Dernière mise-à-jour : 2020/01/30 03:28

LSF113 - Gestion de la Journalisation

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 :

```
SLES12SP1:~ # dmesg | more
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Initializing cgroup subsys cpuacct
[    0.000000] Linux version 3.12.49-11-default (geeko@buildhost) (gcc version 4
.8.5 (SUSE Linux) ) #1 SMP Wed Nov 11 20:52:43 UTC 2015 (8d714a0)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-3.12.49-11-default root=UU
ID=65337196-2d6b-4c8b-b917-30c3867bf265 resume=/dev/sda1 splash=silent quiet sho
wopts crashkernel=104M,high
[    0.000000] e820: BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
```

```
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000006ffeffff] usable
[    0.000000] BIOS-e820: [mem 0x000000006fff0000-0x000000006fffffff] ACPI data
[    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] SMBIOS 2.5 present.
[    0.000000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/20
06
[    0.000000] Hypervisor detected: KVM
[    0.000000] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
--More--
```

Options de la Commande

Les option de cette commande sont :

```
SLES12SP1:~ # dmesg --help

Usage:
 dmesg [options]

Options:
 -C, --clear                 clear the kernel ring buffer
 -c, --read-clear            read and clear all messages
 -D, --console-off           disable printing messages to console
 -E, --console-on            enable printing messages to console
 -F, --file <file>           use the file instead of the kernel log buffer
 -f, --facility <list>       restrict output to defined facilities
 -H, --human                 human readable output
 -k, --kernel                display kernel messages
```

```
 -L, --color[=<when>]        colorize messages (auto, always or never)
 -l, --level <list>          restrict output to defined levels
 -n, --console-level <level> set level of messages printed to console
 -P, --nopager               do not pipe output into a pager
 -r, --raw                   print the raw message buffer
 -S, --syslog                force to use syslog(2) rather than /dev/kmsg
 -s, --buffer-size <size>    buffer size to query the kernel ring buffer
 -u, --userspace             display userspace messages
 -w, --follow                wait for new messages
 -x, --decode                decode facility and level to readable string
 -d, --show-delta            show time delta between printed messages
 -e, --reltime               show local time and time delta in readable format
 -T, --ctime                 show human readable timestamp
 -t, --notime                don't print messages timestamp
     --time-format <format>  show time stamp using format:
                               [delta|reltime|ctime|notime|iso]
Suspending/resume will make ctime and iso timestamps inaccurate.

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

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

Supported log levels (priorities):
   emerg - system is unusable
   alert - action must be taken immediately
```

```
    crit - critical conditions
     err - error conditions
    warn - warning conditions
  notice - normal but significant condition
    info - informational
   debug - debug-level messages


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

Surveillance Sécuritaire

La commande last

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

```
SLES12SP1:~ # last
trainee  pts/0        2.2.0.10.rev.sfr Sun Oct 15 12:06   still logged in
trainee  pts/1        2.2.0.10.rev.sfr Sun Oct 15 06:14 - 11:49  (05:34)
trainee  pts/0        2.2.0.10.rev.sfr Fri Oct 13 15:56 - 08:00 (1+16:03)
trainee  pts/0        2.2.0.10.rev.sfr Fri Oct 13 14:47 - 15:56  (01:09)
trainee  pts/0        2.2.0.10.rev.sfr Fri Oct 13 07:04 - 07:04  (00:00)
(unknown :0           :0               Fri Oct 13 06:56   still logged in
reboot   system boot  3.12.49-11-defau Fri Oct 13 06:56 - 12:08 (2+05:12)
trainee  pts/1        2.2.0.10.rev.sfr Mon Oct  9 11:53 - 11:58  (00:04)
trainee  pts/0        :0               Mon Oct  9 11:52 - 11:57  (00:05)
trainee  console      :0               Mon Oct  9 11:45 - 11:58  (00:12)
trainee  :0           :0               Mon Oct  9 11:45 - 11:58  (00:12)
(unknown :0           :0               Mon Oct  9 11:45 - 11:45  (00:00)
reboot   system boot  3.12.49-11-defau Mon Oct  9 11:44 - 11:58  (00:13)
trainee  pts/1        :0               Mon Oct  9 11:24 - 11:29  (00:04)
```

```
trainee  pts/0        :0               Mon Oct  9 11:18 - 11:30  (00:11)
trainee  console      :0               Mon Oct  9 11:17 - 11:30  (00:12)
trainee  :0           :0               Mon Oct  9 11:17 - 11:30  (00:12)
(unknown :0           :0               Mon Oct  9 11:17 - 11:17  (00:00)
reboot   system boot  3.12.49-11-defau Mon Oct  9 11:17 - 11:30  (00:13)
trainee  pts/0        :0               Tue Oct 10 13:29 - crash (-1+-2:-12)
trainee  console      :0               Tue Oct 10 13:28 - crash (-1+-2:-10)
trainee  :0           :0               Tue Oct 10 13:28 - crash (-1+-2:-10)
(unknown :0           :0               Tue Oct 10 13:26 - 13:28  (00:01)
reboot   system boot  3.12.49-11-defau Tue Oct 10 13:26 - 11:30 (-1+-1:-55)
trainee  pts/1        2.2.0.10.rev.sfr Sat Oct  7 16:47 - 18:14 (1+01:27)
trainee  pts/0        2.2.0.10.rev.sfr Sat Oct  7 16:07 - 18:12 (1+02:05)
trainee  tty1                          Sat Oct  7 16:06 - 18:14 (1+02:07)
trainee  pts/0        2.2.0.10.rev.sfr Sat Oct  7 16:01 - 16:07  (00:05)
reboot   system boot  3.12.49-11-defau Sat Oct  7 16:01 - 18:14 (1+02:13)
trainee  pts/1        10.0.2.2         Tue May  3 13:58 - crash (522+02:02)
trainee  pts/0        :0               Tue May  3 13:54 - crash (522+02:06)
trainee  console      :0               Tue May  3 13:54 - crash (522+02:06)
trainee  :0           :0               Tue May  3 13:54 - crash (522+02:06)
(unknown :0           :0               Tue May  3 13:53 - 13:54  (00:00)
reboot   system boot  3.12.49-11-defau Tue May  3 13:53 - 18:14 (523+04:21)
trainee  tty1                          Tue May  3 13:46 - 13:49  (00:02)
reboot   system boot  3.12.49-11-defau Tue May  3 13:46 - 13:49  (00:03)
reboot   system boot  3.12.49-11-defau Mon May  2 16:45 - 13:49  (21:04)
trainee  pts/1        10.0.2.2         Mon May  2 16:15 - 16:19  (00:04)
trainee  pts/0        :0               Mon May  2 16:12 - 16:19  (00:07)
trainee  console      :0               Mon May  2 16:11 - 16:19  (00:08)
trainee  :0           :0               Mon May  2 16:11 - 16:19  (00:08)
(unknown :0           :0               Mon May  2 15:56 - 16:11  (00:15)
reboot   system boot  3.12.49-11-defau Mon May  2 15:55 - 16:20  (00:24)

wtmp begins Mon May  2 15:55:45 2016
```

Options de la Commande

Les option de cette commande sont :

```
SLES12SP1:~ # last --help
last: invalid option -- '-'
Usage: last [-num | -n num] [-f file] [-t YYYYMMDDHHMMSS] [-R] [-adioxFw] [username..] [tty..]
```

La commande lastlog

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

```
SLES12SP1:~ # lastlog
Username         Port     From             Latest
at                                         **Never logged in**
bin                                        **Never logged in**
daemon                                     **Never logged in**
ftp                                        **Never logged in**
ftpsecure                                  **Never logged in**
games                                      **Never logged in**
gdm                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
man                                        **Never logged in**
messagebus                                 **Never logged in**
news                                       **Never logged in**
nobody                                     **Never logged in**
nscd                                       **Never logged in**
ntp                                        **Never logged in**
openslp                                    **Never logged in**
polkitd                                    **Never logged in**
postfix                                    **Never logged in**
```

```
pulse                                     **Never logged in**
root                                      **Never logged in**
rpc                                       **Never logged in**
rtkit                                     **Never logged in**
scard                                     **Never logged in**
sshd                                      **Never logged in**
statd                                     **Never logged in**
usbmux                                    **Never logged in**
uucp                                      **Never logged in**
vnc                                       **Never logged in**
wwwrun                                    **Never logged in**
trainee          pts/0    2.2.0.10.rev.sfr Sun Oct 15 12:06:30 +0200 2017
vboxadd                                   **Never logged in**
```

Options de la Commande

Les option de cette commande sont :

```
SLES12SP1:~ # lastlog --help
Usage: lastlog [options]

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

La Commande lastb

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

```
SLES12SP1:~ # lastb
trainee  ssh:notty    2.2.0.10.rev.sfr Sun Oct 15 12:10 - 12:10  (00:00)
trainee  ssh:notty    2.2.0.10.rev.sfr Sun Oct 15 12:10 - 12:10  (00:00)
trainee  ssh:notty    2.2.0.10.rev.sfr Sun Oct 15 12:10 - 12:10  (00:00)

btmp begins Sun Oct 15 12:10:37 2017
```

Options de la Commande

Les options de cette commande sont :

```
SLES12SP1:~ # lastb --help
lastb: invalid option -- '-'
Usage: lastb [-num | -n num] [-f file] [-t YYYYMMDDHHMMSS] [-R] [-adioxFw] [username..] [tty..]
```

Le Fichier /var/log/warn

Sous SLES ce fichier contient la journalisation des erreurs et des avertissements du système :

```
SLES12SP1:~ # tail -n 15 /var/log/warn
2017-10-13T06:56:35.294726+02:00 15 org.a11y.atspi.Registry[1482]: Xlib:  extension "XEVIE" missing on display
":0".
2017-10-13T06:56:38.677696+02:00 15 pulseaudio[1514]: [pulseaudio] sink.c: Default and alternate sample rates are
the same.
2017-10-13T06:56:38.770068+02:00 15 pulseaudio[1514]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us up to write
new data to the device, but there was actually nothing to write!
2017-10-13T06:56:38.771155+02:00 15 pulseaudio[1514]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely this is a
bug in the ALSA driver 'snd_intel8x0'. Please report this issue to the ALSA developers.
2017-10-13T06:56:38.772194+02:00 15 pulseaudio[1514]: [alsa-sink-Intel ICH] alsa-sink.c: We were woken up with
POLLOUT set -- however a subsequent snd_pcm_avail() returned 0 or another value < min_avail.
2017-10-13T14:47:06.568545+02:00 15 wickedd[814]: route ipv4 0.0.0.0/0 via 10.0.2.2 dev eth0 type unicast table
```

```
main scope universe protocol dhcp covered by a ipv4:dhcp lease
2017-10-13T16:40:03.030330+02:00 15 systemd[1]: [/etc/systemd/system/simplegateway.service:6] Not an absolute
path, ignoring: "/opt/JWrapper-Remote Access/JWAppsSharedConfig/SimpleGatewayService"
2017-10-13T17:05:37.595410+02:00 15 kernel: [ 8819.140012] e1000 0000:00:03.0 eth0: Reset adapter
2017-10-13T17:05:39.701312+02:00 15 wickedd[814]: route ipv4 0.0.0.0/0 via 10.0.2.2 dev eth0 type unicast table
main scope universe protocol dhcp covered by a ipv4:dhcp lease
2017-10-15T11:49:17.974449+02:00 SUSE12SP1 kernel: [28940.801687] ohci-pci 0000:00:06.0: bad entry 36788001
2017-10-15T12:06:22.299315+02:00 SUSE12SP1 wickedd-dhcp4[746]: unable to renew lease within renewal period;
trying to rebind
2017-10-15T12:06:22.312100+02:00 SUSE12SP1 wickedd[814]: route ipv4 0.0.0.0/0 via 10.0.2.2 dev eth0 type unicast
table main scope universe protocol dhcp covered by a ipv4:dhcp lease
2017-10-15T12:10:37.285124+02:00 15 sshd[13306]: error: PAM: Authentication failure for trainee from
2.2.0.10.rev.sfr.net
2017-10-15T12:10:40.801429+02:00 15 sshd[13306]: error: PAM: Authentication failure for trainee from
2.2.0.10.rev.sfr.net
2017-10-15T12:10:44.768756+02:00 15 sshd[13306]: error: PAM: Authentication failure for trainee from
2.2.0.10.rev.sfr.net
```

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

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

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

Sous SLES, le système audit n'est pas activé par défault :

```
SLES12SP1:~ # systemctl status auditd
auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; disabled)
```

```
   Active: inactive (dead)

SLES12SP1:~ # systemctl enable auditd
SLES12SP1:~ # systemctl start auditd
SLES12SP1:~ # systemctl status auditd
auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled)
   Active: active (running) since Sun 2017-10-15 14:18:31 CEST; 2s ago
  Process: 17114 ExecStartPost=/sbin/auditctl -R /etc/audit/audit.rules (code=exited, status=0/SUCCESS)
 Main PID: 17113 (auditd)
   CGroup: /system.slice/auditd.service
           └─17113 /sbin/auditd -n

Oct 15 14:18:31 SLES12SP1.fenetros.loc auditd[17113]: Started dispatcher: /sbin/audispd pid: 17116
Oct 15 14:18:31 SLES12SP1.fenetros.loc auditd[17113]: Init complete, auditd 2.3.6 listening for events (startup
state enable)
Oct 15 14:18:31 SLES12SP1.fenetros.loc auditctl[17114]: No rules
Oct 15 14:18:31 SLES12SP1.fenetros.loc auditctl[17114]: AUDIT_STATUS: enabled=1 flag=1 pid=17113 rate_limit=0
backlog_limit=32...log=1
Hint: Some lines were ellipsized, use -l to show in full.
```

Gestion des évènements audit

La gestion des évènements audit se repose sur trois exécutables :

auditd

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

```
SLES12SP1:~ # cat /etc/audit/auditd.conf
```

```
#
# This file controls the configuration of the audit daemon
#

log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 5
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 6
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
```

Options de la Commande

Les option de cette commande sont :

```
SLES12SP1:~ # auditd --help
auditd: invalid option -- '-'
Usage: auditd [-f] [-l] [-n] [-s disable|enable|nochange]
```

auditctl

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

```
SLES12SP1:~ # cat /etc/audit/audit.rules
# This file contains the auditctl rules that are loaded
# whenever the audit daemon is started via the initscripts.
# The rules are simply the parameters that would be passed
# to auditctl.

# First rule - delete all
-D

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

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

Options de la Commande

Les options de cette commande sont :

```
SLES12SP1:~ # auditctl --help
usage: auditctl [options]
    -a <l,a>            Append rule to end of <l>ist with <a>ction
```

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

audispd

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

```
SLES12SP1:~ # ls /etc/audisp/plugins.d
af_unix.conf  syslog.conf
```

Le contenu de ces fichiers suit un format précis :

```
SLES12SP1:~ # cat /etc/audisp/plugins.d/syslog.conf
# This file controls the configuration of the syslog plugin.
# It simply takes events and writes them to syslog. The
# arguments provided can be the default priority that you
# want the events written with. And optionally, you can give
# a second argument indicating the facility that you want events
# logged to. Valid options are LOG_LOCAL0 through 7.

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

La consultation des évènements audit

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

La commande aureport

Cette commande est utilisée pour générer des rapports :

```
SLES12SP1:~ # aureport

Summary Report
======================
Range of time in logs: 10/15/17 14:18:31.598 - 10/15/17 14:24:01.961
Selected time for report: 10/15/17 14:18:31 - 10/15/17 14:24:01.961
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 2
Number of terminals: 2
Number of host names: 1
Number of executables: 2
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 0
Number of process IDs: 8
Number of events: 44

SLES12SP1:~ # exit
logout
```

```
trainee@SLES12SP1:~> su -
Mot de passe :
su: Échec d'authentification
trainee@SLES12SP1:~> su -
Mot de passe :
SLES12SP1:~ # aureport

Summary Report
======================
Range of time in logs: 10/15/17 14:18:31.598 - 10/15/17 14:25:06.733
Selected time for report: 10/15/17 14:18:31 - 10/15/17 14:25:06.733
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 1
Number of failed authentications: 1
Number of users: 2
Number of terminals: 3
Number of host names: 1
Number of executables: 3
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 0
Number of process IDs: 12
Number of events: 58
```

Options de la Commande

Les options de cette commande sont :

```
SLES12SP1:~ # aureport --help
usage: aureport [options]
    -a,--avc            Avc report
    -au,--auth            Authentication report
    -c,--config            Config change report
    -cr,--crypto            Crypto report
    -e,--event            Event report
    -f,--file            File name report
    --failed            only failed events in report
    -h,--host            Remote Host name report
    --help                help
    -i,--interpret            Interpretive mode
    -if,--input <Input File name>    use this file as input
    --input-logs            Use the logs even if stdin is a pipe
    -l,--login            Login report
    -k,--key            Key report
    -m,--mods            Modification to accounts report
    -ma,--mac            Mandatory Access Control (MAC) report
    -n,--anomaly            aNomaly report
    -nc,--no-config            Don't include config events
    --node <node name>        Only events from a specific node
    -p,--pid            Pid report
    -r,--response            Response to anomaly report
    -s,--syscall            Syscall report
    --success            only success events in report
    --summary            sorted totals for main object in report
    -t,--log            Log time range report
    -te,--end [end date] [end time]    ending date & time for reports
    -tm,--terminal            TerMinal name report
```

```
    -ts,--start [start date] [start time]    starting data & time for reports
    --tty                Report about tty keystrokes
    -u,--user            User name report
    -v,--version            Version
    -x,--executable            eXecutable name report
    If no report is given, the summary report will be displayed
```

La commande ausearch

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

```
SLES12SP1:~ # ausearch -ui 1000 | more
----
time->Sun Oct 15 14:24:48 2017
type=USER_END msg=audit(1508070288.753:84): pid=13480 uid=1000 auid=1000 ses=448  msg='op=PAM:session_close
acct="root" exe="/usr/bin/
su" hostname=? addr=? terminal=pts/0 res=success'
----
time->Sun Oct 15 14:24:48 2017
type=CRED_DISP msg=audit(1508070288.753:85): pid=13480 uid=1000 auid=1000 ses=448  msg='op=PAM:setcred
acct="root" exe="/usr/bin/su" h
ostname=? addr=? terminal=pts/0 res=success'
----
time->Sun Oct 15 14:24:55 2017
type=USER_AUTH msg=audit(1508070295.937:86): pid=18919 uid=1000 auid=1000 ses=448  msg='op=PAM:authentication
acct="root" exe="/usr/bi
n/su" hostname=? addr=? terminal=pts/0 res=failed'
----
time->Sun Oct 15 14:25:06 2017
type=USER_AUTH msg=audit(1508070306.721:94): pid=18984 uid=1000 auid=1000 ses=448  msg='op=PAM:authentication
acct="root" exe="/usr/bi
n/su" hostname=? addr=? terminal=pts/0 res=success'
```

```
----
time->Sun Oct 15 14:25:06 2017
type=USER_ACCT msg=audit(1508070306.721:95): pid=18984 uid=1000 auid=1000 ses=448  msg='op=PAM:accounting
acct="root" exe="/usr/bin/su
" hostname=? addr=? terminal=pts/0 res=success'
----
time->Sun Oct 15 14:25:06 2017
type=CRED_ACQ msg=audit(1508070306.729:96): pid=18984 uid=1000 auid=1000 ses=448  msg='op=PAM:setcred acct="root"
exe="/usr/bin/su" ho
stname=? addr=? terminal=pts/0 res=success'
----
time->Sun Oct 15 14:25:06 2017
type=USER_START msg=audit(1508070306.733:97): pid=18984 uid=1000 auid=1000 ses=448  msg='op=PAM:session_open
acct="root" exe="/usr/bin
/su" hostname=? addr=? terminal=pts/0 res=success'
```

Options de la Commande

Les options de cette commande sont :

```
SLES12SP1:~ # ausearch --help
usage: ausearch [options]
    -a,--event <Audit event id>    search based on audit event id
    --arch <CPU>            search based on the CPU architecture
    -c,--comm  <Comm name>        search based on command line name
    --checkpoint <checkpoint file>    search from last complete event
    --debug            Write malformed events that are skipped to stderr
    -e,--exit  <Exit code or errno>    search based on syscall exit code
    -f,--file  <File name>        search based on file name
    -ga,--gid-all <all Group id>    search based on All group ids
    -ge,--gid-effective <effective Group id>  search based on Effective
                    group id
    -gi,--gid <Group Id>        search based on group id
```

```
-h,--help            help
-hn,--host <Host Name>        search based on remote host name
-i,--interpret            Interpret results to be human readable
-if,--input <Input File name>    use this file instead of current logs
--input-logs            Use the logs even if stdin is a pipe
--just-one            Emit just one event
-k,--key  <key string>        search based on key field
-l, --line-buffered        Flush output on every line
-m,--message  <Message type>    search based on message type
-n,--node  <Node name>        search based on machine's name
-o,--object  <SE Linux Object context> search based on context of object
-p,--pid  <Process id>        search based on process id
-pp,--ppid <Parent Process id>    search based on parent process id
-r,--raw            output is completely unformatted
-sc,--syscall <SysCall name>    search based on syscall name or number
-se,--context <SE Linux context> search based on either subject or
                 object
--session <login session id>    search based on login session id
-su,--subject <SE Linux context> search based on context of the Subject
-sv,--success <Success Value>    search based on syscall or event
                success value
-te,--end [end date] [end time]    ending date & time for search
-ts,--start [start date] [start time]    starting data & time for search
-tm,--terminal <TerMinal>    search based on terminal
-ua,--uid-all <all User id>    search based on All user id's
-ue,--uid-effective <effective User id>  search based on Effective
                user id
-ui,--uid <User Id>        search based on user id
-ul,--loginuid <login id>    search based on the User's Login id
-uu,--uuid <guest UUID>        search for events related to the virtual
                machine with the given UUID.
-v,--version            version
-vm,--vm-name <guest name>    search for events related to the virtual
                machine with the name.
```

```
    -w,--word            string matches are whole word
    -x,--executable <executable name>  search based on executable name
```

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

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

Les traces brutes utilisées par les commandes **ausearch** et **aureport** sont stockées dans le fichier **/var/log/audit/audit.log** :

```
SLES12SP1:~ # cat /var/log/audit/audit.log | grep failed
type=USER_AUTH msg=audit(1508070295.937:86): pid=18919 uid=1000 auid=1000 ses=448  msg='op=PAM:authentication
acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=pts/0 res=failed'
```

Le fichier /var/log/messages

Ce fichier contient la plupart des messages du système :

```
SLES12SP1:~ # tail -n 15 /var/log/messages
2017-10-15T14:30:01.341755+02:00 15 CRON[20417]: pam_unix(crond:session): session closed for user trainee
2017-10-15T14:30:01.377761+02:00 15 systemd: pam_unix(systemd-user:session): session opened for user root by
(uid=0)
2017-10-15T14:30:01.533004+02:00 15 CRON[20416]: pam_unix(crond:session): session closed for user root
2017-10-15T14:30:01.605902+02:00 15 systemd: pam_unix(systemd-user:session): session closed for user root
2017-10-15T14:30:01.909165+02:00 15 sh[1557]: Sleeping '1250' '1250'
2017-10-15T14:30:58.736868+02:00 15 sh[1557]: message repeated 8 times: [ Sleeping '1250' '1250']
2017-10-15T14:31:01.552723+02:00 15 cron[20721]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
```

```
2017-10-15T14:31:01.573635+02:00 15 CRON[20722]: (trainee) CMD (/bin/pwd > pwd.txt)
2017-10-15T14:31:01.583659+02:00 15 CRON[20721]: pam_unix(crond:session): session closed for user trainee
2017-10-15T14:31:05.839672+02:00 15 sh[1557]: Sleeping '1250' '1250'
2017-10-15T14:31:55.559977+02:00 15 sh[1557]: message repeated 7 times: [ Sleeping '1250' '1250']
2017-10-15T14:32:01.602394+02:00 15 cron[21002]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
2017-10-15T14:32:01.626472+02:00 15 CRON[21004]: (trainee) CMD (/bin/pwd > pwd.txt)
2017-10-15T14:32:01.636669+02:00 15 CRON[21002]: pam_unix(crond:session): session closed for user trainee
2017-10-15T14:32:02.666112+02:00 15 sh[1557]: Sleeping '1250' '1250'
```

Applications

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

- YaST2,
- cups,
- samba.

```
SLES12SP1:~ # ls -l /var/log
total 4796
-rw-r----- 1 root root       0 May  1  2016 NetworkManager
-rw-r--r-- 1 root root      48 Oct  9 11:29 VBoxGuestAdditions.log
-rw-r--r-- 1 root root   35347 Oct 15 11:49 Xorg.0.log
-rw-r--r-- 1 root root   39235 Oct  9 11:58 Xorg.0.log.old
drwx------ 1 root root     402 Oct  9 11:48 YaST2
-rw-r----- 1 root root       0 May  1  2016 acpid
-rw-r--r-- 1 root root    9854 May  1  2016 alternatives.log
drwxr-xr-x 1 root root       0 Aug 21  2015 apparmor
drwx------ 1 root root      18 Oct 15 14:18 audit
-rw-r--r-- 1 root root    9749 Oct 13 06:56 boot.log
-rw------- 1 root root    1536 Oct 15 14:24 btmp
drwxr-xr-x 1 lp   lp         0 Jun 10  2015 cups
```

```
lrwxrwxrwx 1 root root      10 May  1  2016 dump -> /var/crash
-rw------- 1 root root   32160 Oct 10 13:30 faillog
-rw-r----- 1 root root       0 May  1  2016 firewall
drwx--x--x 1 root gdm      232 Oct 13 06:56 gdm
drwx------ 1 root root       0 Oct 30  2015 krb5
-rw-r--r-- 1 root root  293460 Oct 15 12:10 lastlog
-rw-r----- 1 root root    1908 Oct 13 06:56 mail
-rw-r----- 1 root root     120 May  2  2016 mail.err
-rw-r----- 1 root root    1908 Oct 13 06:56 mail.info
-rw-r----- 1 root root     120 May  2  2016 mail.warn
-rw-r----- 1 root root 1185566 Oct 15 14:32 messages
drwxr-x--- 1 news news      56 May  1  2016 news
-rw-r--r-- 1 root root       0 May  1  2016 ntp
-rw------- 1 root root  243992 May  1  2016 pbl.log
-rw-r----- 1 root root  290429 Oct  9 11:18 pk_backend_zypp
drwxr-x--- 1 root root       0 Nov 12  2015 samba
-rw-r----- 1 root root   38081 Oct 15 06:16 snapper.log
drwx------ 1 root root       0 Sep 23  2014 speech-dispatcher
-rw-r--r-- 1 root root      73 Oct 13 06:56 vboxadd-install-x11.log
-rw-r--r-- 1 root root  235259 Oct  9 11:29 vboxadd-install.log
-rw-r--r-- 1 root root   86709 Oct 15 14:18 warn
-rw-rw-r-- 1 root utmp   44928 Oct 15 12:10 wtmp
drwxr-xr-x 1 root root      14 Nov 12  2015 zypp
-rw-r----- 1 root root 2595962 Oct 13 16:15 zypper.log
```

rsyslog

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

rsyslog apporte des améliorations par rapport à syslogd :

- l'addition du protocole **TCP** pour la communication,

- la haute disponibilité,
- l'utilisation des bases de données au format MySQL et PostgreSQL pour stocker des journaux.

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

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

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

Sous SLES, le daemon rsyslog est configuré par l'édition du fichier **/etc/sysconfig/syslog** :

```
SLES12SP1:~ # cat /etc/sysconfig/syslog
## Type:           string
## Default:        ""
## Config:         ""
## ServiceRestart: syslog
#
# Parameters for rsyslogd, except of the version compatibility (-c)
# and the config file (-f), because they're used by sysconfig and
# earlysysconfig init scripts.
#
# See also the RSYSLOGD_COMPAT_VERSION variable in this file, the
# documentation provided in /usr/share/doc/packages/rsyslog/doc by
# the rsyslog-doc package and the rsyslogd(8) and rsyslog.conf(5)
# manual pages.
#
RSYSLOGD_PARAMS=""
```

La directive **RSYSLOGD_COMPAT_VERSION** qui peut se trouver dans ce fichier spécifie la version de rsyslog à utiliser :

Directive	Version
RSYSLOGD_COMPAT_VERSION=“”	Mode natif - aucune compatibilité avec une version précédente
RSYSLOGD_COMPAT_VERSION=“2”	rsyslog V2 - mode compatibilité avec la version indiquée

La directive **RSYSLOGD_NATIVE_VERSION** spécifie la version native de rsyslog à utiliser quand la valeur de la directive RSYSLOGD_COMPAT_VERSION est vide :

Directive	Version
RSYSLOGD_NATIVE_VERSION=“5”	rsyslog V5

Priorités

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

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

Sous-systèmes applicatifs

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

Fonction	Description
auth/auth-priv	Message de sécurité / autorisation
cron	Message de cron ou at
daemon	Message d'un daemon

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

/etc/rsyslog.conf

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

```
SLES12SP1:~ # cat /etc/rsyslog.conf
##
## === When you're using remote logging, enable on-disk queues ===
## === in rsyslog.d/remote.conf. When neccesary also set the   ===
## === SYSLOG_REQUIRES_NETWORK=yes in /etc/sysconfig/syslog,   ===
## === e.g. when rsyslog has to receive on a specific IP only. ===
##
## Note, that when the MYSQL, PGSQL, GSSAPI, GnuTLS or SNMP modules
## (provided in separate rsyslog-module-* packages) are enabled, the
## configuration can't be used on a system with /usr on a remote
## filesystem, except on newer systems where initrd mounts /usr.
```

```
## [The modules are linked against libraries installed bellow of
##  /usr thus also installed in /usr/lib*/rsyslog because of this.]
##

#
# if you experience problems, check
# http://www.rsyslog.com/troubleshoot for assistance
# and report them at http://bugzilla.novell.com/
#

# since rsyslog v3: load input modules
# If you do not load inputs, nothing happens!

# provides --MARK-- message capability (every 1 hour)
$ModLoad immark.so
$MarkMessagePeriod      3600

# provides support for local system logging (e.g. via logger command)
$ModLoad imuxsock.so

# reduce dupplicate log messages (last message repeated n times)
$RepeatedMsgReduction   on

# kernel logging (may be also provided by /sbin/klogd)
# see also http://www.rsyslog.com/doc-imklog.html.
$ModLoad imklog.so
# set log level 1 (same as in /etc/sysconfig/syslog).
$klogConsoleLogLevel    1

# Use rsyslog native, rfc5424 conform log format as default
# ($ActionFileDefaultTemplate RSYSLOG_FileFormat).
#
# To change a single file to use obsolete BSD syslog format
# (rfc 3164, no high-precision timestamps), set the variable
```

```
# bellow or append ";RSYSLOG_FileFormat" to the filename.
# See
#   http://www.rsyslog.com/doc/rsyslog_conf_templates.html
# for more informations.
#
#$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

#
# Include config generated by /etc/init.d/syslog script
# using the SYSLOGD_ADDITIONAL_SOCKET* variables in the
# /etc/sysconfig/syslog file.
#
$IncludeConfig /run/rsyslog/additional-log-sockets.conf

#
# Include config files, that the admin provided? :
#
$IncludeConfig /etc/rsyslog.d/*.conf


###
# print most important on tty10 and on the xconsole pipe
#
if  ( \
        /* kernel up to warning except of firewall  */ \
        ($syslogfacility-text == 'kern')      and      \
        ($syslogseverity <= 4 /* warning */ ) and not  \
        ($msg contains 'IN=' and $msg contains 'OUT=') \
    ) or ( \
        /* up to errors except of facility authpriv */ \
        ($syslogseverity <= 3 /* errors  */ ) and not  \
        ($syslogfacility-text == 'authpriv')           \
    ) \
then {
```

```
    /dev/tty10
    |/dev/xconsole
}



# Emergency messages to everyone logged on (wall)
*.emerg                  :omusrmsg:*

# enable this, if you want that root is informed
# immediately, e.g. of logins
#*.alert                root



#
# firewall messages into separate file and stop their further processing
#
if  ($syslogfacility-text == 'kern') and \
    ($msg contains 'IN=' and $msg contains 'OUT=') \
then {
    -/var/log/firewall
    stop
}



#
# acpid messages into separate file and stop their further processing
#
# => all acpid messages for debuging (uncomment if needed):
#if ($programname == 'acpid' or $syslogtag == '[acpid]:') then \
#   -/var/log/acpid
#
# => up to notice (skip info and debug)
if  ($programname == 'acpid' or $syslogtag == '[acpid]:') and \
    ($syslogseverity <= 5 /* notice */) \
```

```
then {
    -/var/log/acpid
    stop
}



#
# NetworkManager into separate file and stop their further processing
#
if      ($programname == 'NetworkManager') or \
    ($programname startswith 'nm-') \
then {
    -/var/log/NetworkManager
    stop
}



#
# email-messages
#
mail.*                  -/var/log/mail
mail.info               -/var/log/mail.info
mail.warning                -/var/log/mail.warn
mail.err                 /var/log/mail.err



#
# news-messages
#
news.crit               -/var/log/news/news.crit
news.err                -/var/log/news/news.err
news.notice             -/var/log/news/news.notice
# enable this, if you want to keep all news messages
# in one file
```

```
#news.*                 -/var/log/news.all


#
# Warnings in one file
#
*.=warning;*.=err           -/var/log/warn
*.crit                   /var/log/warn


#
# the rest in one file
#
*.*;mail.none;news.none         -/var/log/messages


#
# enable this, if you want to keep all messages
# in one file
#*.*                    -/var/log/allmessages


#
# Some foreign boot scripts require local7
#
local0.*;local1.*           -/var/log/localmessages
local2.*;local3.*           -/var/log/localmessages
local4.*;local5.*           -/var/log/localmessages
local6.*;local7.*           -/var/log/localmessages

###
```

ainsi que par le fichier **/etc/rsyslog.d/remote.conf** :

```
SLES12SP1:~ # cat /etc/rsyslog.d/remote.conf
##
## === When you're using remote logging, enable on-disk queues ===
## === in rsyslog.d/remote.conf. When neccesary also set the   ===
## === SYSLOG_REQUIRES_NETWORK=yes in /etc/sysconfig/syslog,   ===
## === e.g. when rsyslog has to receive on a specific IP only. ===
##
## Note, that when the MYSQL, PGSQL, GSSAPI, GnuTLS or SNMP modules
## (provided in separate rsyslog-module-* packages) are enabled, the
## configuration can't be used on a system with /usr on a remote
## filesystem, except on newer systems where initrd mounts /usr.
## [The modules are linked against libraries installed bellow of
##  /usr thus also installed in /usr/lib*/rsyslog because of this.]
##

# ######### Enable On-Disk queues for remote logging ##########
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#
#$WorkDirectory /var/spool/rsyslog # where to place spool files
#$ActionQueueFileName uniqName # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down

# ######### Sending Messages to Remote Hosts ##########

# Remote Logging using TCP for reliable delivery
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host

# Remote Logging using UDP
```

```
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @remote-host


# ######### Receiving Messages from Remote Hosts ##########
# TCP Syslog Server:
# provides TCP syslog reception and GSS-API (if compiled to support it)
#$ModLoad imtcp.so         # load module
##$UDPServerAddress 10.10.0.1 # force to listen on this IP only,
##                           # needs SYSLOG_REQUIRES_NETWORK=yes.
#$InputTCPServerRun <port> # Starts a TCP server on selected port

# UDP Syslog Server:
#$ModLoad imudp.so         # provides UDP syslog reception
##$UDPServerAddress 10.10.0.1 # force to listen on this IP only,
##                           # needs SYSLOG_REQUIRES_NETWORK=yes.
#$UDPServerRun 514         # start a UDP syslog server at standard port 514


########### Encrypting Syslog Traffic with TLS ##########
# -- TLS Syslog Server:
## make gtls driver the default
#$DefaultNetstreamDriver gtls
#
## certificate files
#$DefaultNetstreamDriverCAFile /etc/rsyslog.d/ca.pem
#$DefaultNetstreamDriverCertFile /etc/rsyslog.d/server_cert.pem
#$DefaultNetstreamDriverKeyFile /etc/rsyslog.d/server_key.pem
#
#$ModLoad imtcp # load TCP listener
#
#$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
#$InputTCPServerStreamDriverAuthMode anon # client is NOT authenticated
#$InputTCPServerRun 10514 # start up listener at port 10514
```

```
#
# -- TLS Syslog Client:
## certificate files - just CA for a client
#$DefaultNetstreamDriverCAFile /etc/rsyslog.d/ca.pem
#
## set up the action
#$DefaultNetstreamDriver gtls # use gtls netstream driver
#$ActionSendStreamDriverMode 1 # require TLS for the connection
#$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
#*.* @@(o)server.example.net:10514 # send (all) messages
```

Modules

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

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

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

```
...
# since rsyslog v3: load input modules
# If you do not load inputs, nothing happens!

# provides --MARK-- message capability (every 1 hour)
$ModLoad immark.so
$MarkMessagePeriod      3600
```

```
# provides support for local system logging (e.g. via logger command)
$ModLoad imuxsock.so

# reduce dupplicate log messages (last message repeated n times)
$RepeatedMsgReduction   on

# kernel logging (may be also provided by /sbin/klogd)
# see also http://www.rsyslog.com/doc-imklog.html.
$ModLoad imklog.so
# set log level 1 (same as in /etc/sysconfig/syslog).
$klogConsoleLogLevel    1

# Use rsyslog native, rfc5424 conform log format as default
# ($ActionFileDefaultTemplate RSYSLOG_FileFormat).
#
# To change a single file to use obsolete BSD syslog format
# (rfc 3164, no high-precision timestamps), set the variable
# bellow or append ";RSYSLOG_FileFormat" to the filename.
# See
#   http://www.rsyslog.com/doc/rsyslog_conf_templates.html
# for more informations.
#
#$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
...
```

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.d/remote.conf** et de re-démarrer le service :

```
...
# ######### Receiving Messages from Remote Hosts ##########
# TCP Syslog Server:
# provides TCP syslog reception and GSS-API (if compiled to support it)
#$ModLoad imtcp.so         # load module
##$UDPServerAddress 10.10.0.1 # force to listen on this IP only,
```

```
##                            # needs SYSLOG_REQUIRES_NETWORK=yes.
#$InputTCPServerRun <port> # Starts a TCP server on selected port

# UDP Syslog Server:
#$ModLoad imudp.so         # provides UDP syslog reception
##$UDPServerAddress 10.10.0.1 # force to listen on this IP only,
##                            # needs SYSLOG_REQUIRES_NETWORK=yes.
#$UDPServerRun 514         # start a UDP syslog server at standard port 514
...
```

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

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

```
...
# ######### Sending Messages to Remote Hosts ##########

# Remote Logging using TCP for reliable delivery
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host

# Remote Logging using UDP
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @remote-host
...
```

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

Directives Globales

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

```
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
```

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

Règles

Chaque règle prend la forme suivante :

```
Sélecteur[; ...]  [-] Action
```

Un Sélecteur est défini d'une des façons suivantes :

Sous-système applicatif.Priorité

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

Sous-système applicatif!Priorité

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

Sous-système applicatif=Priorité

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

L'utilisation du caractère spécial *

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

n Sous-systèmes avec la même priorité

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

n Sélecteurs avec la même Action

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

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

/usr/bin/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 :

```
SLES12SP1:~ # logger -p user.info Linux est super
```

Consultez la fin de votre syslog :

```
SLES12SP1:~ # tail /var/log/messages
2017-10-15T15:02:01.764277+02:00 15 CRON[29563]: pam_unix(crond:session): session closed for user trainee
2017-10-15T15:02:07.252694+02:00 15 sh[1557]: Sleeping '1250' '1250'
2017-10-15T15:02:56.983435+02:00 15 sh[1557]: message repeated 7 times: [ Sleeping '1250' '1250']
2017-10-15T15:03:01.784426+02:00 15 cron[29835]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
2017-10-15T15:03:01.804874+02:00 15 CRON[29836]: (trainee) CMD (/bin/pwd > pwd.txt)
2017-10-15T15:03:01.814994+02:00 15 CRON[29835]: pam_unix(crond:session): session closed for user trainee
2017-10-15T15:03:04.084314+02:00 15 sh[1557]: Sleeping '1250' '1250'
2017-10-15T15:03:18.298428+02:00 15 sh[1557]: message repeated 2 times: [ Sleeping '1250' '1250']
2017-10-15T15:03:22.432980+02:00 15 trainee: Linux est super
2017-10-15T15:03:25.397972+02:00 15 sh[1557]: Sleeping '1250' '1250'
```

Options de la commande

Les options de la commande logger sont :

```
SLES12SP1:~ # logger --help

Usage:
 logger [options] [<message>]

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

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

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

/usr/sbin/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** ainsi que les fichiers dans **/etc/logrotate.d** :

```
SLES12SP1:~ # cat /etc/logrotate.conf
```

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

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

# use date as a suffix of the rotated file
dateext

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

# comment these to switch compression to use gzip or another
# compression scheme
compresscmd /usr/bin/xz
uncompresscmd /usr/bin/xzdec

# former versions had to have the compressext set accordingly
#compressext .xz

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

Dans 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.

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

Options de la commande

Les options de la commande logrotate sont :

```
SLES12SP1:~ # logrotate --help
Usage: logrotate [OPTION...] <configfile>
  -d, --debug               Don't do anything, just test (implies -v)
  -f, --force               Force file rotation
  -m, --mail=command        Command to send mail (instead of `/bin/mail')
  -s, --state=statefile     Path of state file
  -v, --verbose             Display messages during rotation
      --version             Display version information

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

La Journalisation avec journald

Sous SLES 12, 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** :

```
SLES12SP1:~ # ls -l /run/log/journal/
total 0
drwxr-sr-x 2 root systemd-journal 60 Oct 13 06:56 cb3d6e8d47dd4526b350676d48eb3e24
```

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

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

```
SLES12SP1:~ # mkdir /var/log/journal
SLES12SP1:~ # ls -l /var/log/journal/
total 0
SLES12SP1:~ # systemctl restart systemd-journald
SLES12SP1:~ # ls -l /run/log/journal/
ls: cannot access /run/log/journal/: No such file or directory
SLES12SP1:~ # ls -l /var/log/journal/
total 0
drwxr-xr-x 1 root root 28 Oct 15 15:09 cb3d6e8d47dd4526b350676d48eb3e24
```

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

```
SLES12SP1:~ # 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.
#
# See journald.conf(5) for details

[Journal]
#Storage=auto
```

```
#Compress=yes
#Seal=yes
#SplitMode=login
#SyncIntervalSec=5m
#RateLimitInterval=30s
#RateLimitBurst=1000
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize=
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#TTYPath=/dev/tty10
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
```

Consultation des Journaux

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

```
SLES12SP1:~ # journalctl
-- Logs begin at Fri 2017-10-13 06:56:12 CEST, end at Sun 2017-10-15 15:10:01 CEST. --
Oct 13 06:56:12 linux-9gh3 systemd-journal[96]: Runtime journal is using 8.0M (max allowed 82.3M, trying to leave
123.5M free of 815.6
Oct 13 06:56:12 linux-9gh3 systemd-journal[96]: Runtime journal is using 8.0M (max allowed 82.3M, trying to leave
123.5M free of 815.6
```

```
Oct 13 06:56:12 linux-9gh3 kernel: Initializing cgroup subsys cpuset
Oct 13 06:56:12 linux-9gh3 kernel: Initializing cgroup subsys cpu
Oct 13 06:56:12 linux-9gh3 kernel: Initializing cgroup subsys cpuacct
Oct 13 06:56:12 linux-9gh3 kernel: Linux version 3.12.49-11-default (geeko@buildhost) (gcc version 4.8.5 (SUSE
Linux) ) #1 SMP Wed Nov
Oct 13 06:56:12 linux-9gh3 kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-3.12.49-11-default
root=UUID=65337196-2d6b-4c8b-b917-30c3867
Oct 13 06:56:12 linux-9gh3 kernel: e820: BIOS-provided physical RAM map:
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x0000000000100000-0x000000006ffeffff] usable
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x000000006fff0000-0x000000006fffffff] ACPI data
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: NX (Execute Disable) protection: active
Oct 13 06:56:12 linux-9gh3 kernel: SMBIOS 2.5 present.
Oct 13 06:56:12 linux-9gh3 kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 13 06:56:12 linux-9gh3 kernel: Hypervisor detected: KVM
Oct 13 06:56:12 linux-9gh3 kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 13 06:56:12 linux-9gh3 kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 13 06:56:12 linux-9gh3 kernel: No AGP bridge found
Oct 13 06:56:12 linux-9gh3 kernel: e820: last_pfn = 0x6fff0 max_arch_pfn = 0x400000000
Oct 13 06:56:12 linux-9gh3 kernel: MTRR default type: uncachable
Oct 13 06:56:12 linux-9gh3 kernel: MTRR variable ranges disabled:
Oct 13 06:56:12 linux-9gh3 kernel: x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
Oct 13 06:56:12 linux-9gh3 kernel: CPU MTRRs all blank - virtualized system.
Oct 13 06:56:12 linux-9gh3 kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff] mapped at [ffff88000009fff0]
Oct 13 06:56:12 linux-9gh3 kernel: Scanning 1 areas for low memory corruption
Oct 13 06:56:12 linux-9gh3 kernel: Base memory trampoline at [ffff880000099000] 99000 size 24576
Oct 13 06:56:12 linux-9gh3 kernel: init_memory_mapping: [mem 0x00000000-0x000fffff]
Oct 13 06:56:12 linux-9gh3 kernel:  [mem 0x00000000-0x000fffff] page 4k
Oct 13 06:56:12 linux-9gh3 kernel: BRK [0x02195000, 0x02195fff] PGTABLE
```

```
lines 1-35
```

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

Consultation des Journaux d'une Application Spécifique

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

```
SLES12SP1:~ # journalctl /usr/sbin/anacron
-- Logs begin at Fri 2017-10-13 06:56:12 CEST, end at Sun 2017-10-15 15:11:01 CEST. --
Oct 13 17:00:01 SLES12SP1.fenestros.loc anacron[10298]: Anacron started on 2017-10-13
Oct 13 17:00:01 SLES12SP1.fenestros.loc anacron[10298]: Will run job `cron.daily' in 41 min.
Oct 13 17:00:01 SLES12SP1.fenestros.loc anacron[10298]: Will run job `cron.weekly' in 61 min.
Oct 13 17:00:01 SLES12SP1.fenestros.loc anacron[10298]: Will run job `cron.monthly' in 81 min.
Oct 13 17:00:01 SLES12SP1.fenestros.loc anacron[10298]: Jobs will be executed sequentially
Oct 15 06:15:01 SUSE12SP1.fenestros.loc anacron[12477]: Anacron started on 2017-10-15
Oct 15 06:15:01 SUSE12SP1.fenestros.loc anacron[12477]: Job `cron.daily' locked by another anacron - skipping
Oct 15 06:15:01 SUSE12SP1.fenestros.loc anacron[12477]: Job `cron.weekly' locked by another anacron - skipping
Oct 15 06:15:01 SUSE12SP1.fenestros.loc anacron[12477]: Job `cron.monthly' locked by another anacron - skipping
Oct 15 06:15:01 SUSE12SP1.fenestros.loc anacron[12477]: Normal exit (0 jobs run)
Oct 15 06:49:20 SUSE12SP1.fenestros.loc anacron[10298]: Job `cron.daily' started
Oct 15 06:49:20 SUSE12SP1.fenestros.loc anacron[10298]: Job `cron.daily' terminated
Oct 15 06:49:20 SUSE12SP1.fenestros.loc anacron[10298]: Job `cron.weekly' started
Oct 15 06:49:20 SUSE12SP1.fenestros.loc anacron[10298]: Job `cron.weekly' terminated
Oct 15 06:49:20 SUSE12SP1.fenestros.loc anacron[10298]: Job `cron.monthly' started
Oct 15 06:49:20 SUSE12SP1.fenestros.loc anacron[10298]: Job `cron.monthly' terminated
Oct 15 06:49:20 SUSE12SP1.fenestros.loc anacron[10298]: Normal exit (3 jobs run)
Oct 15 07:15:01 SUSE12SP1.fenestros.loc anacron[31311]: Anacron started on 2017-10-15
```

```
Oct 15 07:15:01 SUSE12SP1.fenestros.loc anacron[31311]: Will run job `cron.daily' in 9 min.
Oct 15 07:15:01 SUSE12SP1.fenestros.loc anacron[31311]: Jobs will be executed sequentially
Oct 15 07:24:01 SUSE12SP1.fenestros.loc anacron[31311]: Job `cron.daily' started
Oct 15 07:24:01 SUSE12SP1.fenestros.loc anacron[31311]: Job `cron.daily' terminated
Oct 15 07:24:01 SUSE12SP1.fenestros.loc anacron[31311]: Normal exit (1 job run)
```

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 :

```
SLES12SP1:~ # journalctl -b | more
-- Logs begin at Fri 2017-10-13 06:56:12 CEST, end at Sun 2017-10-15 15:11:01 CEST. --
Oct 13 06:56:12 linux-9gh3 systemd-journal[96]: Runtime journal is using 8.0M (max allowed 82.3M, trying to leave
123.5M free of 815.6
M available → current limit 82.3M).
Oct 13 06:56:12 linux-9gh3 systemd-journal[96]: Runtime journal is using 8.0M (max allowed 82.3M, trying to leave
123.5M free of 815.6
M available → current limit 82.3M).
Oct 13 06:56:12 linux-9gh3 kernel: Initializing cgroup subsys cpuset
Oct 13 06:56:12 linux-9gh3 kernel: Initializing cgroup subsys cpu
Oct 13 06:56:12 linux-9gh3 kernel: Initializing cgroup subsys cpuacct
Oct 13 06:56:12 linux-9gh3 kernel: Linux version 3.12.49-11-default (geeko@buildhost) (gcc version 4.8.5 (SUSE
Linux) ) #1 SMP Wed Nov
 11 20:52:43 UTC 2015 (8d714a0)
Oct 13 06:56:12 linux-9gh3 kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-3.12.49-11-default
root=UUID=65337196-2d6b-4c8b-b917-30c3867
bf265 resume=/dev/sda1 splash=silent quiet showopts crashkernel=104M,high
Oct 13 06:56:12 linux-9gh3 kernel: e820: BIOS-provided physical RAM map:
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x0000000000100000-0x000000006ffeffff] usable
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x000000006fff0000-0x000000006fffffff] ACPI data
```

```
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 13 06:56:12 linux-9gh3 kernel: NX (Execute Disable) protection: active
Oct 13 06:56:12 linux-9gh3 kernel: SMBIOS 2.5 present.
Oct 13 06:56:12 linux-9gh3 kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Oct 13 06:56:12 linux-9gh3 kernel: Hypervisor detected: KVM
Oct 13 06:56:12 linux-9gh3 kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Oct 13 06:56:12 linux-9gh3 kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Oct 13 06:56:12 linux-9gh3 kernel: No AGP bridge found
Oct 13 06:56:12 linux-9gh3 kernel: e820: last_pfn = 0x6fff0 max_arch_pfn = 0x400000000
Oct 13 06:56:12 linux-9gh3 kernel: MTRR default type: uncachable
Oct 13 06:56:12 linux-9gh3 kernel: MTRR variable ranges disabled:
Oct 13 06:56:12 linux-9gh3 kernel: x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
Oct 13 06:56:12 linux-9gh3 kernel: CPU MTRRs all blank - virtualized system.
Oct 13 06:56:12 linux-9gh3 kernel: found SMP MP-table at [mem 0x0009fff0-0x0009ffff] mapped at [ffff88000009fff0]
Oct 13 06:56:12 linux-9gh3 kernel: Scanning 1 areas for low memory corruption
--More--
```

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 :

```
SLES12SP1:~ # journalctl -p warning
-- Logs begin at Fri 2017-10-13 06:56:12 CEST, end at Sun 2017-10-15 15:13:01 CEST. --
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: RSDP 0x00000000000E0000 00024 (v02 VBOX  )
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: XSDT 0x000000006FFF0030 0003C (v01 VBOX   VBOXXSDT 00000001 ASL
00000061)
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: FACP 0x000000006FFF00F0 000F4 (v04 VBOX   VBOXFACP 00000001 ASL
00000061)
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: DSDT 0x000000006FFF0470 021C8 (v02 VBOX   VBOXBIOS 00000002 INTL
20160831)
```

```
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: FACS 0x000000006FFF0200 00040
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: APIC 0x000000006FFF0240 00054 (v02 VBOX   VBOXAPIC 00000001 ASL
00000061)
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: SSDT 0x000000006FFF02A0 001CC (v01 VBOX   VBOXCPUT 00000002 INTL
20160831)
Oct 13 06:56:12 linux-9gh3 kernel: Zone ranges:
Oct 13 06:56:12 linux-9gh3 kernel:   DMA      [mem 0x00001000-0x00ffffff]
Oct 13 06:56:12 linux-9gh3 kernel:   DMA32    [mem 0x01000000-0xffffffff]
Oct 13 06:56:12 linux-9gh3 kernel:   Normal   empty
Oct 13 06:56:12 linux-9gh3 kernel: Movable zone start for each node
Oct 13 06:56:12 linux-9gh3 kernel: Early memory node ranges
Oct 13 06:56:12 linux-9gh3 kernel:   node   0: [mem 0x00001000-0x0009efff]
Oct 13 06:56:12 linux-9gh3 kernel:   node   0: [mem 0x00100000-0x6ffeffff]
Oct 13 06:56:12 linux-9gh3 kernel: Built 1 zonelists in Node order, mobility grouping on.  Total pages: 452345
Oct 13 06:56:12 linux-9gh3 kernel: Policy zone: DMA32
Oct 13 06:56:12 linux-9gh3 kernel: Memory: 1669008K/1834552K available (5305K kernel code, 1263K rwdata, 4168K
rodata, 1932K init, 248
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: All ACPI Tables successfully acquired
Oct 13 06:56:12 linux-9gh3 kernel: APIC calibration not consistent with PM-Timer: 96ms instead of 100ms
Oct 13 06:56:12 linux-9gh3 kernel: NMI watchdog: disabled (cpu0): hardware events not enabled
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: Executed 1 blocks of module-level executable AML code
Oct 13 06:56:12 linux-9gh3 kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S1_]
(20130725/hwxface-571)
Oct 13 06:56:12 linux-9gh3 kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S2_]
(20130725/hwxface-571)
Oct 13 06:56:12 linux-9gh3 kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S3_]
(20130725/hwxface-571)
Oct 13 06:56:12 linux-9gh3 kernel: ACPI Exception: AE_NOT_FOUND, While evaluating Sleep State [\_S4_]
(20130725/hwxface-571)
Oct 13 06:56:12 linux-9gh3 kernel: acpi PNP0A03:00: fail to add MMCONFIG information, can't access extended PCI
configuration space un
Oct 13 06:56:12 linux-9gh3 kernel: ACPI: Enabled 2 GPEs in block 00 to 07
Oct 13 06:56:12 linux-9gh3 kernel: pci 0000:00:07.0: BAR 13: [io  0x4000-0x403f] has bogus alignment
Oct 13 06:56:12 linux-9gh3 kernel: Dquot-cache hash table entries: 512 (order 0, 4096 bytes)
```

```
Oct 13 06:56:14 linux-9gh3 kernel: sr0: scsi3-mmc drive: 32x/32x xa/form2 tray
Oct 13 06:56:15 linux-9gh3 kernel: raid6: sse2x1    1708 MB/s
Oct 13 06:56:15 linux-9gh3 kernel: raid6: sse2x2    1610 MB/s
Oct 13 06:56:15 linux-9gh3 kernel: raid6: sse2x4     929 MB/s
lines 1-35
```

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 :

```
SLES12SP1:~ # journalctl --since 15:00 --until now
-- Logs begin at Fri 2017-10-13 06:56:12 CEST, end at Sun 2017-10-15 15:14:01 CEST. --
Oct 15 15:00:01 SLES12SP1.fenetros.loc cron[28955]: pam_unix(crond:session): session opened for user root by
(uid=0)
Oct 15 15:00:01 SLES12SP1.fenetros.loc cron[28956]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
Oct 15 15:00:01 SLES12SP1.fenetros.loc systemd[28957]: pam_unix(systemd-user:session): session opened for user
root by (uid=0)
Oct 15 15:00:01 SLES12SP1.fenetros.loc CRON[28958]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 15 15:00:01 SLES12SP1.fenetros.loc CRON[28956]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:00:01 SLES12SP1.fenetros.loc CRON[28955]: pam_unix(crond:session): session closed for user root
Oct 15 15:00:01 SLES12SP1.fenetros.loc systemd[28959]: pam_unix(systemd-user:session): session closed for user
root
Oct 15 15:00:06 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:00:13 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:00:20 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:00:27 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:00:34 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:00:41 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:00:49 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:00:56 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:01:01 SLES12SP1.fenetros.loc cron[29283]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
```

```
Oct 15 15:01:01 SLES12SP1.fenetros.loc CRON[29284]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 15 15:01:01 SLES12SP1.fenetros.loc CRON[29283]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:01:03 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:01:10 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:01:17 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:01:24 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:01:31 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:01:38 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:01:45 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:01:53 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:02:00 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:02:01 SLES12SP1.fenetros.loc cron[29563]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
Oct 15 15:02:01 SLES12SP1.fenetros.loc CRON[29564]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 15 15:02:01 SLES12SP1.fenetros.loc CRON[29563]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:02:07 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:02:14 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:02:21 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
Oct 15 15:02:28 SLES12SP1.fenetros.loc sh[1557]: Sleeping '1250' '1250'
lines 1-35
```

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

Consultation des Journaux en Live

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

```
SLES12SP1:~ # journalctl -f
-- Logs begin at Fri 2017-10-13 06:56:12 CEST. --
```

```
Oct 15 15:11:01 SLES12SP1.fenetros.loc CRON[32066]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:12:01 SLES12SP1.fenetros.loc cron[32319]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
Oct 15 15:12:01 SLES12SP1.fenetros.loc CRON[32320]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 15 15:12:01 SLES12SP1.fenetros.loc CRON[32319]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:13:01 SLES12SP1.fenetros.loc cron[32597]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
Oct 15 15:13:01 SLES12SP1.fenetros.loc CRON[32598]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 15 15:13:01 SLES12SP1.fenetros.loc CRON[32597]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:14:01 SLES12SP1.fenetros.loc cron[417]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
Oct 15 15:14:01 SLES12SP1.fenetros.loc CRON[418]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 15 15:14:01 SLES12SP1.fenetros.loc CRON[417]: pam_unix(crond:session): session closed for user trainee
```

Ouvrez un deuxième terminal et saisissez la commande suivante :

```
trainee@SLES12SP1:~> logger -p user.info Linux est super
```

Retournez consulter le premier terminal :

```
SLES12SP1:~ # journalctl -f
-- Logs begin at Fri 2017-10-13 06:56:12 CEST. --
Oct 15 15:11:01 SLES12SP1.fenetros.loc CRON[32066]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:12:01 SLES12SP1.fenetros.loc cron[32319]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
Oct 15 15:12:01 SLES12SP1.fenetros.loc CRON[32320]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 15 15:12:01 SLES12SP1.fenetros.loc CRON[32319]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:13:01 SLES12SP1.fenetros.loc cron[32597]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
Oct 15 15:13:01 SLES12SP1.fenetros.loc CRON[32598]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 15 15:13:01 SLES12SP1.fenetros.loc CRON[32597]: pam_unix(crond:session): session closed for user trainee
Oct 15 15:14:01 SLES12SP1.fenetros.loc cron[417]: pam_unix(crond:session): session opened for user trainee by
(uid=0)
Oct 15 15:14:01 SLES12SP1.fenetros.loc CRON[418]: (trainee) CMD (/bin/pwd > pwd.txt)
```

```
Oct 15 15:14:01 SLES12SP1.fenetros.loc CRON[417]: pam_unix(crond:session): session closed for user trainee
...
Oct 15 15:16:12 SLES12SP1.fenetros.loc packagekitd[1195]:
DownloadProgressReportReceiver::start():https://updates.suse.com/SUSE/Updates/SLE-SERVER/12-SP1/x86_64/update?4Z3
imOnkmCfmVfTjzKnS5a1z21vEfrb1Qhxjo8tVzrZ2-
Bz_VQxbeJkQJ8Uo7f7IH1MNmeNGZOLUxhVkga2iFnLNFd7wwjGUBeBh_c47J_Ngy1uSjUWas-GXe2UdY9wv1yTUy1pQMs5n0HU --gnome-
packagekit-lang;3.10.1-13.50;noarch;SUSE_Linux_Enterprise_Server_12_SP1_x86_64:SLES12-SP1-Updates
Oct 15 15:16:15 SLES12SP1.fenetros.loc trainee[1491]: Linux est super
...
```

Important : Notez la présence de la dernière ligne.

Consultation des Journaux avec des Mots Clefs

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

```
SLES12SP1:~ # journalctl [tab] [tab] [tab]
CODE_FILE=                  SYSLOG_PID=                 _KERNEL_SUBSYSTEM=          _UDEV_DEVLINK=
CODE_FUNC=                  _AUDIT_LOGINUID=            _MACHINE_ID=                _UDEV_DEVNODE=
CODE_LINE=                  _AUDIT_SESSION=             _PID=                       _UDEV_SYSNAME=
COREDUMP_EXE=               _BOOT_ID=                   _SELINUX_CONTEXT=           _UID=
ERRNO=                      _CMDLINE=                   _SOURCE_REALTIME_TIMESTAMP= __CURSOR=
MESSAGE=                    _COMM=                      _SYSTEMD_CGROUP=            __MONOTONIC_TIMESTAMP=
MESSAGE_ID=                 _EXE=                       _SYSTEMD_OWNER_UID=         __REALTIME_TIMESTAMP=
PRIORITY=                   _GID=                       _SYSTEMD_SESSION=
SYSLOG_FACILITY=            _HOSTNAME=                  _SYSTEMD_UNIT=
SYSLOG_IDENTIFIER=          _KERNEL_DEVICE=             _TRANSPORT=
```

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 ⇆ :

```
SLES12SP1:~ # journalctl _UID=
0     1000  486   491   497   499
SLES12SP1:~ # journalctl _COMM=
(sd-pam)         auditd           display-manager  logger           pulseaudio       systemd          wicked
(systemd)        boot.apparmor    dracut-cmdline   master           rtkit-daemon     systemd-journal  wickedd
accounts-daemon  btrfsmaintenanc  echo             mtp-probe        sh               systemd-udevd    wickedd-
dhcp4
anacron          cron             gdm-session-wor  packagekitd      sshd             udisksd          wickedd-
dhcp6
audispd          crontab          irqbalance       polkitd          sshd-gen-keys-s  vboxadd
auditctl         dbus-daemon      iscsiadm         postlog          su               vboxadd-service
```

<html>

</html>
