Version : **2024.01**

Dernière mise-à-jour : 2024/11/28 08:58

RH12411 - 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@redhat9 ~]# dmesg | more
[    0.000000] Linux version 5.14.0-427.37.1.el9_4.x86_64 (mockbuild@x86-64-02.build.eng.rdu2.redhat.com) (gcc
(GCC) 11.4.1 20231218 (Red Hat 11.4.1-3), GNU ld version 2.35.2-43.el9) #1 SMP PREEMPT_DYNAMIC Fri
Sep 13 12:41:50 EDT 2024
[    0.000000] The list of certified hardware and cloud instances for Red Hat Enterprise Linux 9 can be viewed at
the Red Hat Ecosystem Catalog, https://catalog.redhat.com.
[    0.000000] Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.37.1.el9_4.x86_64 root=/dev/mapper/rhel-
root ro crashkernel=1G-4G:192M,4G-64G:256M,64G-:512M resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/r
oot rd.lvm.lv=rhel/swap 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] signal: max sigframe size: 1776
[    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 0x0000000100000000-0x000000023fffffff] 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-1.16.1-0-g3208b098f51a-prebuilt.qemu.org
04/01/2014
[    0.000000] Hypervisor detected: KVM
[    0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[    0.000001] kvm-clock: using sched offset of 11342917026 cycles
[    0.000003] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns:
881590591483 ns
[    0.000010] tsc: Detected 2099.998 MHz processor
[    0.001013] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.001016] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.001021] last_pfn = 0x240000 max_arch_pfn = 0x400000000
[    0.001058] MTRR map: 4 entries (3 fixed + 1 variable; max 19), built from 8 variable MTRRs
[    0.001061] x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
[    0.001103] last_pfn = 0xbffda max_arch_pfn = 0x400000000
[    0.009594] found SMP MP-table at [mem 0x000f5bc0-0x000f5bcf]
[    0.009621] Using GB pages for direct mapping
[    0.009825] RAMDISK: [mem 0x3149c000-0x34a45fff]
[    0.009836] ACPI: Early table checksum verification disabled
[    0.009849] ACPI: RSDP 0x00000000000F5980 000014 (v00 BOCHS )
[    0.009857] ACPI: RSDT 0x00000000BFFE300C 000038 (v01 BOCHS  BXPC     00000001 BXPC 00000001)
[    0.009870] ACPI: FACP 0x00000000BFFE2DDE 000074 (v01 BOCHS  BXPC     00000001 BXPC 00000001)
[    0.009876] ACPI: DSDT 0x00000000BFFDF040 003D9E (v01 BOCHS  BXPC     00000001 BXPC 00000001)
[    0.009881] ACPI: FACS 0x00000000BFFDF000 000040
[    0.009885] ACPI: APIC 0x00000000BFFE2E52 000090 (v01 BOCHS  BXPC     00000001 BXPC 00000001)
[    0.009889] ACPI: SSDT 0x00000000BFFE2EE2 0000CA (v01 BOCHS  VMGENID  00000001 BXPC 00000001)
[    0.009893] ACPI: HPET 0x00000000BFFE2FAC 000038 (v01 BOCHS  BXPC     00000001 BXPC 00000001)
[    0.009898] ACPI: WAET 0x00000000BFFE2FE4 000028 (v01 BOCHS  BXPC     00000001 BXPC 00000001)
[    0.009901] ACPI: Reserving FACP table memory at [mem 0xbffe2dde-0xbffe2e51]
[    0.009902] ACPI: Reserving DSDT table memory at [mem 0xbffdf040-0xbffe2ddd]
[    0.009903] ACPI: Reserving FACS table memory at [mem 0xbffdf000-0xbffdf03f]
[    0.009904] ACPI: Reserving APIC table memory at [mem 0xbffe2e52-0xbffe2ee1]
```

```
[    0.009905] ACPI: Reserving SSDT table memory at [mem 0xbffe2ee2-0xbffe2fab]
[    0.009906] ACPI: Reserving HPET table memory at [mem 0xbffe2fac-0xbffe2fe3]
[    0.009906] ACPI: Reserving WAET table memory at [mem 0xbffe2fe4-0xbffe300b]
[    0.010241] No NUMA configuration found
--More--
[q]
```

Les option de cette commande sont :

```
[root@redhat9 ~]# 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.
     --since <time>          display the lines since the specified time
     --until <time>          display the lines until the specified time

 -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@redhat9 ~]# last
trainee  pts/1        10.0.2.1         Sat Sep 28 08:43   still logged in
trainee  pts/0        10.0.2.1         Sat Sep 28 08:09   still logged in
trainee  pts/0        10.0.2.1         Fri Sep 27 08:02 - 17:23  (09:20)
trainee  pts/0        10.0.2.1         Fri Sep 27 07:49 - 08:02  (00:13)
trainee  pts/0        10.0.2.1         Thu Sep 26 12:20 - 15:44  (03:23)
trainee  pts/0        10.0.2.1         Wed Sep 25 12:47 - 17:31  (04:44)
reboot   system boot  5.14.0-427.37.1. Wed Sep 25 12:44   still running
reboot   system boot  5.14.0-427.37.1. Wed Sep 25 12:29   still running
trainee  pts/0        10.0.2.1         Wed Sep 25 11:35 - 12:29  (00:54)
trainee  pts/0        10.0.2.1         Wed Sep 25 10:14 - 10:50  (00:35)
reboot   system boot  5.14.0-284.11.1. Wed Sep 25 10:14 - 12:29  (02:15)
trainee  pts/1        10.0.2.99        Thu Oct 19 18:35 - 18:35  (00:00)
trainee  tty2         tty2             Thu Oct 19 18:28 - crash (341+15:45)
trainee  seat0        login screen     Thu Oct 19 18:28 - crash (341+15:45)
reboot   system boot  5.14.0-284.11.1. Thu Oct 19 18:27 - 12:29 (341+18:02)

wtmp begins Thu Oct 19 18:27:17 2023
```

Les option de cette commande sont :

```
[root@redhat9 ~]# 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@redhat9 ~]# lastlog
Username         Port     From                                       Latest
root             pts/1                                               Sat Sep 28 08:43:22 +0200 2024
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**
systemd-coredump                                                     **Never logged in**
dbus                                                                 **Never logged in**
polkitd                                                              **Never logged in**
avahi                                                                **Never logged in**
tss                                                                  **Never logged in**
colord                                                               **Never logged in**
clevis                                                               **Never logged in**
rtkit                                                                **Never logged in**
sssd                                                                 **Never logged in**
geoclue                                                              **Never logged in**
libstoragemgmt                                                       **Never logged in**
systemd-oom                                                          **Never logged in**
setroubleshoot                                                       **Never logged in**
pipewire                                                             **Never logged in**
```

```
flatpak                                                     **Never logged in**
gdm              tty1                                       Thu Sep 26 14:55:01 +0200 2024
cockpit-ws                                                  **Never logged in**
cockpit-wsinstance                                            **Never logged in**
gnome-initial-setup                                            **Never logged in**
sshd                                                        **Never logged in**
chrony                                                      **Never logged in**
dnsmasq                                                     **Never logged in**
tcpdump                                                     **Never logged in**
trainee          pts/1    10.0.2.1                          Sat Sep 28 08:43:17 +0200 2024
apache                                                      **Never logged in**
fenestros2       pts/0                                      Fri Sep 27 14:22:01 +0200 2024
fenestros1                                                  **Never logged in**
```

Les option de cette commande sont :

```
[root@redhat9 ~]# 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@redhat9 ~]# lastb
```

```
root     pts/0                        Wed Sep 25 11:41 - 11:41  (00:00)
root     pts/0                        Thu Oct 19 18:29 - 18:29  (00:00)

btmp begins Thu Oct 19 18:29:22 2023
```

Les options de cette commande sont :

```
[root@redhat9 ~]# 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 9 ce fichier contient la journalisation des opérations de gestion des authentifications :

```
[root@redhat9 ~]# tail -n 15 /var/log/secure
Sep 27 14:08:31 redhat9 passwd[10515]: gkr-pam: couldn't update the login keyring password: no old password was
entered
Sep 27 14:21:40 redhat9 su[10537]: pam_unix(su:session): session opened for user fenestros2(uid=1001) by
trainee(uid=0)
Sep 27 14:21:50 redhat9 su[10537]: pam_unix(su:session): session closed for user fenestros2
Sep 27 14:22:01 redhat9 su[10561]: pam_unix(su-l:session): session opened for user fenestros2(uid=1001) by
trainee(uid=0)
Sep 27 14:23:49 redhat9 su[10561]: pam_unix(su-l:session): session closed for user fenestros2
Sep 27 17:23:32 redhat9 sshd[9392]: Received disconnect from 10.0.2.1 port 37560:11: disconnected by user
Sep 27 17:23:32 redhat9 sshd[9392]: Disconnected from user trainee 10.0.2.1 port 37560
Sep 27 17:23:32 redhat9 sshd[9357]: pam_unix(sshd:session): session closed for user trainee
Sep 27 17:23:32 redhat9 su[10062]: pam_unix(su-l:session): session closed for user root
Sep 28 08:09:13 redhat9 sshd[11965]: Accepted password for trainee from 10.0.2.1 port 42238 ssh2
Sep 28 08:09:13 redhat9 systemd[11972]: pam_unix(systemd-user:session): session opened for user trainee(uid=1000)
by trainee(uid=0)
Sep 28 08:09:13 redhat9 sshd[11965]: pam_unix(sshd:session): session opened for user trainee(uid=1000) by
trainee(uid=0)
Sep 28 08:43:17 redhat9 sshd[12053]: Accepted password for trainee from 10.0.2.1 port 33994 ssh2
Sep 28 08:43:17 redhat9 sshd[12053]: pam_unix(sshd:session): session opened for user trainee(uid=1000) by
trainee(uid=0)
Sep 28 08:43:22 redhat9 su[12102]: 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 est installé par défaut dans RHEL 9 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@redhat9 ~]# tail -n 15 /var/log/audit/audit.log
type=CRYPTO_KEY_USER msg=audit(1727528067.947:1046): pid=12618 uid=0 auid=1000 ses=14
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server
fp=SHA256:93:f7:28:a0:3a:d4:ca:78:e9:ac:1a:21:98:58:c9:77:6d:88:8b:6c:65:09:71:5d:4c:7b:7f:1c:05:e9:0c:4e
direction=? spid=12618 suid=0  exe="/usr/sbin/sshd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="trainee" SUID="root"
type=CRED_ACQ msg=audit(1727528067.948:1047): pid=12618 uid=0 auid=1000 ses=14 subj=system_u:system_r:sshd_t:s0-
s0:c0.c1023 msg='op=PAM:setcred grantors=pam_localuser,pam_unix acct="trainee" exe="/usr/sbin/sshd"
hostname=10.0.2.1 addr=10.0.2.1 terminal=ssh res=success'UID="root" AUID="trainee"
type=USER_LOGIN msg=audit(1727528067.994:1048): pid=12613 uid=0 auid=1000 ses=14
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=1000 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.1
terminal=/dev/pts/1 res=success'UID="root" AUID="trainee" ID="trainee"
type=USER_START msg=audit(1727528067.994:1049): pid=12613 uid=0 auid=1000 ses=14
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=1000 exe="/usr/sbin/sshd" hostname=? addr=10.0.2.1
terminal=/dev/pts/1 res=success'UID="root" AUID="trainee" ID="trainee"
type=CRYPTO_KEY_USER msg=audit(1727528067.996:1050): pid=12613 uid=0 auid=1000 ses=14
subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server
fp=SHA256:93:f7:28:a0:3a:d4:ca:78:e9:ac:1a:21:98:58:c9:77:6d:88:8b:6c:65:09:71:5d:4c:7b:7f:1c:05:e9:0c:4e
direction=? spid=12628 suid=1000  exe="/usr/sbin/sshd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="trainee" SUID="trainee"
```

```
type=BPF msg=audit(1727528068.011:1051): prog-id=189 op=LOAD
type=BPF msg=audit(1727528068.011:1052): prog-id=190 op=LOAD
type=SERVICE_START msg=audit(1727528068.076:1053): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd"
hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=USER_AUTH msg=audit(1727528075.273:1054): pid=12662 uid=1000 auid=1000 ses=14
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix
acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="trainee" AUID="trainee"
type=USER_ACCT msg=audit(1727528075.276:1055): pid=12662 uid=1000 auid=1000 ses=14
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser
acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="trainee" AUID="trainee"
type=CRED_ACQ msg=audit(1727528075.277:1056): pid=12662 uid=1000 auid=1000 ses=14
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root"
exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'UID="trainee" AUID="trainee"
type=USER_START msg=audit(1727528075.281:1057): pid=12662 uid=1000 auid=1000 ses=14
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=? addr=? terminal=/dev/pts/1 res=success'UID="trainee" AUID="trainee"
type=SERVICE_STOP msg=audit(1727528105.326:1058): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd"
hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=BPF msg=audit(1727528105.369:1059): prog-id=190 op=UNLOAD
type=BPF msg=audit(1727528105.369:1060): prog-id=189 op=UNLOAD
```

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@redhat9 ~]# 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 = 2000
overflow_action = SYSLOG
max_restarts = 10
plugin_dir = /etc/audit/plugins.d
end_of_event_timeout = 2
```

Les option de cette commande sont :

```
[root@redhat9 ~]# 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@redhat9 ~]# cat /etc/audit/audit.rules
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1
--backlog_wait_time 60000

[root@redhat9 ~]# ls -l /etc/audit/rules.d
total 4
-rw-------. 1 root root 244 Oct 19  2023 audit.rules

[root@redhat9 ~]# cat /etc/audit/rules.d/audit.rules
## First rule - delete all
-D
```

```
## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1
```

Les options de cette commande sont :

```
[root@redhat9 ~]# 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,filesystem
                                    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
There was an error while processing parameters
```

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@redhat9 ~]# aureport

Summary Report
======================
```

```
Range of time in logs: 10/19/2023 18:27:19.140 - 09/28/2024 14:57:20.231
Selected time for report: 10/19/2023 18:27:19 - 09/28/2024 14:57:20.231
Number of changes in configuration: 72
Number of changes to accounts, groups, or roles: 30
Number of logins: 12
Number of failed logins: 0
Number of authentications: 43
Number of failed authentications: 11
Number of users: 4
Number of terminals: 9
Number of host names: 4
Number of executables: 21
Number of commands: 11
Number of files: 0
Number of AVC's: 0
Number of MAC events: 41
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 104
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 158
Number of events: 2567
```

Les options de cette commande sont :

```
[root@redhat9 ~]# 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
        --debug                             Write malformed events that are skipped to stderr
        --eoe-timeout secs                  End of Event Timeout
        -e,--event                          Event report
        --escape option                     Escape output
        -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
        -k,--key                            Key report
        -l,--login                          Login 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@redhat9 ~]# ausearch -ui 1000 | more
----
time->Thu Oct 19 18:29:20 2023
type=USER_AUTH msg=audit(1697732960.285:140): pid=6261 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=? acct="root"
exe="/usr/bin/su" hos
tname=? addr=? terminal=/dev/pts/0 res=failed'
----
time->Thu Oct 19 18:29:31 2023
type=USER_AUTH msg=audit(1697732971.707:144): pid=6294 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix
acct="root" exe="/usr/bin/
su" hostname=? addr=? terminal=/dev/pts/0 res=success'
----
time->Thu Oct 19 18:29:31 2023
type=USER_ACCT msg=audit(1697732971.746:145): pid=6294 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser
acct="root" exe=
"/usr/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'
----
time->Thu Oct 19 18:29:31 2023
type=CRED_ACQ msg=audit(1697732971.747:146): pid=6294 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root"
exe="/usr/bin/su" host
name=? addr=? terminal=/dev/pts/0 res=success'
----
```

```
time->Thu Oct 19 18:29:31 2023
type=USER_START msg=audit(1697732971.835:147): pid=6294 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open
grantors=pam_keyinit,pam_keyinit,pam_limits,p
am_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/0
res=success'
----
time->Thu Oct 19 18:35:21 2023
type=USER_AUTH msg=audit(1697733321.865:218): pid=6500 uid=1000 auid=1000 ses=6
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix
acct="root" exe="/usr/bin/
su" hostname=? addr=? terminal=/dev/pts/1 res=success'
----
time->Thu Oct 19 18:35:21 2023
type=USER_ACCT msg=audit(1697733321.905:219): pid=6500 uid=1000 auid=1000 ses=6
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser
acct="root" exe=
"/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1 res=success'
----
time->Thu Oct 19 18:35:21 2023
type=CRED_ACQ msg=audit(1697733321.905:220): pid=6500 uid=1000 auid=1000 ses=6
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root"
exe="/usr/bin/su" host
name=? addr=? terminal=/dev/pts/1 res=success'
----
time->Thu Oct 19 18:35:21 2023
type=USER_START msg=audit(1697733321.909:221): pid=6500 uid=1000 auid=1000 ses=6
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open
grantors=pam_keyinit,pam_keyinit,pam_limits,p
am_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1
res=success'
----
time->Thu Oct 19 18:35:40 2023
type=USER_END msg=audit(1697733340.703:222): pid=6500 uid=1000 auid=1000 ses=6
```

```
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_close
grantors=pam_keyinit,pam_keyinit,pam_limits,pa
m_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/1
res=success'
----
time->Thu Oct 19 18:35:40 2023
type=CRED_DISP msg=audit(1697733340.704:223): pid=6500 uid=1000 auid=1000 ses=6
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root"
exe="/usr/bin/su" hos
tname=? addr=? terminal=/dev/pts/1 res=success'
----
time->Wed Sep 25 10:15:06 2024
type=USER_AUTH msg=audit(1727252106.538:115): pid=1963 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix
acct="root" exe="/usr/bin/
su" hostname=? addr=? terminal=/dev/pts/0 res=success'
----
time->Wed Sep 25 10:15:06 2024
type=USER_ACCT msg=audit(1727252106.579:116): pid=1963 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser
acct="root" exe=
"/usr/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'
----
time->Wed Sep 25 10:15:06 2024
type=CRED_ACQ msg=audit(1727252106.579:117): pid=1963 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root"
exe="/usr/bin/su" host
--More--
[q]
```

Les options de cette commande sont :

```
[root@redhat9 ~]# 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
-escape <option>                escape output
--eoe-timeout secs              End of Event timeout
--extra-keys                    add a final column with key information
--extra-labels                  add columns of information about subject and object labels
--extra-obj2                    add columns of information about a second object
--extra-time                    add columns of information about broken down time
-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@redhat9 ~]# tail -n 15 /var/log/messages
```

```
Sep 28 13:33:57 redhat9 systemd[1]: dnf-makecache.service: Consumed 1.476s CPU time.
Sep 28 13:35:04 redhat9 cupsd[5736]: REQUEST localhost - - "POST / HTTP/1.1" 200 182 Renew-Subscription
successful-ok
Sep 28 14:33:24 redhat9 cupsd[5736]: REQUEST localhost - - "POST / HTTP/1.1" 200 182 Renew-Subscription
successful-ok
Sep 28 14:54:27 redhat9 systemd-logind[5671]: New session 14 of user trainee.
Sep 28 14:54:27 redhat9 systemd[1]: Started Session 14 of User trainee.
Sep 28 14:54:28 redhat9 systemd[1]: Starting Hostname Service...
Sep 28 14:54:28 redhat9 systemd[1]: Started Hostname Service.
Sep 28 14:54:35 redhat9 su[12662]: (to root) trainee on pts/1
Sep 28 14:55:05 redhat9 systemd[1]: systemd-hostnamed.service: Deactivated successfully.
Sep 28 14:57:20 redhat9 systemd[1]: Starting Cleanup of Temporary Directories...
Sep 28 14:57:20 redhat9 systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Sep 28 14:57:20 redhat9 systemd[1]: Finished Cleanup of Temporary Directories.
Sep 28 14:57:20 redhat9 systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated
successfully.
Sep 28 15:02:37 redhat9 systemd[5851]: Starting Cleanup of User's Temporary Files and Directories...
Sep 28 15:02:37 redhat9 systemd[5851]: Finished Cleanup of User's Temporary Files and Directories.
```

Applications

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

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

```
[root@redhat9 ~]# ls -l /var/log
total 1952
drwxr-xr-x. 2 root   root     4096 Oct 19  2023 anaconda
drwx------. 2 root   root       23 Nov  8  2023 audit
```

```
-rw-------. 1 root   root        0 Sep 26 00:00 boot.log
-rw-------. 1 root   root    68528 Sep 26 00:00 boot.log-20240926
-rw-rw----. 1 root   utmp      768 Sep 25 11:41 btmp
drwxr-x---. 2 chrony chrony      6 Jan 23  2024 chrony
-rw-------. 1 root   root    31832 Sep 28 15:01 cron
drwxr-xr-x. 2 lp     sys        57 Jun 19 11:00 cups
-rw-r--r--. 1 root   root   150441 Sep 28 13:33 dnf.librepo.log
-rw-r--r--. 1 root   root   672698 Sep 28 13:33 dnf.log
-rw-r--r--. 1 root   root    96613 Sep 28 13:33 dnf.rpm.log
-rw-r-----. 1 root   root        0 Oct 19  2023 firewalld
drwx--x--x. 2 root   gdm         6 Jan 18  2024 gdm
-rw-r--r--. 1 root   root     4440 Sep 28 14:39 hawkey.log
drwx------. 2 root   root       41 Sep 26 15:01 httpd
drwx------. 2 root   root        6 Feb 15  2024 insights-client
-rw-------. 1 root   root     3942 Sep 26 14:55 kdump.log
-rw-rw-r--. 1 root   utmp   293168 Sep 28 14:54 lastlog
-rw-------. 1 root   root        0 Oct 19  2023 maillog
-rw-------. 1 root   root   875426 Sep 28 15:02 messages
drwx------. 2 root   root        6 Oct 19  2023 private
drwxr-xr-x. 2 root   root        6 Aug 15 09:40 qemu-ga
lrwxrwxrwx. 1 root   root       39 Oct 19  2023 README -> ../../usr/share/doc/systemd/README.logs
drwxr-xr-x. 2 root   root       43 Jan 18  2024 rhsm
drwx------. 3 root   root       17 May  1 21:13 samba
-rw-------. 1 root   root    28327 Sep 28 14:54 secure
drwx------. 2 root   root        6 Aug 11  2021 speech-dispatcher
-rw-------. 1 root   root        0 Oct 19  2023 spooler
drwxr-x---. 2 sssd   sssd       26 May 17 03:59 sssd
-rw-------. 1 root   root        0 Oct 19  2023 tallylog
drwxr-xr-x. 2 root   root       23 Feb 22  2024 tuned
-rw-rw-r--. 1 root   utmp    12288 Sep 28 14:54 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 9, le daemon rsyslog est configuré par l'édition du fichier **/etc/sysconfig/rsyslog** :

```
[root@redhat9 ~]# 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
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

Fonction	Description
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@redhat9 ~]# 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

#### GLOBAL DIRECTIVES ####

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

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

#### 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
       UsePid="system" # PID nummber is retrieved as the ID of the process the journal entry originates from
       FileCreateMode="0644" # Set the access permissions for the state file
```

```
       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

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

# 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")

#### 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”** et **module(load=“imjournal”** 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
       UsePid="system" # PID nummber is retrieved as the ID of the process the journal entry originates from
       FileCreateMode="0644" # Set the access permissions for the state file
       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
...
```

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 la ligne **Target** 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="XXX" 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@redhat9 ~]# logger -p user.info Linux est super
```

Consultez la fin de votre syslog :

```
[root@redhat9 ~]# tail /var/log/messages
Sep 28 15:05:26 redhat9 dnf[12735]: Extra Packages for Enterprise Linux 9 openh264  6.9 kB/s | 993  B     00:00
Sep 28 15:05:26 redhat9 dnf[12735]: Extra Packages for Enterprise Linux 9 - Next -  199 kB/s |  26 kB     00:00
Sep 28 15:05:27 redhat9 dnf[12735]: Red Hat Enterprise Linux 9 for x86_64 - AppStre  12 kB/s | 4.5 kB     00:00
Sep 28 15:05:27 redhat9 dnf[12735]: Red Hat Enterprise Linux 9 for x86_64 - BaseOS  7.4 kB/s | 4.1 kB     00:00
Sep 28 15:05:28 redhat9 dnf[12735]: Red Hat CodeReady Linux Builder for RHEL 9 x86_  34 kB/s | 4.5 kB     00:00
Sep 28 15:05:28 redhat9 dnf[12735]: Metadata cache created.
Sep 28 15:05:28 redhat9 systemd[1]: dnf-makecache.service: Deactivated successfully.
Sep 28 15:05:28 redhat9 systemd[1]: Finished dnf makecache.
Sep 28 15:05:28 redhat9 systemd[1]: dnf-makecache.service: Consumed 2.948s CPU time.
```

```
Sep 28 15:15:29 redhat9 root[12751]: Linux est super
```

Les options de la commande logger sont :

```
[root@redhat9 ~]# 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@redhat9 ~]# 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 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@redhat9 ~]# 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
      --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 RHEL 9, 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@redhat9 ~]# ls -l /run/log/journal/
total 0
drwxr-s---+ 2 root systemd-journal 60 Sep 25 12:44 5a35a3eb625c45cea1d33535723e791f
```

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

La configuration de ce comportement se trouve dans le fichier **/etc/systemd/journald.conf** et est défini par la valeur de la variable **Storage** :

```
[root@redhat9 ~]# 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. Local configuration
# should be created by either modifying this file, or by creating "drop-ins" in
```

```
# the journald.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# Use 'systemd-analyze cat-config systemd/journald.conf' to display the full config.
#
# 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
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
```

```
#MaxLevelWall=emerg
#LineMax=48K
#ReadKMsg=yes
Audit=
```

La valeur de la variable peut être :

- **auto** - si le répertoire **/var/log/journal** existe, le journal devient persistant,
- **persistent** - le journal est persistant et est stocké dans le répertoire **/var/log/journal**,
- **volatile** - le journal est stocké dans un fichier dynamique dans le répertoire **/run/log/journal**.

Pour rendre le journal permenant, modifiez le fichier **/etc/systemd/journald.conf** et décommentez la directive **Storage** :

```
[root@redhat9 ~]# vi /etc/systemd/journald.conf
[root@redhat9 ~]# 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. Local configuration
# should be created by either modifying this file, or by creating "drop-ins" in
# the journald.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# Use 'systemd-analyze cat-config systemd/journald.conf' to display the full config.
#
# 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
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
#LineMax=48K
#ReadKMsg=yes
Audit=
```

Créez le répertoire **/var/log/journal** :

```
[root@redhat9 ~]# mkdir /var/log/journal
[root@redhat9 ~]# ls -l /var/log/journal/
```

```
total 0
```

Redémarrez votre VM :

```
[root@redhat9 ~]# reboot
[root@redhat9 ~]# Connection to 10.0.2.101 closed by remote host.
Connection to 10.0.2.101 closed.
```

Reconnectez-vous à votre VM :

```
[trainee@redhat9 ~]$ su -
Password: fenestros

[root@redhat9 ~]# ls -l /run/log/journal/
total 0

[root@redhat9 ~]# ls -l /var/log/journal/
total 0
drwxr-sr-x+ 2 root systemd-journal 53 Sep 28 15:39 5a35a3eb625c45cea1d33535723e791f
```

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

5.1 - Consultation des Journaux

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

```
[root@redhat9 ~]# journalctl
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Linux version 5.14.0-427.37.1.el9_4.x86_64
(mockbuild@x86-64-02.build.eng.rdu2.redhat.com) (gcc (GCC) 11.4.1 20231218 (Red Hat 11.4.1-3), GNU ld version
2.35.2-43>
```

```
Sep 28 15:36:59 redhat9.ittraining.loc kernel: The list of certified hardware and cloud instances for Red Hat
Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https://catalog.redhat.com.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Command line:
BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.37.1.el9_4.x86_64 root=/dev/mapper/rhel-root ro
crashkernel=1G-4G:192M,4G-64G:256M,64G-:512M resume=/dev/>
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes,
using 'standard' format.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: signal: max sigframe size: 1776
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-provided physical RAM map:
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000100000000-0x000000023fffffff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: NX (Execute Disable) protection: active
Sep 28 15:36:59 redhat9.ittraining.loc kernel: SMBIOS 2.8 present.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.1-0-
g3208b098f51a-prebuilt.qemu.org 04/01/2014
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Hypervisor detected: KVM
Sep 28 15:36:59 redhat9.ittraining.loc kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 28 15:36:59 redhat9.ittraining.loc kernel: kvm-clock: using sched offset of 269552729537899 cycles
Sep 28 15:36:59 redhat9.ittraining.loc kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles:
0x1cd42e4dffb, max_idle_ns: 881590591483 ns
Sep 28 15:36:59 redhat9.ittraining.loc kernel: tsc: Detected 2099.998 MHz processor
Sep 28 15:36:59 redhat9.ittraining.loc kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
```

```
Sep 28 15:36:59 redhat9.ittraining.loc kernel: last_pfn = 0x240000 max_arch_pfn = 0x400000000
Sep 28 15:36:59 redhat9.ittraining.loc kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 19), built from 8
variable MTRRs
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
Sep 28 15:36:59 redhat9.ittraining.loc kernel: last_pfn = 0xbffda max_arch_pfn = 0x400000000
Sep 28 15:36:59 redhat9.ittraining.loc kernel: found SMP MP-table at [mem 0x000f5bc0-0x000f5bcf]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Using GB pages for direct mapping
Sep 28 15:36:59 redhat9.ittraining.loc kernel: RAMDISK: [mem 0x3149c000-0x34a45fff]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Early table checksum verification disabled
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: RSDP 0x00000000000F5980 000014 (v00 BOCHS )
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: RSDT 0x00000000BFFE300C 000038 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: FACP 0x00000000BFFE2DDE 000074 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: DSDT 0x00000000BFFDF040 003D9E (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: FACS 0x00000000BFFDF000 000040
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: APIC 0x00000000BFFE2E52 000090 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: SSDT 0x00000000BFFE2EE2 0000CA (v01 BOCHS  VMGENID  00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: HPET 0x00000000BFFE2FAC 000038 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: WAET 0x00000000BFFE2FE4 000028 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving FACP table memory at [mem 0xbffe2dde-0xbffe2e51]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving DSDT table memory at [mem 0xbffdf040-0xbffe2ddd]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving FACS table memory at [mem 0xbffdf000-0xbffdf03f]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving APIC table memory at [mem 0xbffe2e52-0xbffe2ee1]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving SSDT table memory at [mem 0xbffe2ee2-0xbffe2fab]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving HPET table memory at [mem 0xbffe2fac-0xbffe2fe3]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving WAET table memory at [mem 0xbffe2fe4-0xbffe300b]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: No NUMA configuration found
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Faking a node at [mem 0x0000000000000000-0x000000023fffffff]
```

```
Sep 28 15:36:59 redhat9.ittraining.loc kernel: NODE_DATA(0) allocated [mem 0x23ffd5000-0x23fffffff]
lines 1-55
```

> **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@redhat9 ~]# journalctl /sbin/crond
Sep 28 15:37:18 redhat9.ittraining.loc crond[1138]: (CRON) STARTUP (1.5.7)
Sep 28 15:37:18 redhat9.ittraining.loc crond[1138]: (CRON) INFO (Syslog will be used instead of sendmail.)
Sep 28 15:37:18 redhat9.ittraining.loc crond[1138]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 65% if
used.)
Sep 28 15:37:18 redhat9.ittraining.loc crond[1138]: (CRON) INFO (running with inotify support)
```

> **Important** : Rappelez-vous que sous RHEL9 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@redhat9 ~]# journalctl -b | more
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Linux version 5.14.0-427.37.1.el9_4.x86_64
(mockbuild@x86-64-02.build.eng.rdu2.redhat.com) (gcc (GCC) 11.4.1 20231218 (Red Hat 11.4.1-3), GNU ld version
2.35.2-43.
el9) #1 SMP PREEMPT_DYNAMIC Fri Sep 13 12:41:50 EDT 2024
Sep 28 15:36:59 redhat9.ittraining.loc kernel: The list of certified hardware and cloud instances for Red Hat
Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https://catalog.redhat.com.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Command line:
BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.37.1.el9_4.x86_64 root=/dev/mapper/rhel-root ro
crashkernel=1G-4G:192M,4G-64G:256M,64G-:512M resume=/dev/m
apper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes,
using 'standard' format.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: signal: max sigframe size: 1776
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-provided physical RAM map:
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000100000000-0x000000023fffffff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: NX (Execute Disable) protection: active
Sep 28 15:36:59 redhat9.ittraining.loc kernel: SMBIOS 2.8 present.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.1-0-
g3208b098f51a-prebuilt.qemu.org 04/01/2014
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Hypervisor detected: KVM
Sep 28 15:36:59 redhat9.ittraining.loc kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
```

```
Sep 28 15:36:59 redhat9.ittraining.loc kernel: kvm-clock: using sched offset of 269552729537899 cycles
Sep 28 15:36:59 redhat9.ittraining.loc kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles:
0x1cd42e4dffb, max_idle_ns: 881590591483 ns
Sep 28 15:36:59 redhat9.ittraining.loc kernel: tsc: Detected 2099.998 MHz processor
Sep 28 15:36:59 redhat9.ittraining.loc kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: last_pfn = 0x240000 max_arch_pfn = 0x400000000
Sep 28 15:36:59 redhat9.ittraining.loc kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 19), built from 8
variable MTRRs
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
Sep 28 15:36:59 redhat9.ittraining.loc kernel: last_pfn = 0xbffda max_arch_pfn = 0x400000000
Sep 28 15:36:59 redhat9.ittraining.loc kernel: found SMP MP-table at [mem 0x000f5bc0-0x000f5bcf]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Using GB pages for direct mapping
Sep 28 15:36:59 redhat9.ittraining.loc kernel: RAMDISK: [mem 0x3149c000-0x34a45fff]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Early table checksum verification disabled
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: RSDP 0x00000000000F5980 000014 (v00 BOCHS )
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: RSDT 0x00000000BFFE300C 000038 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: FACP 0x00000000BFFE2DDE 000074 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: DSDT 0x00000000BFFDF040 003D9E (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: FACS 0x00000000BFFDF000 000040
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: APIC 0x00000000BFFE2E52 000090 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: SSDT 0x00000000BFFE2EE2 0000CA (v01 BOCHS  VMGENID  00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: HPET 0x00000000BFFE2FAC 000038 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: WAET 0x00000000BFFE2FE4 000028 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving FACP table memory at [mem 0xbffe2dde-0xbffe2e51]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving DSDT table memory at [mem 0xbffdf040-0xbffe2ddd]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving FACS table memory at [mem 0xbffdf000-0xbffdf03f]
```

```
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving APIC table memory at [mem 0xbffe2e52-0xbffe2ee1]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving SSDT table memory at [mem 0xbffe2ee2-0xbffe2fab]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving HPET table memory at [mem 0xbffe2fac-0xbffe2fe3]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving WAET table memory at [mem 0xbffe2fe4-0xbffe300b]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: No NUMA configuration found
--More--
[q]
```

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@redhat9 ~]# journalctl -p warning
Sep 28 15:36:59 redhat9.ittraining.loc kernel:  #3
Sep 28 15:36:59 redhat9.ittraining.loc kernel: acpi PNP0A03:00: fail to add MMCONFIG information, can't access
extended configuration space under this bridge
Sep 28 15:36:59 redhat9.ittraining.loc kernel: device-mapper: core: CONFIG_IMA_DISABLE_HTABLE is disabled.
Duplicate IMA measurements will not be recorded in the IMA log.
Sep 28 15:37:00 redhat9.ittraining.loc systemd[1]: sys-module-fuse.device: Failed to enqueue SYSTEMD_WANTS= job,
ignoring: Unit sys-fs-fuse-connections.mount not found.
Sep 28 15:37:00 redhat9.ittraining.loc kernel: sd 0:0:0:0: Power-on or device reset occurred
Sep 28 15:37:10 redhat9.ittraining.loc lvm[696]: PV /dev/sda2 online, VG rhel is complete.
Sep 28 15:37:12 redhat9.ittraining.loc avahi-daemon[752]: WARNING: No NSS support for mDNS detected, consider
installing nss-mdns!
Sep 28 15:37:16 redhat9.ittraining.loc kernel: Warning: Unmaintained driver is detected: ip_set
Sep 28 15:37:20 redhat9.ittraining.loc kernel: block dm-0: the capability attribute has been deprecated.
```

```
Sep 28 15:37:23 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: Cannot change IRQ 28 affinity: Input/output
error
Sep 28 15:37:23 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: IRQ 28 affinity is now unmanaged
Sep 28 15:37:23 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: Cannot change IRQ 30 affinity: Input/output
error
Sep 28 15:37:23 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: IRQ 30 affinity is now unmanaged
Sep 28 15:37:23 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: Cannot change IRQ 29 affinity: Input/output
error
Sep 28 15:37:23 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: IRQ 29 affinity is now unmanaged
Sep 28 15:37:23 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: Cannot change IRQ 0 affinity: Input/output
error
Sep 28 15:37:23 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: IRQ 0 affinity is now unmanaged
Sep 28 15:37:23 redhat9.ittraining.loc org.gnome.Shell.desktop[1802]: pci id for fd 13: 1234:1111, driver (null)
Sep 28 15:37:23 redhat9.ittraining.loc org.gnome.Shell.desktop[1802]: MESA-LOADER: failed to open bochs-drm:
/usr/lib64/dri/bochs-drm_dri.so: cannot open shared object file: No such file or directory (search p>
Sep 28 15:37:25 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Activating service name='org.a11y.Bus' requested by ':1.4' (uid=42 pid=1802 comm="/us>
Sep 28 15:37:25 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Successfully activated service 'org.a11y.Bus'
Sep 28 15:37:27 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Activating service name='org.freedesktop.portal.IBus' requested by ':1.6' (uid=42 pid>
Sep 28 15:37:27 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Successfully activated service 'org.freedesktop.portal.IBus'
Sep 28 15:37:27 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Activating service name='org.freedesktop.impl.portal.PermissionStore' requested by ':>
Sep 28 15:37:27 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Successfully activated service 'org.freedesktop.impl.portal.PermissionStore'
Sep 28 15:37:28 redhat9.ittraining.loc wireplumber[1859]: Failed to set scheduler settings: Operation not
permitted
Sep 28 15:37:28 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Activating service name='org.gnome.Shell.Notifications' requested by ':1.3' (uid=42 p>
Sep 28 15:37:28 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1825]: dbus-daemon[1825]: Activating
service name='org.a11y.atspi.Registry' requested by ':1.0' (uid=42 pid=1802 comm="/usr/bin/gnome-she>
Sep 28 15:37:28 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1825]: dbus-daemon[1825]: Successfully
```

```
activated service 'org.a11y.atspi.Registry'
Sep 28 15:37:28 redhat9.ittraining.loc wireplumber[1859]: GetManagedObjects() failed:
org.freedesktop.DBus.Error.NameHasNoOwner
Sep 28 15:37:28 redhat9.ittraining.loc gnome-shell[1802]: Realizing HW cursor failed: drmModeAddFB does not
support format 'AR24' (0x34325241)
Sep 28 15:37:28 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Activating service name='org.freedesktop.systemd1' requested by ':1.16' (uid=42 pid=1>
Sep 28 15:37:28 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Successfully activated service 'org.gnome.Shell.Notifications'
Sep 28 15:37:28 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Activated service 'org.freedesktop.systemd1' failed: Process org.freedesktop.systemd1>
Sep 28 15:37:28 redhat9.ittraining.loc gsd-sharing[1908]: Failed to StopUnit service:
GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process org.freedesktop.systemd1 exited with status 1
Sep 28 15:37:28 redhat9.ittraining.loc gsd-sharing[1908]: Failed to StopUnit service:
GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process org.freedesktop.systemd1 exited with status 1
Sep 28 15:37:28 redhat9.ittraining.loc gsd-sharing[1908]: Failed to StopUnit service:
GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process org.freedesktop.systemd1 exited with status 1
Sep 28 15:37:28 redhat9.ittraining.loc org.gnome.Shell.desktop[1831]: Failed to initialize glamor, falling back
to sw
Sep 28 15:37:28 redhat9.ittraining.loc gnome-shell[1802]: Realizing HW cursor failed: drmModeAddFB does not
support format 'AR24' (0x34325241)
Sep 28 15:37:29 redhat9.ittraining.loc dbus-broker[751]: A security policy denied :1.25 to send method call
/org/freedesktop/PackageKit:org.freedesktop.DBus.Properties.GetAll to :1.33.
Sep 28 15:37:29 redhat9.ittraining.loc dbus-broker[751]: A security policy denied :1.25 to send method call
/org/freedesktop/PackageKit:org.freedesktop.DBus.Properties.GetAll to :1.33.
Sep 28 15:37:29 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Activating service name='org.gnome.Shell.Screencast' requested by ':1.23' (uid=42 pid>
Sep 28 15:37:30 redhat9.ittraining.loc gnome-shell[1802]: ATK Bridge is disabled but a11y has already been
enabled.
Sep 28 15:37:30 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Activating service name='org.freedesktop.portal.IBus' requested by ':1.33' (uid=42 pi>
Sep 28 15:37:30 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Successfully activated service 'org.freedesktop.portal.IBus'
Sep 28 15:37:30 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
```

```
pid=1793] Activating service name='org.gnome.ScreenSaver' requested by ':1.25' (uid=42 pid=1928>
Sep 28 15:37:30 redhat9.ittraining.loc gsd-media-keys[1923]: Failed to grab accelerator for keybinding
settings:hibernate
Sep 28 15:37:30 redhat9.ittraining.loc gsd-media-keys[1923]: Failed to grab accelerator for keybinding
settings:playback-repeat
Sep 28 15:37:30 redhat9.ittraining.loc org.gnome.Shell.desktop[2153]: The XKEYBOARD keymap compiler (xkbcomp)
reports:
Sep 28 15:37:30 redhat9.ittraining.loc org.gnome.Shell.desktop[2153]: > Warning:          Unsupported maximum
keycode 708, clipping.
Sep 28 15:37:30 redhat9.ittraining.loc org.gnome.Shell.desktop[2153]: >                  X11 cannot support
keycodes above 255.
Sep 28 15:37:30 redhat9.ittraining.loc org.gnome.Shell.desktop[2153]: Errors from xkbcomp are not fatal to the X
server
Sep 28 15:37:30 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Successfully activated service 'org.gnome.ScreenSaver'
Sep 28 15:37:30 redhat9.ittraining.loc /usr/libexec/gdm-wayland-session[1793]: dbus-daemon[1793]: [session uid=42
pid=1793] Successfully activated service 'org.gnome.Shell.Screencast'
Sep 28 15:39:43 redhat9.ittraining.loc /usr/sbin/irqbalance[754]: Cannot change IRQ 27 affinity: Input/output
error
lines 1-55
```

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@redhat9 ~]# journalctl --since 03:45 --until now
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Linux version 5.14.0-427.37.1.el9_4.x86_64
(mockbuild@x86-64-02.build.eng.rdu2.redhat.com) (gcc (GCC) 11.4.1 20231218 (Red Hat 11.4.1-3), GNU ld version
2.35.2-43>
Sep 28 15:36:59 redhat9.ittraining.loc kernel: The list of certified hardware and cloud instances for Red Hat
Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https://catalog.redhat.com.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Command line:
BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.37.1.el9_4.x86_64 root=/dev/mapper/rhel-root ro
crashkernel=1G-4G:192M,4G-64G:256M,64G-:512M resume=/dev/>
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes,
using 'standard' format.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: signal: max sigframe size: 1776
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-provided physical RAM map:
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: BIOS-e820: [mem 0x0000000100000000-0x000000023fffffff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: NX (Execute Disable) protection: active
Sep 28 15:36:59 redhat9.ittraining.loc kernel: SMBIOS 2.8 present.
Sep 28 15:36:59 redhat9.ittraining.loc kernel: DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.1-0-
```

```
g3208b098f51a-prebuilt.qemu.org 04/01/2014
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Hypervisor detected: KVM
Sep 28 15:36:59 redhat9.ittraining.loc kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Sep 28 15:36:59 redhat9.ittraining.loc kernel: kvm-clock: using sched offset of 269552729537899 cycles
Sep 28 15:36:59 redhat9.ittraining.loc kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles:
0x1cd42e4dffb, max_idle_ns: 881590591483 ns
Sep 28 15:36:59 redhat9.ittraining.loc kernel: tsc: Detected 2099.998 MHz processor
Sep 28 15:36:59 redhat9.ittraining.loc kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 28 15:36:59 redhat9.ittraining.loc kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 28 15:36:59 redhat9.ittraining.loc kernel: last_pfn = 0x240000 max_arch_pfn = 0x400000000
Sep 28 15:36:59 redhat9.ittraining.loc kernel: MTRR map: 4 entries (3 fixed + 1 variable; max 19), built from 8
variable MTRRs
Sep 28 15:36:59 redhat9.ittraining.loc kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
Sep 28 15:36:59 redhat9.ittraining.loc kernel: last_pfn = 0xbffda max_arch_pfn = 0x400000000
Sep 28 15:36:59 redhat9.ittraining.loc kernel: found SMP MP-table at [mem 0x000f5bc0-0x000f5bcf]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Using GB pages for direct mapping
Sep 28 15:36:59 redhat9.ittraining.loc kernel: RAMDISK: [mem 0x3149c000-0x34a45fff]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Early table checksum verification disabled
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: RSDP 0x00000000000F5980 000014 (v00 BOCHS )
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: RSDT 0x00000000BFFE300C 000038 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: FACP 0x00000000BFFE2DDE 000074 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: DSDT 0x00000000BFFDF040 003D9E (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: FACS 0x00000000BFFDF000 000040
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: APIC 0x00000000BFFE2E52 000090 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: SSDT 0x00000000BFFE2EE2 0000CA (v01 BOCHS  VMGENID  00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: HPET 0x00000000BFFE2FAC 000038 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: WAET 0x00000000BFFE2FE4 000028 (v01 BOCHS  BXPC     00000001
BXPC 00000001)
```

```
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving FACP table memory at [mem 0xbffe2dde-0xbffe2e51]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving DSDT table memory at [mem 0xbffdf040-0xbffe2ddd]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving FACS table memory at [mem 0xbffdf000-0xbffdf03f]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving APIC table memory at [mem 0xbffe2e52-0xbffe2ee1]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving SSDT table memory at [mem 0xbffe2ee2-0xbffe2fab]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving HPET table memory at [mem 0xbffe2fac-0xbffe2fe3]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: ACPI: Reserving WAET table memory at [mem 0xbffe2fe4-0xbffe300b]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: No NUMA configuration found
Sep 28 15:36:59 redhat9.ittraining.loc kernel: Faking a node at [mem 0x0000000000000000-0x000000023fffffff]
Sep 28 15:36:59 redhat9.ittraining.loc kernel: NODE_DATA(0) allocated [mem 0x23ffd5000-0x23fffffff]
lines 1-55
```

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@redhat9 ~]# journalctl -f
Sep 28 15:41:02 redhat9.ittraining.loc systemd[2200]: Starting Mark boot as successful...
Sep 28 15:41:03 redhat9.ittraining.loc systemd[2200]: Finished Mark boot as successful.
Sep 28 15:42:29 redhat9.ittraining.loc PackageKit[1886]: daemon quit
Sep 28 15:42:29 redhat9.ittraining.loc systemd[1]: packagekit.service: Deactivated successfully.
Sep 28 15:43:02 redhat9.ittraining.loc systemd[1340]: Created slice User Background Tasks Slice.
Sep 28 15:43:02 redhat9.ittraining.loc systemd[1340]: Starting Cleanup of User's Temporary Files and
Directories...
Sep 28 15:43:02 redhat9.ittraining.loc systemd[1340]: Finished Cleanup of User's Temporary Files and Directories.
Sep 28 15:44:02 redhat9.ittraining.loc systemd[2200]: Created slice User Background Tasks Slice.
Sep 28 15:44:02 redhat9.ittraining.loc systemd[2200]: Starting Cleanup of User's Temporary Files and
Directories...
```

```
Sep 28 15:44:02 redhat9.ittraining.loc systemd[2200]: Finished Cleanup of User's Temporary Files and Directories.
^C
```

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@redhat9 ~]# journalctl
_AUDIT_LOGINUID=                        DBUS_BROKER_MESSAGE_TYPE=               INVOCATION_ID=
_PID=                                   _SYSTEMD_UNIT=
_AUDIT_SESSION=                         DBUS_BROKER_MESSAGE_UNIX_FDS=           JOB_ID=
PRIORITY=                               _SYSTEMD_USER_SLICE=
AVAILABLE=                              DBUS_BROKER_POLICY_TYPE=                JOB_RESULT=
REALMD_OPERATION=                       _SYSTEMD_USER_UNIT=
AVAILABLE_PRETTY=                       DBUS_BROKER_RECEIVER_SECURITY_LABEL=    JOB_TYPE=
_RUNTIME_SCOPE=                         THREAD_ID=
_BOOT_ID=                               DBUS_BROKER_RECEIVER_UNIQUE_NAME=       JOURNAL_NAME=
SEAT_ID=                                TID=
_CAP_EFFECTIVE=                         DBUS_BROKER_RECEIVER_WELL_KNOWN_NAME_0= JOURNAL_PATH=
_SELINUX_CONTEXT=                       TIMESTAMP_BOOTTIME=
_CMDLINE=                               DBUS_BROKER_SENDER_SECURITY_LABEL=      _KERNEL_DEVICE=
SESSION_ID=                             TIMESTAMP_MONOTONIC=
CODE_FILE=                              DBUS_BROKER_SENDER_UNIQUE_NAME=         _KERNEL_SUBSYSTEM=
_SOURCE_MONOTONIC_TIMESTAMP=            _TRANSPORT=
CODE_FUNC=                              DBUS_BROKER_TRANSMIT_ACTION=            KERNEL_USEC=
_SOURCE_REALTIME_TIMESTAMP=             _UDEV_DEVLINK=
CODE_LINE=                              DISK_AVAILABLE=                         LEADER=
_STREAM_ID=                             _UDEV_DEVNODE=
_COMM=                                  DISK_AVAILABLE_PRETTY=                  LIMIT=
SYSLOG_FACILITY=                        _UDEV_SYSNAME=
CURRENT_USE=                            DISK_KEEP_FREE=                         LIMIT_PRETTY=
SYSLOG_IDENTIFIER=                      _UID=
CURRENT_USE_PRETTY=                     DISK_KEEP_FREE_PRETTY=                  _MACHINE_ID=
```

```
SYSLOG_PID=                          UNIT=
DBUS_BROKER_LOG_DROPPED=             ERRNO=                                MAX_USE=
SYSLOG_RAW=                          USER_ID=
DBUS_BROKER_MESSAGE_DESTINATION=     _EXE=                                 MAX_USE_PRETTY=
SYSLOG_TIMESTAMP=                    USER_INVOCATION_ID=
DBUS_BROKER_MESSAGE_INTERFACE=       _GID=                                 MESSAGE=
_SYSTEMD_CGROUP=                     USERSPACE_USEC=
DBUS_BROKER_MESSAGE_MEMBER=          GLIB_DOMAIN=                          MESSAGE_ID=
_SYSTEMD_INVOCATION_ID=              USER_UNIT=
DBUS_BROKER_MESSAGE_PATH=            GLIB_OLD_LOG_API=                     NM_DEVICE=
_SYSTEMD_OWNER_UID=
DBUS_BROKER_MESSAGE_SERIAL=          _HOSTNAME=                            NM_LOG_DOMAINS=
_SYSTEMD_SESSION=
DBUS_BROKER_MESSAGE_SIGNATURE=       INITRD_USEC=                          NM_LOG_LEVEL=
_SYSTEMD_SLICE=
```

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@redhat9 ~]# journalctl _UID=
0     1000  172   42    70    81    994   998

[root@redhat9 ~]# journalctl _COMM=
accounts-daemon  avahi-daemon     dbus-broker-lau  geoclue          httpd            lvm_scan         polkitd
sshd             systemd-journal  udisksd
at-spi2-registr  bootctl          dbus-daemon      gnome-session-b  irqbalance       ModemManager     realmd
su               systemd-logind   wireplumber
auditctl         crond            dracut-cmdline   gnome-shell      iscsiadm         mtp-probe        rsyslogd
(systemd)        systemd-modules  wpa_supplicant
auditd           cupsd            fsck.xfs         gsd-media-keys   kdumpctl         NetworkManager   rtkit-
daemon     systemd          systemd-udevd    xkbcomp
augenrules       dbus-broker      gdm-session-wor  gsd-sharing      lvm              packagekitd      spice-
vdagent    systemd-hiberna  udevadm          Xwayland
```

LAB #6 - Le Serveur d'Horloge

6.1 - Introduction

Dans le cas d'un serveur de réseau, il est souvent important de maintenir l'heure de la machine à l'heure exacte pour des raisons de simplification de synchronisation avec des portables ou bien des systèmes de fichiers externes. Pour accomplir cette tâche, nous utilisons les services de serveurs de temps publics disponibles sur Internet sur lesquels nous synchronisons l'horloge de notre serveur. De même, les machines de notre réseau peuvent se synchroniser ensuite avec l'heure de notre serveur.

Le protocole utilisé s'appelle **NTP** (**Network Time Protocol**) qui utilise le port **123**. Celui-ci, permet la synchronisation avec plusieurs serveurs publics. Les serveurs de temps de racine s'appellent des serveurs de **Strate 1**. En dessous se trouvent des serveurs de Strate 2, Strate 3 etc..

> **Important** - La commande **ntpdate**, utilisée pour synchroniser l'horloge **sans** utiliser le démon **ntpd** est maintenant remplacée par l'option **-q** de la commande **ntp**. Lors de l'utilisation de **ntpdate**, le démon **ntpd** doit être arrêté. Si ntpdate constatait que l'erreur de l'horloge local était supérieur à 0,5 secondes, celle-ci appelait la routine **settimeofday()** tandis que si l'erreur était inférieur à 0,5 secondes, elle appelait la routine **adjtime()**.

Linux utilise le fuseau d'horaire **UTC** (*Coordinated Universal Time*) en interne. Linux doit donc être capable de traduire entre l'UTC et l'heure locale et vice versa. Linux utilise le fichier **/etc/localtime** pour connaître l'heure locale :

```
[root@redhat9 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 34 Oct 19  2023 /etc/localtime -> ../usr/share/zoneinfo/Europe/Paris
```

Ce fichier peut être un fichier ordinaire ou bien un lien symbolique pointant vers un de sfichiers dans le répertoire **/usr/share/zoneinfo** :

```
[root@redhat9 ~]# ls /usr/share/zoneinfo/
Africa      Asia       Canada   Cuba   EST      Factory  GMT+0      Hongkong  Iran         Japan
Libya   MST7MDT  Pacific   posixrules  ROC        tzdata.zi  UTC           zone.tab
America     Atlantic   CET      EET    EST5EDT  GB       GMT-0      HST       iso3166.tab  Kwajalein         MET
```

```
Navajo   Poland    PRC         ROK        UCT        WET           Zulu
Antarctica  Australia  Chile    Egypt  Etc      GB-Eire  GMT0       Iceland   Israel       leapseconds
Mexico  NZ       Portugal  PST8PDT     Singapore  Universal  W-SU
Arctic      Brazil     CST6CDT  Eire   Europe   GMT      Greenwich  Indian    Jamaica      leap-seconds.list  MST
NZ-CHAT  posix     right       Turkey     US         zone1970.tab
```

Pour connaître le fuseau d'horaire local, utilisez la commande **date** :

```
[root@redhat9 ~]# date
Sat Sep 28 03:55:32 PM CEST 2024
```

> **Important** - Vous pouvez consulter la liste des codes des zones à l'adresse **http://www.timeanddate.com/library/abbreviations/timezones/**.

Le fuseau d'horaire peut être consulté en usilisant la commande **timedatectl** :

```
[root@redhat9 ~]# timedatectl
               Local time: Sat 2024-09-28 15:57:01 CEST
           Universal time: Sat 2024-09-28 13:57:01 UTC
                 RTC time: Sat 2024-09-28 13:57:01
                Time zone: Europe/Paris (CEST, +0200)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

La commande **timedatectl** peut être utilisée pour modifier le fuseau d'horaire en utilisant l'option **set-timezone** :

```
[root@redhat9 ~]# timedatectl set-timezone America/Phoenix

[root@redhat9 ~]# timedatectl
               Local time: Sat 2024-09-28 07:05:43 MST
```

```
           Universal time: Sat 2024-09-28 14:05:43 UTC
                 RTC time: Sat 2024-09-28 14:05:43
                Time zone: America/Phoenix (MST, -0700)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no

[root@redhat9 ~]# timedatectl set-timezone Europe/Paris
[root@redhat9 ~]# timedatectl
                Local time: Sat 2024-09-28 16:06:35 CEST
           Universal time: Sat 2024-09-28 14:06:35 UTC
                 RTC time: Sat 2024-09-28 14:06:35
                Time zone: Europe/Paris (CEST, +0200)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

L'option **set-time** de la commande **timedatectl** permet de modifier l'heure du système. Le format doit être **AAAA-MM-JJ hh:mm:ss**.

Vous pouvez aussi modifier le fuseau d'horaire à l'aide de la commande **tzselect** :

```
[root@redhat9 ~]# tzselect
Please identify a location so that time zone rules can be set correctly.
Please select a continent, ocean, "coord", or "TZ".
1) Africa                                                       5) Atlantic Ocean
9) Pacific Ocean
2) Americas                                                     6) Australia
10) coord - I want to use geographical coordinates.
3) Antarctica                                                   7) Europe
11) TZ - I want to specify the timezone using the Posix TZ format.
4) Asia                                                         8) Indian Ocean
#? ^C
```

Il est est possible de modifier le fuseau d'horaire uniquement pour la session en cours et dans le shell courant :

```
[root@redhat9 ~]# date
Sat Sep 28 03:59:46 PM CEST 2024
[root@redhat9 ~]# export TZ=:/usr/share/zoneinfo/Europe/London
[root@redhat9 ~]# date
Sat Sep 28 02:59:54 PM BST 2024
[root@redhat9 ~]# export TZ=:/usr/share/zoneinfo/Europe/Paris
[root@redhat9 ~]# date
Sat Sep 28 04:00:06 PM CEST 2024
```

6.2 - Le Service chronyd

Sous RHEL 9, le serveur d'horloge n'est pas activé par défaut :

```
[root@redhat9 ~]# systemctl status chronyd
○ chronyd.service - NTP client/server
     Loaded: loaded (/usr/lib/systemd/system/chronyd.service; disabled; preset: enabled)
     Active: inactive (dead)
       Docs: man:chronyd(8)
             man:chrony.conf(5)
```

Pour activer ce serveur, utilisez l'option **set-ntp yes** de la commande **timedatectl** :

```
[root@redhat9 ~]# timedatectl set-ntp yes

[root@redhat9 ~]# timedatectl
               Local time: Sat 2024-09-28 16:53:46 CEST
           Universal time: Sat 2024-09-28 14:53:46 UTC
                 RTC time: Sat 2024-09-28 14:53:46
                Time zone: Europe/Paris (CEST, +0200)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

Vérifiez ensuite que le service **chronyd** est démarré :

```
[root@redhat9 ~]# systemctl status chronyd
● chronyd.service - NTP client/server
     Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-09-28 16:53:41 CEST; 16s ago
       Docs: man:chronyd(8)
             man:chrony.conf(5)
    Process: 2673 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 2675 (chronyd)
      Tasks: 1 (limit: 48800)
     Memory: 1.3M
        CPU: 45ms
     CGroup: /system.slice/chronyd.service
             └─2675 /usr/sbin/chronyd -F 2

Sep 28 16:53:41 redhat9.ittraining.loc systemd[1]: Starting NTP client/server...
Sep 28 16:53:41 redhat9.ittraining.loc chronyd[2675]: chronyd version 4.5 starting (+CMDMON +NTP +REFCLOCK +RTC
+PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
Sep 28 16:53:41 redhat9.ittraining.loc chronyd[2675]: Loaded 0 symmetric keys
Sep 28 16:53:41 redhat9.ittraining.loc chronyd[2675]: Using right/UTC timezone to obtain leap second data
Sep 28 16:53:41 redhat9.ittraining.loc chronyd[2675]: Loaded seccomp filter (level 2)
Sep 28 16:53:41 redhat9.ittraining.loc systemd[1]: Started NTP client/server.
Sep 28 16:53:46 redhat9.ittraining.loc chronyd[2675]: Selected source 54.39.23.64 (2.rhel.pool.ntp.org)
Sep 28 16:53:46 redhat9.ittraining.loc chronyd[2675]: System clock TAI offset set to 37 seconds
```

La commande **chronyc** permet de voir le statut de la synchronisation :

```
[root@redhat9 ~]# chronyc sources -v

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current best, '+' = combined, '-' = not combined,
| /             'x' = may be in error, '~' = too variable, '?' = unusable.
||                                                 .- xxxx [ yyyy ] +/- zzzz
```

```
||      Reachability register (octal) -.           |  xxxx = adjusted offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured offset,
||                                \     |          |  zzzz = estimated error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* 64.ip-54-39-23.net            3   7   377    54    +24us[  +35us] +/- 2831us
^- rikku.vrillusions.com         4   7   377    55   -197us[ -186us] +/-   17ms
^- rwhois.dargalsolutions.c>     2   7   377    59  -5891us[-5880us] +/-   68ms
^- ntp.pawdesigns.ca             3   6   377    55    +38us[  +49us] +/-   74ms
```

6.3 - Le Fichier /etc/chrony.conf

Le service **chronyd** maintient l'horloge matérielle locale (RTC), généralement inexacte, à la bonne heure en le synchronisant avec les serveurs NTP configurés. Si aucune connectivité réseau n'est disponible, chronyd calcule la dérive de l'horloge RTC, qui est enregistrée dans le fichier de dérive spécifié dans le fichier **/etc/chrony.conf**.

Les serveurs NTP configurés sont : **pool 2.rhel.pool.ntp.org iburst**. L'option **iburst** implique qu'après le démarrage initial du service 4 requêtes sont formulées pour une synchronisation initiale plus exacte.

Le protocole NTP utilise le port 123. Les serveurs de temps de racine s'appellent des serveurs de **Stratum 0**. En dessous se trouvent des serveurs de Stratum 1, Stratum 2, Stratum 3 etc..

```
[root@redhat9 ~]# cat /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
pool 2.rhel.pool.ntp.org iburst

# Use NTP servers from DHCP.
sourcedir /run/chrony-dhcp

# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift
```

```
# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3

# Enable kernel synchronization of the real-time clock (RTC).
rtcsync

# Enable hardware timestamping on all interfaces that support it.
#hwtimestamp *

# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2

# Allow NTP client access from local network.
#allow 192.168.0.0/16

# Serve time even if not synchronized to a time source.
#local stratum 10

# Require authentication (nts or key option) for all NTP sources.
#authselectmode require

# Specify file containing keys for NTP authentication.
keyfile /etc/chrony.keys

# Save NTS keys and cookies.
ntsdumpdir /var/lib/chrony

# Insert/delete leap seconds by slewing instead of stepping.
#leapsecmode slew

# Get TAI-UTC offset and leap seconds from the system tz database.
leapsectz right/UTC
```

```
# Specify directory for log files.
logdir /var/log/chrony

# Select which information is logged.
#log measurements statistics tracking
```

Copyright © 2024 Hugh Norris.