Niveau : Admin Junior	Numéro de la Leçon	Dernière Modification
2/4	<progrecss 8/12 style=inline />	2020/01/30 03:28

Gestion de la Journalisation

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

<note 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. </note>

Le fichier /var/log/messages

Ce fichier contient la plupart des messages du système, y compris les heures de connexion et déconnexion réussies ou non :

```
root@debian:~# tail /var/log/messages
May 29 15:23:56 debian kernel: [   12.357748] Bluetooth: BNEP (Ethernet Emulation) ver 1.3
May 29 15:23:56 debian kernel: [   12.357753] Bluetooth: BNEP filters: protocol multicast
May 29 15:23:56 debian kernel: [   12.389661] Bridge firewalling registered
May 29 15:23:56 debian kernel: [   12.461197] Bluetooth: SCO (Voice Link) ver 0.6
May 29 15:23:56 debian kernel: [   12.461202] Bluetooth: SCO socket layer initialized
May 29 15:23:57 debian kernel: [   12.800941] lp: driver loaded but no devices found
May 29 15:23:57 debian kernel: [   12.829458] ppdev: user-space parallel port driver
May 29 15:23:57 debian kernel: [   13.060799] [drm] Initialized drm 1.1.0 20060810
May 29 15:23:57 debian kernel: [   13.122463] pci 0000:00:02.0: PCI INT A -> GSI 18 (level, low) -> IRQ 18
May 29 15:23:57 debian kernel: [   13.122702] [drm] Initialized vboxvideo 1.0.0 20090303 for 0000:00:02.0 on
minor 0
```

La commande /bin/dmesg

Cette commande afficher le tampon des messages du noyau :

```
root@debian:~# dmesg | more
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Linux version 2.6.32-5-686 (Debian 2.6.32-31) (ben@decadent.org.u
k) (gcc version 4.3.5 (Debian 4.3.5-4) ) #1 SMP Tue Mar 8 21:36:00 UTC 2011
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   NSC Geode by NSC
[    0.000000]   Cyrix CyrixInstead
[    0.000000]   Centaur CentaurHauls
[    0.000000]   Transmeta GenuineTMx86
[    0.000000]   Transmeta TransmetaCPU
[    0.000000]   UMC UMC UMC UMC
[    0.000000] BIOS-provided physical RAM map:
[    0.000000]  BIOS-e820: 0000000000000000 - 000000000009fc00 (usable)
[    0.000000]  BIOS-e820: 000000000009fc00 - 00000000000a0000 (reserved)
[    0.000000]  BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
[    0.000000]  BIOS-e820: 0000000000100000 - 000000003fff0000 (usable)
[    0.000000]  BIOS-e820: 000000003fff0000 - 0000000040000000 (ACPI data)
[    0.000000]  BIOS-e820: 00000000fffc0000 - 0000000100000000 (reserved)
[    0.000000] DMI 2.5 present.
[    0.000000] last_pfn = 0x3fff0 max_arch_pfn = 0x100000
[    0.000000] MTRR default type: uncachable
--More--
```

Le fichier /var/log/dmesg

Ce fichier contient messages du noyau affichés lors du dernier démarrage du système :

```
root@debian:~# tail -n 15 /var/log/dmesg
[   10.685827] ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
[   12.258861] Bluetooth: Core ver 2.15
[   12.258896] NET: Registered protocol family 31
[   12.258897] Bluetooth: HCI device and connection manager initialized
[   12.258899] Bluetooth: HCI socket layer initialized
[   12.298740] Bluetooth: L2CAP ver 2.14
[   12.298743] Bluetooth: L2CAP socket layer initialized
[   12.469897] Bluetooth: RFCOMM TTY layer initialized
[   12.469901] Bluetooth: RFCOMM socket layer initialized
[   12.469902] Bluetooth: RFCOMM ver 1.11
[   12.558955] Bluetooth: BNEP (Ethernet Emulation) ver 1.3
[   12.558960] Bluetooth: BNEP filters: protocol multicast
[   12.618935] Bridge firewalling registered
[   12.810130] Bluetooth: SCO (Voice Link) ver 0.6
[   12.810133] Bluetooth: SCO socket layer initialized
```

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

Le fichier **/var/log/audit/audit.log** contient les messages du système d'audit, appelés des **évènements**. Le système d'audit n'est pas installé par défaut sous Debian. Pour l'installer, utilisez la commande apt-get :

```
root@debian:~# apt-get install auditd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Paquets suggérés :
```

```
  audispd-plugins
Les NOUVEAUX paquets suivants seront installés :
  auditd
0 mis à jour, 1 nouvellement installés, 0 à enlever et 219 non mis à jour.
Il est nécessaire de prendre 356 ko dans les archives.
Après cette opération, 1 053 ko d'espace disque supplémentaires seront utilisés.
Réception de : 1 http://ftp.fr.debian.org/debian/ squeeze/main auditd i386 1.7.13-1+b2 [356 kB]
356 ko réceptionnés en 5s (71,2 ko/s)
Sélection du paquet auditd précédemment désélectionné.
(Lecture de la base de données... 130583 fichiers et répertoires déjà installés.)
Dépaquetage de auditd (à partir de .../auditd_1.7.13-1+b2_i386.deb) ...
Traitement des actions différées (« triggers ») pour « man-db »...
Paramétrage de auditd (1.7.13-1+b2) ...
update-rc.d: warning: auditd start runlevel arguments (S) do not match LSB Default-Start values (2 3 4 5)
update-rc.d: warning: auditd stop runlevel arguments (0 6) do not match LSB Default-Stop values (0 1 6)
```

Le système audit collectionne des informations telles :

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

```
root@debian:~# cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1334678847.365:495): auditd start, ver=1.7.13 format=raw kernel=2.6.32-5-686
auid=4294967295 pid=2994 res=success
type=CONFIG_CHANGE msg=audit(1334678847.467:2): audit_backlog_limit=320 old=64 auid=4294967295 ses=4294967295
res=1
```

<note important> SELinux n'est pas installé par défaut sous Debian. Pour cette raison, le fichier **/var/log/audit/audit.log** contient très peu d'évènements. L'installation de SELinux sera abordée dans la léçon **La Sécurité du Serveur sous Debian**. </note>

Gestion des évènements audit

La gestion des évènements audit se repose sur trois exécutables :

auditd

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

```
root@debian:~# 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 = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 5
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_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
```

Les option de cette commande sont :

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

auditctl

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

```
root@debian:~# 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
```

Les options de cette commande sont :

```
root@debian:~# 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
    -d <l,a>            Delete rule from <l>ist with <a>ction
                        l=task,entry,exit,user,watch,exclude
                        a=never,possible,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** :

```
root@debian:~# ls /etc/audisp/plugins.d
af_unix.conf  syslog.conf
```

Le contenu de ces fichiers suit un format précis :

```
root@debian:~# 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.

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, voire des graphiques.

Les options de cette commande sont :

```
root@debian:~# aureport --help
usage: aureport [options]
    -a,--avc            Avc report
    --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
    --node <node name>        Only events from a specific node
    -n,--anomaly            aNomaly report
    -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
    -u,--user            User name report
    -v,--version            Version
    -x,--executable            eXecutable name report
```

```
    If no report is given, the summary report will be displayed
```

<note important> Vous pouvez consulter un exemple de l'utilisation de cette commande dans l'unité **Gestion de la Journalisation sous CentOS/Redhat** de cette leçon. </note>

La commande ausearch

Cette commande est utilisée pour rechercher des évènements.

Les options de cette commande sont :

```
root@debian:~# ausearch --help
usage: ausearch [options]
    -a,--event <Audit event id>    search based on audit event id
    -c,--comm  <Comm name>        search based on command line name
    -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
    -v,--version            version
    -w,--word            string matches are whole word
    -x,--executable  <executable name>  search based on excutable name
```

<note important> Vous pouvez consulter un exemple de l'utilisation de cette commande dans l'unité **Gestion de la Journalisation sous CentOS/Redhat** de cette leçon. </note>

<note important> Pour plus d'information concernant le système audit, consultez les manuels de **auditd**, **auditctl**, **audispd**, **aureport** et **ausearch**. </note>

Applications

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

- cups,

- apt,
- gdm3,
- ...

```
root@debian:~# ls -l /var/log
total 1780
-rw-r--r-- 1 root        root         737  9 avril 13:55 alternatives.log
-rw-r--r-- 1 root        root        1191 28 juil.  2011 alternatives.log.1
-rw-r--r-- 1 root        root        5055 28 avril  2011 alternatives.log.2.gz
drwxr-xr-x 2 root        root        4096  3 avril 10:40 apt
-rw-r--r-- 1 root        root           0 24 mai    2011 aptitude
-rw-r--r-- 1 root        root        7337 24 avril  2011 aptitude.1.gz
-rw-r----- 1 root        adm         7976 17 avril 18:01 auth.log
-rw-r----- 1 root        adm        90396 10 avril 10:35 auth.log.1
-rw-r----- 1 root        adm         1247  3 avril 10:21 auth.log.2.gz
-rw-r----- 1 root        adm          580 28 juil.  2011 auth.log.3.gz
-rw-r----- 1 root        adm         1824 24 mai    2011 auth.log.4.gz
-rw-r----- 1 root        adm           31 24 avril  2011 boot
-rw-rw---- 1 root        utmp           0  3 avril 10:40 btmp
-rw-rw---- 1 root        utmp           0 28 juil.  2011 btmp.1
drwxr-xr-x 2 root        root        4096  3 avril 10:40 ConsoleKit
drwxr-xr-x 2 root        root        4096 10 avril 10:35 cups
-rw-r----- 1 root        adm         5698 17 avril 17:52 daemon.log
-rw-r----- 1 root        adm       120481 10 avril 10:31 daemon.log.1
-rw-r----- 1 root        adm         5846  3 avril 10:11 daemon.log.2.gz
-rw-r----- 1 root        adm         3321 28 juil.  2011 daemon.log.3.gz
-rw-r----- 1 root        adm        10604 24 mai    2011 daemon.log.4.gz
-rw-r----- 1 root        adm           0 10 avril 10:35 debug
-rw-r----- 1 root        adm        27019 10 avril 09:41 debug.1
-rw-r----- 1 root        adm         3016  3 avril 10:05 debug.2.gz
-rw-r----- 1 root        adm         1535 28 juil.  2011 debug.3.gz
-rw-r----- 1 root        adm         4987 24 mai    2011 debug.4.gz
-rw-r----- 1 root        adm        23378  9 avril 15:41 dmesg
-rw-r----- 1 root        adm        25226  8 avril 13:16 dmesg.0
```

```
-rw-r----- 1 root        adm          7729  7 avril 13:33 dmesg.1.gz
-rw-r----- 1 root        adm          7322  4 avril 07:16 dmesg.2.gz
-rw-r----- 1 root        adm          7319  3 avril 10:05 dmesg.3.gz
-rw-r----- 1 root        adm          8136  4 déc.  08:53 dmesg.4.gz
-rw-r--r-- 1 root        root         4040  9 avril 13:55 dpkg.log
-rw-r--r-- 1 root        root         9378 28 juil.  2011 dpkg.log.1
-rw-r--r-- 1 root        root          656 28 juil.  2011 dpkg.log.2.gz
-rw-r--r-- 1 root        root        70042 28 avril  2011 dpkg.log.3.gz
drwxr-s--- 2 Debian-exim adm          4096 10 avril 10:35 exim4
-rw-r--r-- 1 root        root        24024 27 avril  2011 faillog
-rw-r--r-- 1 root        root         1938 28 avril  2011 fontconfig.log
drwxr-xr-x 2 root        root         4096 24 avril  2011 fsck
drwxrwx--T 2 root        Debian-gdm   4096  9 avril 15:41 gdm3
drwxr-xr-x 3 root        root         4096 24 avril  2011 installer
-rw-r----- 1 root        adm          1332 17 avril 17:52 kern.log
-rw-r----- 1 root        adm        149120 10 avril 10:31 kern.log.1
-rw-r----- 1 root        adm         32104  3 avril 10:05 kern.log.2.gz
-rw-r----- 1 root        adm          9228 28 juil.  2011 kern.log.3.gz
-rw-r----- 1 root        adm         65855 24 mai    2011 kern.log.4.gz
-rw-rw-r-- 1 root        utmp       292292 27 avril  2011 lastlog
-rw-r----- 1 root        adm             0 10 avril 10:35 lpr.log
-rw-r----- 1 root        adm           520  9 avril 15:41 lpr.log.1
-rw-r----- 1 root        adm           146  3 avril 10:05 lpr.log.2.gz
-rw-r----- 1 root        adm           102 28 juil.  2011 lpr.log.3.gz
-rw-r----- 1 root        adm           192 24 mai    2011 lpr.log.4.gz
-rw-r----- 1 root        adm             0 24 avril  2011 mail.err
-rw-r----- 1 root        adm             0 24 avril  2011 mail.info
-rw-r----- 1 root        adm             0 24 avril  2011 mail.log
-rw-r----- 1 root        adm             0 24 avril  2011 mail.warn
-rw-r----- 1 root        adm          1318 17 avril 17:52 messages
-rw-r----- 1 root        adm        125210 10 avril 10:35 messages.1
-rw-r----- 1 root        adm         15091  3 avril 10:40 messages.2.gz
-rw-r----- 1 root        adm          8194 28 juil.  2011 messages.3.gz
-rw-r----- 1 root        adm         25305 24 mai    2011 messages.4.gz
```

```
drwxr-xr-x 2 root        root         4096 24 avril  2011 news
-rw-r--r-- 1 root        root          939  9 avril 15:41 pm-powersave.log
-rw-r--r-- 1 root        root          540  3 avril 10:05 pm-powersave.log.1
-rw-r--r-- 1 root        root          106 28 juil.  2011 pm-powersave.log.2.gz
-rw-r--r-- 1 root        root          116 24 mai    2011 pm-powersave.log.3.gz
-rw-r--r-- 1 root        root            0 24 avril  2011 pycentral.log
-rw-r----- 1 root        adm         10854 17 avril 18:01 syslog
-rw-r----- 1 root        adm        175011 10 avril 10:35 syslog.1
-rw-r----- 1 root        adm         13765  7 avril 13:53 syslog.2.gz
-rw-r----- 1 root        adm         13030  4 avril 07:30 syslog.3.gz
-rw-r----- 1 root        adm         45717  3 avril 10:17 syslog.4.gz
-rw-r----- 1 root        adm         13319 28 juil.  2011 syslog.5.gz
-rw-r----- 1 root        adm         35060 24 mai    2011 syslog.6.gz
-rw-r----- 1 root        adm         37856 28 avril  2011 syslog.7.gz
drwxr-xr-x 2 root        root         4096  9 avril 14:45 sysstat
drwxr-xr-x 2 root        root         4096 18 nov.   2010 unattended-upgrades
-rw-r----- 1 root        adm             0 10 avril 10:35 user.log
-rw-r----- 1 root        adm           317  9 avril 15:40 user.log.1
-rw-r----- 1 root        adm           139  4 déc.  08:55 user.log.2.gz
-rw-r----- 1 root        adm           458 28 avril  2011 user.log.3.gz
-rw-r--r-- 1 root        root       155349  4 déc.  08:31 vboxadd-install.log
-rw-r--r-- 1 root        root           73  4 déc.  08:31 vboxadd-install-x11.log
-rw-r--r-- 1 root        root           75  4 déc.  08:31 VBoxGuestAdditions.log
-rw-r--r-- 1 root        root          246  4 déc.  08:30 VBoxGuestAdditions-uninstall.log
-rw-rw-r-- 1 root        utmp        44928 10 avril 09:42 wtmp
-rw-rw-r-- 1 root        utmp        53760  3 avril 10:05 wtmp.1
-rw-r--r-- 1 root        root        26408 10 avril 11:04 Xorg.0.log
-rw-r--r-- 1 root        root        26498  9 avril 15:40 Xorg.0.log.old
```

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**).

Le daemon rsyslog est configuré par l'édition du fichier **/etc/default/rsyslog** :

```
root@debian:~# cat /etc/default/rsyslog
# Options for rsyslogd
# -m 0 disables 'MARK' messages (deprecated, only used in compat mode < 3)
# -r enables logging from remote machines (deprecated, only used in compat mode < 3)
# -x disables DNS lookups on messages received with -r
# -c compatibility mode
# See rsyslogd(8) for more details
RSYSLOGD_OPTIONS="-c4"
```

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

Directive	Version
SYSLOGD_OPTIONS="-c 2"	rsyslog V2 - mode compatibilité
SYSLOGD_OPTIONS="-c 0"	syslogd

Priorités

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

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

Sous-systèmes applicatifs

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

Fonction	Description
auth/auth-priv	Message de sécurité / autorisation
cron	Message de cron ou at
daemon	Message d'un daemon
kern	Message du noyau
lpr	Message du système d'impression
mail	Message du système de mail
news	Message du système de news
syslog	Message interne de rsyslogd

Fonction	Description
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** ainsi que le contenu des fichiers éventuels se trouvant dans le répertoire **/etc/rsyslog.d** :

```
root@debian:~# cat /etc/rsyslog.conf
#  /etc/rsyslog.conf    Configuration file for rsyslog.
#
#           For more information see
#           /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html


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

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

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

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

```
#############################
#### GLOBAL DIRECTIVES ####
#############################

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

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

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


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

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*         /var/log/auth.log
*.*;auth,authpriv.none      -/var/log/syslog
```

```
#cron.*             /var/log/cron.log
daemon.*            -/var/log/daemon.log
kern.*              -/var/log/kern.log
lpr.*               -/var/log/lpr.log
mail.*              -/var/log/mail.log
user.*              -/var/log/user.log

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

#
# Logging for INN news system.
#
news.crit           /var/log/news/news.crit
news.err            /var/log/news/news.err
news.notice         -/var/log/news/news.notice

#
# Some "catch-all" log files.
#
*.=debug;\
    auth,authpriv.none;\
    news.none;mail.none    -/var/log/debug
*.=info;*.=notice;*.=warn;\
    auth,authpriv.none;\
    cron,daemon.none;\
    mail,news.none        -/var/log/messages

#
```

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

#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
#daemon,mail.*;\
#   news.=crit;news.=err;news.=notice;\
#   *.=debug;*.=info;\
#   *.=notice;*.=warn    /dev/tty8

# The named pipe /dev/xconsole is for the `xconsole' utility.  To use it,
# you must invoke `xconsole' with the `-file' option:
#
#    $ xconsole -file /dev/xconsole [...]
#
# NOTE: adjust the list below, or you'll go crazy if you have a reasonably
#      busy site..
#
daemon.*;mail.*;\
    news.err;\
    *.=debug;*.=info;\
    *.=notice;*.=warn    |/dev/xconsole
```

Ce fichier est divisé en 3 parties :

- **Modules**,
  - Section traitant le chargement des modules offrant des fonctionnalités étendues à rsyslog,
- **Directives Globales** (*Global Directives*),
  - Section traitant les options de comportement global du service rsyslog,
- **Règles** (*Rules*),
  - Section traitant les règles de configuration des journaux. Les règles au format syslogd gardent le même format. Les nouvelles règles,

compatibles seulement avec rsyslog commencent par **$**.

Modules

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

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

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

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

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

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

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

```
...
```

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

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

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support (previously done by rklogd)
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
...
```

<note 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**. </note>

Pour envoyer l'ensemble des traces de journalisation vers un serveur rsyslog distant, il convient d'ajouter les lignes suivantes dans le fichier **/etc/rsyslog.conf** :

```
...
$WorkDirectory /var/spool/rsyslog # where to place spool files
$ActionQueueFileName fwdRule1 # unique name prefix for spool files
```

```
$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
$ActionQueueType LinkedList   # run asynchronously
$ActionResumeRetryCount -1    # infinite retries if host is down
*.* @@remote-host:514
...
```

<note important> Ces directives utilisent le protocole TCP. Le serveur distant doit donc être configuré pour ce mode de communication.La directive ***.* @@remote-host:514** doit être modifiée pour indiquer l'adresse IP du serveur rsyslog distant. Le répertoire **/var/spool/rsyslog** doit être créé.
</note>

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**.

<note 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. </note>

/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 :

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

Consultez la fin de votre syslog :

```
root@debian:~# tail /var/log/messages
Apr 18 13:50:28 debian kernel: [ 8422.523161] usb 2-1: Manufacturer: VirtualBox
Apr 18 13:50:28 debian kernel: [ 8422.525313] usb 2-1: configuration #1 chosen from 1 choice
Apr 18 13:50:28 debian kernel: [ 8422.534677] input: VirtualBox USB Tablet as
/devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/input/input11
Apr 18 13:50:28 debian kernel: [ 8422.534866] generic-usb 0003:80EE:0021.0006: input,hidraw0: USB HID v1.10 Mouse
[VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
Apr 23 10:38:12 debian kernel: [ 8426.688613] e1000: eth1 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
Apr 23 10:47:42 debian kernel: Kernel logging (proc) stopped.
Apr 23 10:47:42 debian rsyslogd: [origin software="rsyslogd" swVersion="4.6.4" x-pid="886" x-
info="http://www.rsyslog.com"] exiting on signal 15.
Apr 23 10:47:42 debian kernel: imklog 4.6.4, log source = /proc/kmsg started.
Apr 23 10:47:42 debian rsyslogd: [origin software="rsyslogd" swVersion="4.6.4" x-pid="3932" x-
info="http://www.rsyslog.com"] (re)start
Apr 23 10:48:10 debian trainee: Linux est super
```

Options de la commande

Les options de la commande logger sont :

```
root@debian:~# logger --help
logger : option invalide -- '-'
usage: logger [-is] [-f file] [-p pri] [-t tag] [-u socket] [ message ... ]
```

/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** :

```
root@debian:~# 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

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

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

```
# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

# system-specific logs may 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.

Options de la commande

Les options de la commande logrotate sont :

```
root@debian:~# logrotate --help
Utilisation: 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 `/usr/bin/mail')
  -s, --state=statefile     Path of state file
  -v, --verbose             Display messages during rotation

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

~~DISCUSSION:off~~

Donner votre Avis

{(rater>id=debian_6_l114|name=cette page|type=rate|trace=user|tracedetails=1)}