog
-rw-r-----  1 root              adm              10969 Apr 29 14:22 user.log
-rw-rw-r--  1 root              utmp             10368 Apr 29 14:22 wtmp
-rw-r--r--  1 root              root             21631 Apr 26 13:08 Xorg.0.log
-rw-r--r--  1 root              root             21631 Apr 25 07:08 Xorg.0.log.old
```

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**).

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
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@debian11:~# cat /etc/rsyslog.conf
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html


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

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability
```

```
# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")



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

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

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

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

#
```

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



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

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

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

#
# Some "catch-all" log files.
#
*.=debug;\
        auth,authpriv.none;\
```

```
        mail.none               -/var/log/debug
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail.none               -/var/log/messages

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

Ce fichier est divisé en 3 parties :

- **MODULES**,
  - Section traitant le chargement des modules offrant des fonctionnalités étendues à rsyslog,
- **GLOBAL DIRECTIVES**,
  - Section traitant les options de comportement global du service rsyslog,
- **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”)	Active la trace des messages locaux, per exemple de la commande **logger**
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”)** et *module(load=“imklog”) **sont activés : <file> …** * #### MODULES ####

module(load=“imuxsock”) # provides support for local system logging module(load=“imklog”) # provides kernel logging support #module(load=“immark”) # provides –MARK– message capability

provides UDP syslog reception #module(load=“imudp”) #input(type=“imudp” port=“514”)

provides TCP syslog reception #module(load=“imtcp”) #input(type=“imtcp” port=“514”) … </file>

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

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

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
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 port utilisé en modifiant la valeur dans la directive , par exemple : **input(type=“imtcp” port=“1514”)**.

Pour envoyer l'ensemble des traces de journalisation vers un serveur rsyslog distant, il convient d'ajouter la section suivante à la fin du fichier.

```
...
# ### 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 # Pour utiliser le protocol UDP au cas où le protocol TCP n'est pas disponible sur le
serveur distant
*.* @@remote-host:514 # Pour utiliser le protocol TCP
# ### end of the forwarding rule ###
```

Important : La valeur de **remote-host** doit être modifiée pour indiquer l'adresse IP du serveur rsyslog distant.

Directives Globales

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

```
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
```

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

Règles

Chaque règle prend la forme suivante :

```
Sélecteur[; ...]  [-] Action
```

Un Sélecteur est défini d'une des façons suivantes :

Sous-système applicatif.Priorité

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

Sous-système applicatif!Priorité

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

Sous-système applicatif=Priorité

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

L'utilisation du caractère spécial *

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

n Sous-systèmes avec la même priorité

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

n Sélecteurs avec la même Action

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

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

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@debian11:~# logger -p user.info Linux est super
```

Consultez la fin de votre syslog :

```
root@debian11:~# tail /var/log/messages
Apr 29 14:17:31 debian11 pipewire[45354]: could not set nice-level to -11: Permission denied
Apr 29 14:17:31 debian11 pipewire[45354]: could not make thread realtime: Permission denied
Apr 29 14:17:31 debian11 pipewire-media-session[45364]: could not set nice-level to -11: Permission denied
Apr 29 14:17:31 debian11 pipewire-media-session[45364]: could not make thread realtime: Permission denied
Apr 29 14:22:13 debian11 pipewire-media-session[45364]: error id:0 seq:158 res:-32 (Broken pipe): connection
error
Apr 29 14:22:47 debian11 pipewire[45411]: could not set nice-level to -11: Permission denied
Apr 29 14:22:47 debian11 pipewire[45411]: could not make thread realtime: Permission denied
Apr 29 14:22:47 debian11 pipewire-media-session[45423]: could not set nice-level to -11: Permission denied
Apr 29 14:22:47 debian11 pipewire-media-session[45423]: could not make thread realtime: Permission denied
Apr 29 15:06:18 debian11 trainee: Linux est super
```

Les options de la commande logger sont :

```
root@debian11:~# 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@debian11:~# cat /etc/logrotate.conf
# see "man logrotate" for details
```

```
# global options do not affect preceding include directives

# 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

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

# system-specific logs may 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 :

```
root@debian11:~# ls -l /etc/logrotate.d/
total 44
```

```
-rw-r--r-- 1 root root 120 Jan 30  2021 alternatives
-rw-r--r-- 1 root root 173 Jun 10  2021 apt
-rw-r--r-- 1 root root  91 Mar  2  2021 bootlog
-rw-r--r-- 1 root root 130 Oct 14  2019 btmp
-rw-r--r-- 1 root root 181 May 27  2021 cups-daemon
-rw-r--r-- 1 root root 112 Jan 30  2021 dpkg
-rw-r--r-- 1 root root  94 Jan  7  2021 ppp
-rw-r--r-- 1 root root 374 Feb 17  2021 rsyslog
-rw-r--r-- 1 root root 132 Sep 10  2020 sane-utils
-rw-r--r-- 1 root root 677 Sep 15  2021 speech-dispatcher
-rw-r--r-- 1 root root 145 Oct 14  2019 wtmp
```

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

Les options de la commande logrotate sont :

```
root@debian11:~# 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 `/usr/bin/mail')
  -s, --state=statefile     Path of state file
      --skip-state-lock     Do not lock the 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 Debian 11, 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 **/var/log/journal** :

```
root@debian11:~# ls -lR /var/log/journal/
/var/log/journal/:
total 4
drwxr-sr-x+ 2 root systemd-journal 4096 Apr 25 13:36 6f7e96ef32a74c788166a0f3ad41a5c0

/var/log/journal/6f7e96ef32a74c788166a0f3ad41a5c0:
total 32780
-rw-r-----+ 1 root systemd-journal 8388608 Apr 25 07:08 system@0005dd7392809037-23351ec76c7140d3.journal~
-rw-r-----+ 1 root systemd-journal 8388608 Apr 29 15:11 system.journal
-rw-r-----+ 1 root systemd-journal 8388608 Apr 25 13:36 user-1000@0005dd78fd663470-0c9ed794ecc61aa8.journal~
-rw-r-----+ 1 root systemd-journal 8388608 Apr 29 14:35 user-1000.journal
```

Journald ne peut pas envoyer les traces à un autre ordinateur. Pour utiliser un serveur de journalisation distant il faut donc décommenter 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@debian11:~# 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=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
#LineMax=48K
#ReadKMsg=yes
#Audit=no
```

5.1 - Consultation des Journaux

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

```
root@debian11:~# journalctl
-- Journal begins at Mon 2022-04-25 07:01:58 CEST, ends at Fri 2022-04-29 15:06:18 CEST. --
Apr 25 07:01:58 debian11 kernel: Linux version 5.10.0-13-amd64 (debian-kernel@lists.debian.org) (gcc-10 (Debian
10.2.1-6) 10.2.1 20210110, GNU ld (GNU Bin>
Apr 25 07:01:58 debian11 kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.10.0-13-amd64 root=UUID=9887a74f-
a680-4bde-8f04-db5ae9ea186e ro quiet
Apr 25 07:01:58 debian11 kernel: x86/fpu: x87 FPU will use FXSAVE
Apr 25 07:01:58 debian11 kernel: BIOS-provided physical RAM map:
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x0000000100000000-0x000000013fffffff] usable
Apr 25 07:01:58 debian11 kernel: NX (Execute Disable) protection: active
Apr 25 07:01:58 debian11 kernel: SMBIOS 2.8 present.
Apr 25 07:01:58 debian11 kernel: DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-
prebuilt.qemu.org 04/01/2014
Apr 25 07:01:58 debian11 kernel: Hypervisor detected: KVM
Apr 25 07:01:58 debian11 kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Apr 25 07:01:58 debian11 kernel: kvm-clock: cpu 0, msr 86ab8001, primary cpu clock
Apr 25 07:01:58 debian11 kernel: kvm-clock: using sched offset of 2324543470279 cycles
Apr 25 07:01:58 debian11 kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb,
max_idle_ns: 881590591483 ns
Apr 25 07:01:58 debian11 kernel: tsc: Detected 2399.982 MHz processor
Apr 25 07:01:58 debian11 kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Apr 25 07:01:58 debian11 kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
```

```
Apr 25 07:01:58 debian11 kernel: last_pfn = 0x140000 max_arch_pfn = 0x400000000
Apr 25 07:01:58 debian11 kernel: MTRR default type: write-back
Apr 25 07:01:58 debian11 kernel: MTRR fixed ranges enabled:
Apr 25 07:01:58 debian11 kernel:   00000-9FFFF write-back
Apr 25 07:01:58 debian11 kernel:   A0000-BFFFF uncachable
Apr 25 07:01:58 debian11 kernel:   C0000-FFFFF write-protect
Apr 25 07:01:58 debian11 kernel: MTRR variable ranges enabled:
Apr 25 07:01:58 debian11 kernel:   0 base 00C0000000 mask FFC0000000 uncachable
Apr 25 07:01:58 debian11 kernel:   1 disabled
Apr 25 07:01:58 debian11 kernel:   2 disabled
Apr 25 07:01:58 debian11 kernel:   3 disabled
Apr 25 07:01:58 debian11 kernel:   4 disabled
Apr 25 07:01:58 debian11 kernel:   5 disabled
Apr 25 07:01:58 debian11 kernel:   6 disabled
Apr 25 07:01:58 debian11 kernel:   7 disabled
Apr 25 07:01:58 debian11 kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WC  UC- UC
Apr 25 07:01:58 debian11 kernel: last_pfn = 0xbffda max_arch_pfn = 0x400000000
Apr 25 07:01:58 debian11 kernel: found SMP MP-table at [mem 0x000f5a80-0x000f5a8f]
Apr 25 07:01:58 debian11 kernel: RAMDISK: [mem 0x3304d000-0x3581dfff]
Apr 25 07:01:58 debian11 kernel: ACPI: Early table checksum verification disabled
Apr 25 07:01:58 debian11 kernel: ACPI: RSDP 0x00000000000F5880 000014 (v00 BOCHS )
Apr 25 07:01:58 debian11 kernel: ACPI: RSDT 0x00000000BFFE145E 000038 (v01 BOCHS  BXPCRSDT 00000001 BXPC
00000001)
Apr 25 07:01:58 debian11 kernel: ACPI: FACP 0x00000000BFFE1240 000074 (v01 BOCHS  BXPCFACP 00000001 BXPC
00000001)
lines 1-47
[q]
```

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@debian11:~# journalctl /usr/sbin/anacron
-- Journal begins at Mon 2022-04-25 07:01:58 CEST, ends at Fri 2022-04-29 15:06:18 CEST. --
Apr 25 07:02:04 debian11 anacron[355]: Anacron 2.3 started on 2022-04-25
Apr 25 07:02:04 debian11 anacron[355]: Will run job `cron.daily' in 5 min.
Apr 25 07:02:04 debian11 anacron[355]: Will run job `cron.weekly' in 10 min.
Apr 25 07:02:04 debian11 anacron[355]: Will run job `cron.monthly' in 15 min.
Apr 25 07:02:04 debian11 anacron[355]: Jobs will be executed sequentially
-- Boot 7fdaa15ef0664ecb99118b80b4db4cd9 --
Apr 25 07:08:53 debian11 anacron[361]: Anacron 2.3 started on 2022-04-25
Apr 25 07:08:53 debian11 anacron[361]: Will run job `cron.daily' in 5 min.
Apr 25 07:08:53 debian11 anacron[361]: Will run job `cron.weekly' in 10 min.
Apr 25 07:08:53 debian11 anacron[361]: Will run job `cron.monthly' in 15 min.
Apr 25 07:08:53 debian11 anacron[361]: Jobs will be executed sequentially
Apr 25 07:13:54 debian11 anacron[361]: Job `cron.daily' started
Apr 25 07:13:54 debian11 anacron[361]: Job `cron.daily' terminated
Apr 25 07:18:53 debian11 anacron[361]: Job `cron.weekly' started
Apr 25 07:18:53 debian11 anacron[629]: Updated timestamp for job `cron.weekly' to 2022-04-25
Apr 25 07:18:53 debian11 anacron[361]: Job `cron.weekly' terminated
Apr 25 07:23:53 debian11 anacron[361]: Job `cron.monthly' started
Apr 25 07:23:53 debian11 anacron[361]: Job `cron.monthly' terminated
Apr 25 07:23:53 debian11 anacron[361]: Normal exit (3 jobs run)
Apr 25 07:34:38 debian11 anacron[649]: Anacron 2.3 started on 2022-04-25
Apr 25 07:34:38 debian11 anacron[649]: Normal exit (0 jobs run)
Apr 25 08:30:38 debian11 anacron[677]: Anacron 2.3 started on 2022-04-25
Apr 25 08:30:38 debian11 anacron[677]: Normal exit (0 jobs run)
Apr 25 09:31:58 debian11 anacron[708]: Anacron 2.3 started on 2022-04-25
Apr 25 09:31:58 debian11 anacron[708]: Normal exit (0 jobs run)
Apr 25 10:32:58 debian11 anacron[739]: Anacron 2.3 started on 2022-04-25
```

```
Apr 25 10:32:58 debian11 anacron[739]: Normal exit (0 jobs run)
Apr 25 12:34:38 debian11 anacron[799]: Anacron 2.3 started on 2022-04-25
Apr 25 12:34:38 debian11 anacron[799]: Normal exit (0 jobs run)
Apr 25 13:34:58 debian11 anacron[828]: Anacron 2.3 started on 2022-04-25
Apr 25 13:34:58 debian11 anacron[828]: Normal exit (0 jobs run)
Apr 25 14:33:28 debian11 anacron[8989]: Anacron 2.3 started on 2022-04-25
Apr 25 14:33:28 debian11 anacron[8989]: Normal exit (0 jobs run)
Apr 25 15:30:58 debian11 anacron[9035]: Anacron 2.3 started on 2022-04-25
Apr 25 15:30:58 debian11 anacron[9035]: Normal exit (0 jobs run)
Apr 25 16:33:28 debian11 anacron[9066]: Anacron 2.3 started on 2022-04-25
Apr 25 16:33:28 debian11 anacron[9066]: Normal exit (0 jobs run)
Apr 25 17:32:58 debian11 anacron[9277]: Anacron 2.3 started on 2022-04-25
Apr 25 17:32:58 debian11 anacron[9277]: Normal exit (0 jobs run)
Apr 25 18:34:58 debian11 anacron[9307]: Anacron 2.3 started on 2022-04-25
Apr 25 18:34:58 debian11 anacron[9307]: Normal exit (0 jobs run)
Apr 25 19:32:38 debian11 anacron[9337]: Anacron 2.3 started on 2022-04-25
Apr 25 19:32:38 debian11 anacron[9337]: Normal exit (0 jobs run)
Apr 25 20:32:38 debian11 anacron[9366]: Anacron 2.3 started on 2022-04-25
Apr 25 20:32:38 debian11 anacron[9366]: Normal exit (0 jobs run)
Apr 25 21:34:58 debian11 anacron[9396]: Anacron 2.3 started on 2022-04-25
lines 1-47
[q]
```

Important : Rappelez-vous que sous Debian 11 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@debian11:/# journalctl -b | more
```

```
-- Journal begins at Mon 2022-04-25 07:01:58 CEST, ends at Fri 2022-04-29 15:17:01 CEST. --
Apr 26 13:08:18 debian11 kernel: Linux version 5.10.0-13-amd64 (debian-kernel@lists.debian.org) (gcc-10 (Debian
10.2.1-6) 10.2.1 20210110, GNU ld (GNU Binu
tils for Debian) 2.35.2) #1 SMP Debian 5.10.106-1 (2022-03-17)
Apr 26 13:08:18 debian11 kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.10.0-13-amd64 root=UUID=9887a74f-
a680-4bde-8f04-db5ae9ea186e ro quiet
Apr 26 13:08:18 debian11 kernel: x86/fpu: x87 FPU will use FXSAVE
Apr 26 13:08:18 debian11 kernel: BIOS-provided physical RAM map:
Apr 26 13:08:18 debian11 kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Apr 26 13:08:18 debian11 kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Apr 26 13:08:18 debian11 kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Apr 26 13:08:18 debian11 kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
Apr 26 13:08:18 debian11 kernel: BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
Apr 26 13:08:18 debian11 kernel: BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
Apr 26 13:08:18 debian11 kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Apr 26 13:08:18 debian11 kernel: BIOS-e820: [mem 0x0000000100000000-0x000000013fffffff] usable
Apr 26 13:08:18 debian11 kernel: NX (Execute Disable) protection: active
Apr 26 13:08:18 debian11 kernel: SMBIOS 2.8 present.
Apr 26 13:08:18 debian11 kernel: DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-
prebuilt.qemu.org 04/01/2014
Apr 26 13:08:18 debian11 kernel: Hypervisor detected: KVM
Apr 26 13:08:18 debian11 kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Apr 26 13:08:18 debian11 kernel: kvm-clock: cpu 0, msr 5ccb8001, primary cpu clock
Apr 26 13:08:18 debian11 kernel: kvm-clock: using sched offset of 10164710878 cycles
Apr 26 13:08:18 debian11 kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb,
max_idle_ns: 881590591483 ns
Apr 26 13:08:18 debian11 kernel: tsc: Detected 2399.982 MHz processor
Apr 26 13:08:18 debian11 kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Apr 26 13:08:18 debian11 kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Apr 26 13:08:18 debian11 kernel: last_pfn = 0x140000 max_arch_pfn = 0x400000000
Apr 26 13:08:18 debian11 kernel: MTRR default type: write-back
Apr 26 13:08:18 debian11 kernel: MTRR fixed ranges enabled:
Apr 26 13:08:18 debian11 kernel:   00000-9FFFF write-back
Apr 26 13:08:18 debian11 kernel:   A0000-BFFFF uncachable
```

```
Apr 26 13:08:18 debian11 kernel:   C0000-FFFFF write-protect
Apr 26 13:08:18 debian11 kernel: MTRR variable ranges enabled:
Apr 26 13:08:18 debian11 kernel:   0 base 00C0000000 mask FFC0000000 uncachable
Apr 26 13:08:18 debian11 kernel:   1 disabled
Apr 26 13:08:18 debian11 kernel:   2 disabled
Apr 26 13:08:18 debian11 kernel:   3 disabled
Apr 26 13:08:18 debian11 kernel:   4 disabled
Apr 26 13:08:18 debian11 kernel:   5 disabled
Apr 26 13:08:18 debian11 kernel:   6 disabled
Apr 26 13:08:18 debian11 kernel:   7 disabled
Apr 26 13:08:18 debian11 kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WC  UC- UC
Apr 26 13:08:18 debian11 kernel: last_pfn = 0xbffda max_arch_pfn = 0x400000000
Apr 26 13:08:18 debian11 kernel: found SMP MP-table at [mem 0x000f5a80-0x000f5a8f]
Apr 26 13:08:18 debian11 kernel: RAMDISK: [mem 0x3304d000-0x3581dfff]
Apr 26 13:08:18 debian11 kernel: ACPI: Early table checksum verification disabled
Apr 26 13:08:18 debian11 kernel: ACPI: RSDP 0x00000000000F5880 000014 (v00 BOCHS )
Apr 26 13:08:18 debian11 kernel: ACPI: RSDT 0x00000000BFFE145E 000038 (v01 BOCHS  BXPCRSDT 00000001 BXPC
00000001)
--More--
[q]
```

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

```
root@debian11:/# journalctl -b 1 | more
-- Journal begins at Mon 2022-04-25 07:01:58 CEST, ends at Fri 2022-04-29 15:17:01 CEST. --
Apr 25 07:01:58 debian11 kernel: Linux version 5.10.0-13-amd64 (debian-kernel@lists.debian.org) (gcc-10 (Debian
10.2.1-6) 10.2.1 20210110, GNU ld (GNU Binu
tils for Debian) 2.35.2) #1 SMP Debian 5.10.106-1 (2022-03-17)
Apr 25 07:01:58 debian11 kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.10.0-13-amd64 root=UUID=9887a74f-
a680-4bde-8f04-db5ae9ea186e ro quiet
Apr 25 07:01:58 debian11 kernel: x86/fpu: x87 FPU will use FXSAVE
Apr 25 07:01:58 debian11 kernel: BIOS-provided physical RAM map:
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
```

```
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Apr 25 07:01:58 debian11 kernel: BIOS-e820: [mem 0x0000000100000000-0x000000013fffffff] usable
Apr 25 07:01:58 debian11 kernel: NX (Execute Disable) protection: active
Apr 25 07:01:58 debian11 kernel: SMBIOS 2.8 present.
Apr 25 07:01:58 debian11 kernel: DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-
prebuilt.qemu.org 04/01/2014
Apr 25 07:01:58 debian11 kernel: Hypervisor detected: KVM
Apr 25 07:01:58 debian11 kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Apr 25 07:01:58 debian11 kernel: kvm-clock: cpu 0, msr 86ab8001, primary cpu clock
Apr 25 07:01:58 debian11 kernel: kvm-clock: using sched offset of 2324543470279 cycles
Apr 25 07:01:58 debian11 kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb,
max_idle_ns: 881590591483 ns
Apr 25 07:01:58 debian11 kernel: tsc: Detected 2399.982 MHz processor
Apr 25 07:01:58 debian11 kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Apr 25 07:01:58 debian11 kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Apr 25 07:01:58 debian11 kernel: last_pfn = 0x140000 max_arch_pfn = 0x400000000
Apr 25 07:01:58 debian11 kernel: MTRR default type: write-back
Apr 25 07:01:58 debian11 kernel: MTRR fixed ranges enabled:
Apr 25 07:01:58 debian11 kernel:   00000-9FFFF write-back
Apr 25 07:01:58 debian11 kernel:   A0000-BFFFF uncachable
Apr 25 07:01:58 debian11 kernel:   C0000-FFFFF write-protect
Apr 25 07:01:58 debian11 kernel: MTRR variable ranges enabled:
Apr 25 07:01:58 debian11 kernel:   0 base 00C0000000 mask FFC0000000 uncachable
Apr 25 07:01:58 debian11 kernel:   1 disabled
Apr 25 07:01:58 debian11 kernel:   2 disabled
Apr 25 07:01:58 debian11 kernel:   3 disabled
Apr 25 07:01:58 debian11 kernel:   4 disabled
Apr 25 07:01:58 debian11 kernel:   5 disabled
Apr 25 07:01:58 debian11 kernel:   6 disabled
Apr 25 07:01:58 debian11 kernel:   7 disabled
```

```
Apr 25 07:01:58 debian11 kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WC  UC- UC
Apr 25 07:01:58 debian11 kernel: last_pfn = 0xbffda max_arch_pfn = 0x400000000q]
Apr 25 07:01:58 debian11 kernel: found SMP MP-table at [mem 0x000f5a80-0x000f5a8f]
Apr 25 07:01:58 debian11 kernel: RAMDISK: [mem 0x3304d000-0x3581dfff]
Apr 25 07:01:58 debian11 kernel: ACPI: Early table checksum verification disabled
Apr 25 07:01:58 debian11 kernel: ACPI: RSDP 0x00000000000F5880 000014 (v00 BOCHS )
Apr 25 07:01:58 debian11 kernel: ACPI: RSDT 0x00000000BFFE145E 000038 (v01 BOCHS  BXPCRSDT 00000001 BXPC
00000001)
--More--
[q]
```

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@debian11:/# journalctl -p warning
-- Journal begins at Mon 2022-04-25 07:01:58 CEST, ends at Fri 2022-04-29 15:17:01 CEST. --
Apr 25 07:01:58 debian11 kernel: acpi PNP0A03:00: fail to add MMCONFIG information, can't access extended PCI
configuration space under this bridge.
Apr 25 07:01:58 debian11 kernel: sd 2:0:0:0: Power-on or device reset occurred
Apr 25 07:01:58 debian11 systemd[1]: /lib/systemd/system/plymouth-start.service:16: Unit configured to use
KillMode=none. This is unsafe, as it disables s>
Apr 25 07:02:05 debian11 udisksd[368]: failed to load module mdraid: libbd_mdraid.so.2: cannot open shared object
file: No such file or directory
Apr 25 07:02:05 debian11 udisksd[368]: Failed to load the 'mdraid' libblockdev plugin
Apr 25 07:02:05 debian11 lightdm[408]: Could not enumerate user data directory /var/lib/lightdm/data: Error
opening directory '/var/lib/lightdm/data': No >
Apr 25 07:02:05 debian11 NetworkManager[359]: <warn>  [1650862925.6861] ifupdown: interfaces file
/etc/network/interfaces.d/* doesn't exist
Apr 25 07:02:08 debian11 lightdm[485]: Error getting user list from org.freedesktop.Accounts:
GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The n>
Apr 25 07:02:08 debian11 lightdm[408]: Error getting user list from org.freedesktop.Accounts:
```

```
GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The n>
Apr 25 07:02:09 debian11 pulseaudio[505]: Failed to open cookie file '/var/lib/lightdm/.config/pulse/cookie': No
such file or directory
Apr 25 07:02:09 debian11 pulseaudio[505]: Failed to load authentication key
'/var/lib/lightdm/.config/pulse/cookie': No such file or directory
Apr 25 07:02:09 debian11 pulseaudio[505]: Failed to open cookie file '/var/lib/lightdm/.pulse-cookie': No such
file or directory
Apr 25 07:02:09 debian11 pulseaudio[505]: Failed to load authentication key '/var/lib/lightdm/.pulse-cookie': No
such file or directory
Apr 25 07:02:09 debian11 pipewire[504]: Failed to receive portal pid: org.freedesktop.DBus.Error.NameHasNoOwner:
Could not get PID of name 'org.freedeskto>
Apr 25 07:03:23 debian11 lightdm[554]: gkr-pam: unable to locate daemon control file
Apr 25 07:03:23 debian11 lightdm[554]: Error getting user list from org.freedesktop.Accounts:
GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The n>
Apr 25 07:03:23 debian11 lightdm[408]: g_dbus_connection_call_sync_internal: assertion 'G_IS_DBUS_CONNECTION
(connection)' failed
Apr 25 07:03:23 debian11 pipewire[574]: Failed to receive portal pid: org.freedesktop.DBus.Error.NameHasNoOwner:
Could not get PID of name 'org.freedeskto>
Apr 25 07:03:23 debian11 pulseaudio[575]: Failed to open cookie file '/home/trainee/.config/pulse/cookie': No
such file or directory
Apr 25 07:03:23 debian11 pulseaudio[575]: Failed to load authentication key '/home/trainee/.config/pulse/cookie':
No such file or directory
Apr 25 07:03:23 debian11 pulseaudio[575]: Failed to open cookie file '/home/trainee/.pulse-cookie': No such file
or directory
Apr 25 07:03:23 debian11 pulseaudio[575]: Failed to load authentication key '/home/trainee/.pulse-cookie': No
such file or directory
Apr 25 07:04:38 debian11 systemd[1]: /lib/systemd/system/plymouth-start.service:16: Unit configured to use
KillMode=none. This is unsafe, as it disables s>
Apr 25 07:04:38 debian11 systemd[1]: /lib/systemd/system/plymouth-start.service:16: Unit configured to use
KillMode=none. This is unsafe, as it disables s>
Apr 25 07:04:38 debian11 systemd[1]: /lib/systemd/system/plymouth-start.service:16: Unit configured to use
KillMode=none. This is unsafe, as it disables s>
-- Boot 7fdaa15ef0664ecb99118b80b4db4cd9 --
Apr 25 07:08:52 debian11 kernel: acpi PNP0A03:00: fail to add MMCONFIG information, can't access extended PCI
```

```
configuration space under this bridge.
Apr 25 07:08:52 debian11 kernel: sd 2:0:0:0: Power-on or device reset occurred
Apr 25 07:08:52 debian11 systemd[1]: /lib/systemd/system/plymouth-start.service:16: Unit configured to use
KillMode=none. This is unsafe, as it disables s>
Apr 25 07:08:54 debian11 udisksd[388]: failed to load module mdraid: libbd_mdraid.so.2: cannot open shared object
file: No such file or directory
Apr 25 07:08:54 debian11 lightdm[413]: Error getting user list from org.freedesktop.Accounts:
GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The n>
Apr 25 07:08:54 debian11 udisksd[388]: Failed to load the 'mdraid' libblockdev plugin
Apr 25 07:08:54 debian11 NetworkManager[382]: <warn>  [1650863334.4876] ifupdown: interfaces file
/etc/network/interfaces.d/* doesn't exist
Apr 25 07:08:57 debian11 lightdm[491]: Error getting user list from org.freedesktop.Accounts:
GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The n>
Apr 25 07:08:58 debian11 pipewire[510]: Failed to receive portal pid: org.freedesktop.DBus.Error.NameHasNoOwner:
Could not get PID of name 'org.freedeskto>
Apr 25 13:36:40 debian11 pipewire[850]: could not set nice-level to -11: Permission denied
Apr 25 13:36:40 debian11 pipewire[850]: could not make thread realtime: Permission denied
Apr 25 13:36:40 debian11 pipewire[850]: Failed to receive portal pid: org.freedesktop.DBus.Error.NameHasNoOwner:
Could not get PID of name 'org.freedeskto>
Apr 25 13:36:40 debian11 pipewire-media-session[856]: could not set nice-level to -11: Permission denied
Apr 25 13:36:40 debian11 pipewire-media-session[856]: could not make thread realtime: Permission denied
Apr 25 17:18:37 debian11 pipewire-media-session[856]: error id:0 seq:158 res:-32 (Broken pipe): connection error
-- Boot 7644749265b24b9a8f6a8695c083cfaa --
Apr 26 13:08:18 debian11 kernel: acpi PNP0A03:00: fail to add MMCONFIG information, can't access extended PCI
configuration space under this bridge.
Apr 26 13:08:18 debian11 kernel: sd 2:0:0:2: Power-on or device reset occurred
Apr 26 13:08:18 debian11 kernel: sd 2:0:0:1: Power-on or device reset occurred
Apr 26 13:08:18 debian11 kernel: sd 2:0:0:0: Power-on or device reset occurred
lines 1-47
[q]q
```

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@debian11:/# date
Fri 29 Apr 2022 03:22:00 PM CEST
root@debian11:/# journalctl --since 15:00 --until now
-- Journal begins at Mon 2022-04-25 07:01:58 CEST, ends at Fri 2022-04-29 15:17:01 CEST. --
Apr 29 15:06:18 debian11 trainee[45937]: Linux est super
Apr 29 15:17:01 debian11 audit[45961]: USER_ACCT pid=45961 uid=0 auid=4294967295 ses=4294967295 subj==unconfined
msg='op=PAM:accounting grantors=pam_permi>
Apr 29 15:17:01 debian11 audit[45961]: CRED_ACQ pid=45961 uid=0 auid=4294967295 ses=4294967295 subj==unconfined
msg='op=PAM:setcred grantors=pam_permit,pa>
Apr 29 15:17:01 debian11 audit[45961]: USER_START pid=45961 uid=0 auid=0 ses=145 subj==unconfined
msg='op=PAM:session_open grantors=pam_loginuid,pam_env,p>
Apr 29 15:17:01 debian11 audit[45961]: CRED_DISP pid=45961 uid=0 auid=0 ses=145 subj==unconfined
msg='op=PAM:setcred grantors=pam_permit,pam_ecryptfs acct>
Apr 29 15:17:01 debian11 audit[45961]: USER_END pid=45961 uid=0 auid=0 ses=145 subj==unconfined
msg='op=PAM:session_close grantors=pam_loginuid,pam_env,pa>
Apr 29 15:17:01 debian11 CRON[45961]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Apr 29 15:17:01 debian11 CRON[45962]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Apr 29 15:17:01 debian11 CRON[45961]: pam_unix(cron:session): session closed for user root
lines 1-10/10 (END)
[q]
```

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@debian11:/# journalctl -f
-- Journal begins at Mon 2022-04-25 07:01:58 CEST. --
Apr 29 14:38:42 debian11 systemd[1]: Started Updates mlocate database every day.
Apr 29 15:06:18 debian11 trainee[45937]: Linux est super
Apr 29 15:17:01 debian11 audit[45961]: USER_ACCT pid=45961 uid=0 auid=4294967295 ses=4294967295 subj==unconfined
msg='op=PAM:accounting grantors=pam_permit acct="root" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron
res=success'
Apr 29 15:17:01 debian11 audit[45961]: CRED_ACQ pid=45961 uid=0 auid=4294967295 ses=4294967295 subj==unconfined
msg='op=PAM:setcred grantors=pam_permit,pam_ecryptfs acct="root" exe="/usr/sbin/cron" hostname=? addr=?
terminal=cron res=success'
Apr 29 15:17:01 debian11 audit[45961]: USER_START pid=45961 uid=0 auid=0 ses=145 subj==unconfined
msg='op=PAM:session_open grantors=pam_loginuid,pam_env,pam_env,pam_permit,pam_unix,pam_ecryptfs,pam_limits
acct="root" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
Apr 29 15:17:01 debian11 audit[45961]: CRED_DISP pid=45961 uid=0 auid=0 ses=145 subj==unconfined
msg='op=PAM:setcred grantors=pam_permit,pam_ecryptfs acct="root" exe="/usr/sbin/cron" hostname=? addr=?
terminal=cron res=success'
Apr 29 15:17:01 debian11 audit[45961]: USER_END pid=45961 uid=0 auid=0 ses=145 subj==unconfined
msg='op=PAM:session_close grantors=pam_loginuid,pam_env,pam_env,pam_permit,pam_unix,pam_ecryptfs,pam_limits
acct="root" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
Apr 29 15:17:01 debian11 CRON[45961]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Apr 29 15:17:01 debian11 CRON[45962]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Apr 29 15:17:01 debian11 CRON[45961]: pam_unix(cron:session): session closed for user root
^C
```
