Dernière mise-à-jour : 2020/01/30 03:27

Gestion de la Journalisation

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

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.

Le fichier /var/log/syslog

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

```
root@ubuntu:~# tail /var/log/syslog
Oct 25 13:12:01 ubuntu CRON[13276]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:13:01 ubuntu CRON[13280]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:14:01 ubuntu CRON[13283]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:15:01 ubuntu CRON[13289]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:16:01 ubuntu CRON[13294]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:17:01 ubuntu CRON[13299]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:17:01 ubuntu CRON[13301]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Oct 25 13:18:01 ubuntu CRON[13305]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:19:01 ubuntu CRON[13308]: (trainee) CMD (/bin/pwd > pwd.txt)
```

```
Oct 25 13:20:01 ubuntu CRON[13312]: (trainee) CMD (/bin/pwd > pwd.txt)
```

La commande /bin/dmesg

Cette commande afficher le tampon des messages du noyau :

```
root@ubuntu:~# dmesg | more
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Initializing cgroup subsys cpuacct
[    0.000000] Linux version 3.13.0-32-generic (buildd@roseapple) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1) )
#57-Ubuntu SMP Tue Jul 15 03:51:
12 UTC 2014 (Ubuntu 3.13.0-32.57-generic 3.13.11.4)
[    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] 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 0x0000000000100000-0x000000007cfeffff] usable
[    0.000000] BIOS-e820: [mem 0x000000007cff0000-0x000000007cffffff] ACPI data
[    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 12/01/2006
```

```
[    0.000000] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.000000] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.000000] e820: last_pfn = 0x7cff0 max_arch_pfn = 0x1000000
[    0.000000] MTRR default type: uncachable
[    0.000000] MTRR variable ranges disabled:
[    0.000000] x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
[    0.000000] CPU MTRRs all blank - virtualized system.
[    0.000000] Scanning 1 areas for low memory corruption
[    0.000000] initial memory mapped: [mem 0x00000000-0x01ffffff]
[    0.000000] Base memory trampoline at [c009b000] 9b000 size 16384
--Plus--
```

Le fichier /var/log/dmesg

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

```
root@ubuntu:~# tail -n 15 /var/log/dmesg
[   16.029636] type=1400 audit(1413293251.778:11): apparmor="STATUS" operation="profile_load"
profile="unconfined" name="/usr/lib/lightdm/lightdm-guest-session" pid=622 comm="apparmor_parser"
[   16.260774] Bluetooth: Core ver 2.17
[   16.260811] NET: Registered protocol family 31
[   16.260812] Bluetooth: HCI device and connection manager initialized
[   16.261433] Bluetooth: HCI socket layer initialized
[   16.261436] Bluetooth: L2CAP socket layer initialized
[   16.261440] Bluetooth: SCO socket layer initialized
[   16.281341] Bluetooth: RFCOMM TTY layer initialized
[   16.281348] Bluetooth: RFCOMM socket layer initialized
[   16.281352] Bluetooth: RFCOMM ver 1.11
[   16.381432] Bluetooth: BNEP (Ethernet Emulation) ver 1.3
[   16.381435] Bluetooth: BNEP filters: protocol multicast
[   16.381440] Bluetooth: BNEP socket layer initialized
[   16.395159] init: cups main process (607) killed by HUP signal
```

```
[   16.395171] init: cups main process ended, respawning
```

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 Ubuntu. Pour l'installer, utilisez la commande apt-get :

```
root@ubuntu:~# apt-get install auditd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libauparse0
Paquets suggérés :
  audispd-plugins
Les NOUVEAUX paquets suivants seront installés :
  auditd libauparse0
0 mis à jour, 2 nouvellement installés, 0 à enlever et 171 non mis à jour.
Il est nécessaire de prendre 210 ko dans les archives.
Après cette opération, 748 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de : 1 http://fr.archive.ubuntu.com/ubuntu/ trusty/main libauparse0 i386 1:2.3.2-2ubuntu1 [33,6 kB]
Réception de : 2 http://fr.archive.ubuntu.com/ubuntu/ trusty/main auditd i386 1:2.3.2-2ubuntu1 [176 kB]
210 ko réceptionnés en 0s (212 ko/s)
Sélection du paquet libauparse0:i386 précédemment désélectionné.
(Lecture de la base de données... 168348 fichiers et répertoires déjà installés.)
Préparation du décompactage de .../libauparse0_1%3a2.3.2-2ubuntu1_i386.deb ...
Décompactage de libauparse0:i386 (1:2.3.2-2ubuntu1) ...
Sélection du paquet auditd précédemment désélectionné.
Préparation du décompactage de .../auditd_1%3a2.3.2-2ubuntu1_i386.deb ...
Décompactage de auditd (1:2.3.2-2ubuntu1) ...
Traitement déclenché pour  man-db (2.6.7.1-1) ...
```

```
Traitement déclenché pour  ureadahead (0.100.0-16) ...
Paramétrage de libauparse0:i386 (1:2.3.2-2ubuntu1) ...
Paramétrage de auditd (1:2.3.2-2ubuntu1) ...
 * Starting audit daemon auditd
[ OK ]
Traitement déclenché pour  libc-bin (2.19-0ubuntu6) ...
Traitement déclenché pour  ureadahead (0.100.0-16) ...
```

Le système audit collectionne des informations telles :

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

```
root@ubuntu:~# cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1414236266.952:6954): auditd start, ver=2.3.2 format=raw kernel=3.13.0-32-generic
auid=4294967295 pid=13756 subj=unconfined  res=success
type=CONFIG_CHANGE msg=audit(1414236267.054:69): audit_backlog_limit=320 old=64 auid=4294967295 ses=4294967295
res=1
type=USER_ACCT msg=audit(1414236301.827:70): pid=13777 uid=0 auid=4294967295 ses=4294967295
msg='op=PAM:accounting acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1414236301.831:71): pid=13777 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=USER_START msg=audit(1414236301.831:72): pid=13777 uid=0 auid=4294967295 ses=4294967295
msg='op=PAM:session_open acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1414236301.831:73): pid=13777 uid=0 auid=4294967295 ses=4294967295 msg='op=PAM:setcred
acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1414236301.831:74): pid=13777 uid=0 auid=4294967295 ses=4294967295
msg='op=PAM:session_close acct="trainee" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
```

SELinux n'est pas installé par défaut sous Ubuntu. 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 Ubuntu**.

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@ubuntu:~# 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
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
```

Les option de cette commande sont :

```
root@ubuntu:~# 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@ubuntu:~# 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@ubuntu:~# 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** :

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

Le contenu de ces fichiers suit un format précis :

```
root@ubuntu:~# 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, voire des graphiques :

```
root@ubuntu:~# aureport

Summary Report
======================
Range of time in logs: 25/10/2014 13:24:26.952 - 25/10/2014 13:30:01.896
Selected time for report: 25/10/2014 13:24:26 - 25/10/2014 13:30:01.896
Number of changes in configuration: 1
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 1
Number of terminals: 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: 33
```

Les options de cette commande sont :

```
root@ubuntu:~# 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
    --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
    --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 évenements. Par exemple, pour rechercher les évènements liés à un utilisateur représenté par son UID :

```
root@ubuntu:~# id trainee
uid=1000(trainee) gid=1000(trainee)
groupes=1000(trainee),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lpadmin),124(sambashare)
root@ubuntu:~# ausearch -ui 1000 | more
----
time->Sat Oct 25 13:26:56 2014
type=USER_START msg=audit(1414236416.676:80): pid=13796 uid=1000 auid=4294967295 ses=4294967295
msg='op=PAM:session_open acct="root" exe="/usr/b
in/pkexec" hostname=? addr=? terminal=pts/15 res=success'
```

Les options de cette commande sont :

```
root@ubuntu:~# 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
-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 excutable name
```

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

Applications

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

- cups,
- apt,
- ...

```
root@ubuntu:~# ls -l /var/log
total 2608
-rw-r--r-- 1 root             root    1535 oct.   2 16:05 alternatives.log
-rw-r--r-- 1 root             root   22547 sept. 29 14:30 alternatives.log.1
drwxr-xr-x 2 root             root    4096 oct.   2 15:23 apt
drwxr-x--- 2 root             root    4096 oct.  25 13:24 audit
-rw-r----- 1 syslog           adm    55412 oct.  25 13:32 auth.log
-rw-r----- 1 syslog           adm     7322 oct.  14 15:48 auth.log.1
-rw-r----- 1 syslog           adm     4134 oct.   6 15:54 auth.log.2.gz
-rw-r--r-- 1 root             root    3643 oct.  14 15:27 boot.log
-rw-r--r-- 1 root             root   61042 juil. 22 23:59 bootstrap.log
-rw-rw---- 1 root             utmp     384 oct.   6 15:52 btmp
```

```
-rw-rw---- 1 root              utmp       0 juil. 22 23:57 btmp.1
drwxr-xr-x 2 root              root    4096 oct.  14 15:58 cups
drwxr-xr-x 2 root              root    4096 avril 12  2014 dist-upgrade
-rw-r----- 1 root              adm    33330 oct.  14 15:27 dmesg
-rw-r----- 1 root              adm    32555 oct.   6 15:54 dmesg.0
-rw-r----- 1 root              adm    10761 oct.   6 15:51 dmesg.1.gz
-rw-r----- 1 root              adm    10747 oct.   2 15:12 dmesg.2.gz
-rw-r----- 1 root              adm    10746 sept. 29 14:07 dmesg.3.gz
-rw-r----- 1 root              adm    10741 sept. 28 11:35 dmesg.4.gz
-rw-r--r-- 1 root              root   24488 oct.  25 13:24 dpkg.log
-rw-r--r-- 1 root              root 1203495 sept. 27 19:01 dpkg.log.1
-rw-r--r-- 1 root              root   24096 oct.   1 16:43 faillog
-rw-r--r-- 1 root              root    3281 juil. 23 00:12 fontconfig.log
drwxr-xr-x 2 root              root    4096 juil. 22 23:58 fsck
-rw-r--r-- 1 root              root    1119 oct.  14 15:27 gpu-manager.log
drwxr-xr-x 3 root              root    4096 juil. 23 00:08 hp
drwxrwxr-x 2 root              root    4096 sept. 27 19:16 installer
-rw-r----- 1 syslog            adm    10003 oct.  25 13:24 kern.log
-rw-r----- 1 syslog            adm    52749 oct.  14 15:58 kern.log.1
-rw-r----- 1 syslog            adm    66628 oct.   6 16:06 kern.log.2.gz
-rw-rw-r-- 1 root              utmp  293168 oct.   1 16:43 lastlog
drwxr-xr-x 2 root              root    4096 oct.  14 15:27 lightdm
-rw-r--r-- 1 root              root    5352 oct.  14 15:27 pm-powersave.log
-rw-r--r-- 1 root              root    7064 oct.   2 15:13 pm-powersave.log.1
drwxr-x--- 2 root              adm     4096 juin  25 19:12 samba
drwx------ 2 speech-dispatcher root    4096 févr. 19  2014 speech-dispatcher
-rw-r----- 1 syslog            adm    84622 oct.  25 13:32 syslog
-rw-r----- 1 syslog            adm    83591 oct.  14 15:58 syslog.1
-rw-r----- 1 syslog            adm    36313 oct.   6 16:06 syslog.2.gz
-rw-r----- 1 syslog            adm    68542 oct.   2 15:23 syslog.3.gz
-rw-r--r-- 1 root              root  186338 oct.  14 15:27 udev
drwxr-xr-x 2 root              root    4096 sept. 28 11:34 unattended-upgrades
drwxr-xr-x 2 root              root    4096 oct.  17 15:07 upstart
-rw-r--r-- 1 root              root  221311 sept. 28 11:30 vboxadd-install.log
```

```
-rw-r--r-- 1 root              root      73 sept. 28 11:30 vboxadd-install-x11.log
-rw-r--r-- 1 root              root     103 sept. 28 11:30 VBoxGuestAdditions.log
-rw-rw-r-- 1 root              utmp   22656 oct.  25 13:27 wtmp
-rw-rw-r-- 1 root              utmp   26112 oct.   2 15:13 wtmp.1
-rw-r--r-- 1 root              root   69981 oct.  18 15:11 Xorg.0.log
-rw-r--r-- 1 root              root   39955 oct.   7 16:10 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@ubuntu:~# cat /etc/default/rsyslog
# Options for rsyslogd
```

```
# -x disables DNS lookups for remote messages
# See rsyslogd(8) for more details
RSYSLOGD_OPTIONS=""
```

L'option **-c** de la directive **RSYSLOGD_OPTIONS** spécifie le niveau de compatibilité avec les anciennes versions de rsyslog ainsi qu'avec son prédécesseur syslogd :

Directive	**Version**
RSYSLOGD_OPTIONS="-c 4"	Mode natif - aucune compatibilité
RSYSLOGD_OPTIONS="-c 2"	rsyslog V2 - mode compatibilité
RSYSLOGD_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

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

Le fichier /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@ubuntu:~# cat /etc/rsyslog.conf
#  /etc/rsyslog.conf    Configuration file for rsyslog.
#
#           For more information see
#           /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
#  Default logging rules can be found in /etc/rsyslog.d/50-default.conf


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

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$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

# Filter duplicated messages
$RepeatedMsgReduction on

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

#
```

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

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

Ce fichier est divisé en 2 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,

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
$ModLoad imklog   # provides kernel logging support
#$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
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

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

```
...
```

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 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
...
```

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.

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.

Le répertoire /etc/rsyslog.d

Les fichiers dans le répertoire **/etc/rsyslog.d/** contiennent les règles de configuration des journaux. Les règles au format syslogd gardent le même format. Les nouvelles règles, compatibles seulement avec rsyslog commencent par **$**. Par exemple :

```
root@ubuntu:~# cat /etc/rsyslog.d/50-default.conf
#  Default rules for rsyslog.
#
#           For more information see rsyslog.conf(5) and /etc/rsyslog.conf

#
# 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                                 :omusrmsg:*

#
# 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
```

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**.

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.

La commande /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@ubuntu:~# logger -p user.info Linux est super
```

Consultez la fin de votre syslog :

```
root@ubuntu:~# tail /var/log/syslog
Oct 25 13:54:01 ubuntu CRON[14009]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:55:01 ubuntu CRON[14021]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:56:01 ubuntu CRON[14024]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:57:01 ubuntu CRON[14027]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:58:01 ubuntu CRON[14031]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 13:59:01 ubuntu CRON[14034]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 14:00:01 ubuntu CRON[14038]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 14:01:01 ubuntu CRON[14041]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 14:02:01 ubuntu CRON[14044]: (trainee) CMD (/bin/pwd > pwd.txt)
Oct 25 14:02:08 ubuntu trainee: Linux est super
```

Options de la commande

Les options de la commande logger sont :

```
root@ubuntu:~# logger --help
```

```
Usage:
 logger [options] [message]

Options :
 -d, --udp             use UDP (TCP is default)
 -i, --id              log the process ID too
 -f, --file <file>     log the contents of this file
 -h, --help            display this help text and exit
 -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
 -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
 -V, --version         output version information and exit
```

La commande /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@ubuntu:~# cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# use the syslog group by default, since this is the owning group
# of /var/log/syslog.
su root syslog
```

```
# 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@ubuntu:~# 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
      --version             Display version information

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