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 :

```
opensuse:~ # tail -n 15 /var/log/messages
Apr 10 13:29:42 opensuse kernel: [ 9756.180989] usb 2-1: Manufacturer: VirtualBox
Apr 10 13:29:42 opensuse kernel: [ 9756.194920] input: VirtualBox USB Tablet as
/devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/input/input9
Apr 10 13:29:42 opensuse kernel: [ 9756.195110] generic-usb 0003:80EE:0021.0004: input,hidraw0: USB HID v1.10
Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
Apr 10 13:29:42 opensuse mtp-probe: checking bus 2, device 5: "/sys/devices/pci0000:00/0000:00:06.0/usb2/2-1"
Apr 10 13:29:42 opensuse mtp-probe: bus: 2, device: 5 was not an MTP device
Apr 18 11:51:29 opensuse kernel: [ 9760.447599] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control:
RX
Apr 18 11:51:43 opensuse /USR/SBIN/CRON[8207]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 18 11:52:01 opensuse /USR/SBIN/CRON[8214]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 18 11:52:36 opensuse dhclient: XMT: Solicit on eth0, interval 130570ms.
Apr 18 11:53:01 opensuse /USR/SBIN/CRON[8219]: (trainee) CMD (/bin/pwd > pwd.txt)
```

```
Apr 18 11:53:23 opensuse kernel: [ 9873.937561] lo: Disabled Privacy Extensions
Apr 18 11:54:01 opensuse /USR/SBIN/CRON[8355]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 18 11:54:31 opensuse su: The gnome keyring socket is not owned with the same credentials as the user login:
/tmp/keyring-FlmoAC/control
Apr 18 11:54:31 opensuse su: gkr-pam: couldn't unlock the login keyring.
Apr 18 11:54:31 opensuse su: (to root) trainee on /dev/pts/0
```

La commande /bin/dmesg

Cette commande retourne les messages du noyau affichés lors du dernier démarrage du système :

```
opensuse:~ # dmesg | more
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Linux version 2.6.37.6-0.5-desktop (geeko@buildhost) (gcc version 4.5.1 20101208 [gcc-4_5-branch
revision 167585] (SUSE Linux) ) #1 SMP PREEMPT 2011-04-2
5 21:48:33 +0200
[    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] NX (Execute Disable) protection: active
[    0.000000] DMI 2.5 present.
[    0.000000] DMI: innotek GmbH VirtualBox, BIOS VirtualBox 12/01/2006
[    0.000000] e820 update range: 0000000000000000 - 0000000000010000 (usable) ==> (reserved)
[    0.000000] e820 remove range: 00000000000a0000 - 0000000000100000 (usable)
[    0.000000] last_pfn = 0x3fff0 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] found SMP MP-table at [c009fff0] 9fff0
[    0.000000] initial memory mapped : 0 - 01000000
[    0.000000] init_memory_mapping: 0000000000000000-00000000371fe000
[    0.000000]  0000000000 - 0000200000 page 4k
[    0.000000]  0000200000 - 0037000000 page 2M
[    0.000000]  0037000000 - 00371fe000 page 4k
[    0.000000] kernel direct mapping tables up to 371fe000 @ ff6000-1000000
[    0.000000] RAMDISK: 375f2000 - 37ff0000
[    0.000000] Allocated new RAMDISK: 36800000 - 371fd094
[    0.000000] Move RAMDISK from 00000000375f2000 - 0000000037fef093 to 36800000 - 371fd093
[    0.000000] ACPI: RSDP 000e0000 00024 (v02 VBOX  )
[    0.000000] ACPI: XSDT 3fff0030 0003C (v01 VBOX   VBOXXSDT 00000001 ASL  00000061)
[    0.000000] ACPI: FACP 3fff00f0 000F4 (v04 VBOX   VBOXFACP 00000001 ASL  00000061)
--More--
```

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 CentOS/Redhat par le paquet **audit**. Le système audit collectionne des informations telles :

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

```
opensuse:~ # tail -n 15 /var/log/audit/audit.log
type=AVC msg=audit(1333977838.293:36): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=6675 comm="su"
type=DAEMON_END msg=audit(1333978674.692:3085): auditd normal halt, sending auid=0 pid=7084 subj= res=success
type=DAEMON_START msg=audit(1333978732.958:1061): auditd start, ver=2.0.5 format=raw kernel=2.6.37.6-0.5-desktop
auid=4294967295 pid=3682 subj=unconfined  res=success
```

```
type=AVC msg=audit(1333979168.339:27): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=1636 comm="gdm-session-wor"
type=AVC msg=audit(1333979168.340:28): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=1636 comm="gdm-session-wor"
type=AVC msg=audit(1333979262.923:29): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=6349 comm="su"
type=AVC msg=audit(1333979262.924:30): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=6349 comm="su"
type=AVC msg=audit(1334742871.907:31): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=8379 comm="su"
type=AVC msg=audit(1334742871.907:32): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=8379 comm="su"
type=AVC msg=audit(1334743204.034:33): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=8687 comm="su"
type=AVC msg=audit(1334743204.034:34): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=8687 comm="su"
type=AVC msg=audit(1334743204.040:35): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=8691 comm="su"
type=AVC msg=audit(1334743204.041:36): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=8691 comm="su"
type=AVC msg=audit(1334743204.047:37): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=8693 comm="su"
type=AVC msg=audit(1334743204.047:38): apparmor="DENIED" operation="change_hat" info="unconfined" error=-1
pid=8693 comm="su"
```

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** :

```
opensuse:~ # 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_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
```

Les option de cette commande sont :

```
opensuse:~ # 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** :

```
opensuse:~ # 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 :

```
opensuse:~ # 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** :

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

Le contenu de ces fichiers suit un format précis :

```
opensuse:~ # 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 :

```
opensuse:~ # aureport

Summary Report
======================
Range of time in logs: 05/24/11 10:15:14.548 - 04/18/12 12:00:04.047
Selected time for report: 05/24/11 10:15:14 - 04/18/12 12:00:04.047
```

```
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: 1
Number of terminals: 0
Number of host names: 0
Number of executables: 0
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: 27
Number of events: 28
```

Les options de cette commande sont :

```
opensuse:~ # 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 évènements. Par exemple, pour rechercher les évènements liés l'arrêt du daemon audit :

```
opensuse:~ # ausearch -m DAEMON_END
----
time->Thu Jul 28 11:13:13 2011
type=DAEMON_END msg=audit(1311844393.609:5758): auditd normal halt, sending auid=0 pid=12149 subj= res=success
----
```

```
time->Thu Jul 28 11:27:50 2011
type=DAEMON_END msg=audit(1311845270.837:9225): auditd normal halt, sending auid=0 pid=9041 subj= res=success
----
time->Sat Dec  3 15:54:18 2011
type=DAEMON_END msg=audit(1322924058.697:978): auditd normal halt, sending auid=0 pid=19199 subj= res=success
----
time->Sat Dec  3 16:26:09 2011
type=DAEMON_END msg=audit(1322925969.652:1044): auditd normal halt, sending auid=0 pid=9165 subj= res=success
----
time->Sat Dec  3 16:43:48 2011
type=DAEMON_END msg=audit(1322927028.823:6856): auditd normal halt, sending auid=0 pid=7360 subj= res=success
----
time->Sat Dec  3 17:27:34 2011
type=DAEMON_END msg=audit(1322929654.458:9376): auditd normal halt, sending auid=0 pid=9312 subj= res=success
----
time->Sun Dec  4 08:51:30 2011
type=DAEMON_END msg=audit(1322985090.676:8503): auditd normal halt, sending auid=0 pid=8520 subj= res=success
----
time->Sun Dec  4 08:52:39 2011
type=DAEMON_END msg=audit(1322985159.599:9674): auditd normal halt, sending auid=0 pid=4534 subj= res=success
----
time->Sun Jan 29 11:47:21 2012
type=DAEMON_END msg=audit(1327834041.788:2549): auditd normal halt, sending auid=0 pid=6587 subj= res=success
----
time->Sat Apr  7 15:31:12 2012
type=DAEMON_END msg=audit(1333805472.348:1640): auditd normal halt, sending auid=0 pid=10649 subj= res=success
----
time->Mon Apr  9 15:37:54 2012
type=DAEMON_END msg=audit(1333978674.692:3085): auditd normal halt, sending auid=0 pid=7084 subj= res=success
```

Les options de cette commande sont :

```
[root@centos ~]# 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> 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,
- gdm,
- samba,
- ...

```
opensuse:~ # ls -l /var/log
total 17584
drwxr-xr-x 2 root root        4096 May 17  2011 ConsoleKit
-rw-r----- 1 root root           0 May 17  2011 NetworkManager
-rw-r--r-- 1 root root         274 Dec  3 15:52 VBoxGuestAdditions-uninstall.log
-rw-r--r-- 1 root root         125 Dec  3 15:54 VBoxGuestAdditions.log
-rw-r--r-- 1 root root       37376 Apr 18 12:42 Xorg.0.log
-rw-r--r-- 1 root root       30563 Apr  9 15:37 Xorg.0.log.old
drwx------ 3 root root        4096 Dec  3 17:10 YaST2
-rw-r----- 1 root root        1640 Apr  9 15:38 acpid
drwxr-xr-x 5 root root        4096 Mar  2  2011 apparmor
drwx------ 2 root root        4096 May 24  2011 audit
-rw-r----- 1 root root           0 May 17  2011 boot.log
```

```
-rw-r--r-- 1 root root       30678 Apr  9 15:38 boot.msg
-rw-r--r-- 1 root root       37076 Apr  9 15:37 boot.omsg
-rw------- 1 root root           0 Mar  2  2011 btmp
drwxr-xr-x 2 lp   lp          4096 Apr  4 12:59 cups
-rw------- 1 root root        2640 Jul 28  2011 faillog
-rw-r----- 1 root root        3060 Apr  4 13:35 firewall
drwxrwx--T 2 root gdm         4096 Apr  9 15:38 gdm
drwx------ 2 root root        4096 Apr 14  2011 krb5
-rw-r--r-- 1 root root      292292 Apr  9 15:46 lastlog
-rw-r--r-- 1 root root       19886 Apr  9 15:38 localmessages
-rw-r----- 1 root root        5640 Apr  9 15:38 mail
-rw-r----- 1 root root         398 May 17  2011 mail.err
-rw-r----- 1 root root        5640 Apr  9 15:38 mail.info
-rw-r----- 1 root root         398 May 17  2011 mail.warn
-rw-r----- 1 root root      400547 Apr 18 12:52 messages
drwxr-x--- 2 news news        4096 Mar  2  2011 news
-rw-r--r-- 1 root root           0 Apr  9 15:38 nscd.log
-rw-r--r-- 1 root root           0 Mar  2  2011 ntp
-rw-r----- 1 root root     1173055 Apr  9 15:47 pk_backend_zypp
-rw-r----- 1 root root    12593599 Apr  3 07:30 pk_backend_zypp-1
-rw-r--r-- 1 root root        1607 Apr  9 15:38 pm-powersave.log
drwxr-xr-x 2 root root        4096 Apr  9 16:03 sa
drwxr-x--- 2 root root        4096 Mar  1  2011 samba
drwxr-x--- 2 root dialout     4096 Jul 28  2011 smpppd
-rw-r--r-- 1 root root          73 Dec  3 15:54 vboxadd-install-x11.log
-rw-r--r-- 1 root root      161155 Dec  3 15:53 vboxadd-install.log
-rw-r--r-- 1 root root       47556 Apr 18 12:50 warn
-rw-r--r-- 1 root root           0 Apr  8 11:33 webwatch
-rw-r--r-- 1 root root           0 Apr  8 11:33 webwatcherror
-rw-rw-r-- 1 root utmp      219264 Apr 18 11:54 wtmp
drwxr-xr-x 2 root root        4096 Jul 28  2011 zypp
-rw-r----- 1 root root     3049973 Apr  9 15:55 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**).

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

```
opensuse:~ # cat /etc/sysconfig/syslog
## Path:        System/Logging
## Description:     System logging
## Type:        list(0,1,2,3,4,5,6,7)
## Default:     1
## Config:      ""
## ServiceRestart:  syslog
#
# Default loglevel for klogd
#
```

```
KERNEL_LOGLEVEL=1

## Type:        string
## Default:     ""
## Config:      ""
## ServiceRestart:  syslog
#
# if not empty: parameters for syslogd
# for example SYSLOGD_PARAMS="-r -s my.dom.ain"
#
SYSLOGD_PARAMS=""

## Type:        string
## Default:     -x
## Config:      ""
## ServiceRestart:  syslog
#
# if not empty: parameters for klogd
# for example KLOGD_PARAMS="-x" to avoid (duplicate) symbol resolution
#
KLOGD_PARAMS="-x"

## Type:        list(syslogd,syslog-ng,rsyslogd,"")
## Default:     ""
## Config:      ""
## ServiceRestart:  syslog
#
# The name of the syslog daemon to use as syslog service:
# "syslogd", "syslog-ng", "rsyslogd" or "" for autodetect.
#
SYSLOG_DAEMON=""

## Type:           integer(0:5)
## Default:        ""
```

```
## Config:         ""
## ServiceRestart: syslog
#
# Version compatibility level to run rsyslogd with (-c parameter).
# Set to the desired version number rsyslogd shall be compatible with.
#
# Default is to run in native mode if the currently installed rsyslog
# daemon version.
#
# Note: Changes to this variable may need adoption of the config file
# or break features used in the /etc/init.d/syslog script by default.
#
RSYSLOGD_COMPAT_VERSION=""

## 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=""

## Type:           list(5)
## Default:        "5"
## Config:         ""
## ServiceRestart: syslog
```

```
#
# The native version compatibility level of the current rsyslogd.
#
# Note, that this variable is read-only -- please do not change it!
# Instead, please adopt the RSYSLOGD_COMPAT_VERSION variable.
#
# This variable will be updated while every installation/upgrade of
# the rsyslog daemon package.
#
RSYSLOGD_NATIVE_VERSION="5"
```

La directive **RSYSLOGD_COMPAT_VERSION** 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

Niveau	Priorité	Description
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
user	Message utilisateur
uucp	Message du système UUCP
local0 - local7	Réservés pour des utilisations locales

Configuration

Sous openSUSE, rsyslog est configuré par 2 fichiers principaux ainsi que par les fichiers éventuels se trouvant dans le répertoire **/etc/rsyslog.d** :

/etc/rsyslog.early.conf

```
opensuse:~ # cat /etc/rsyslog.early.conf
##
```

```
## WARNING: This config contains only statements that are
##          safe for early syslog start, that is before the
##          network and remote filesystems are available.
##
##          Don't include /etc/rsyslog.d/remote.conf
##          in this configuration file or enable any of the
##          additional (MYSQL, PGSQL, GSSAPI, GnuTLS, SNMP)
##          modules provided in separate module packages.
##
##
## if you experience problems, check
## http://www.rsyslog.com/troubleshoot for assistance
## and report them at http://bugzilla.novell.com/
##

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

$ModLoad immark.so   # provides --MARK-- message capability
$ModLoad imuxsock.so # provides support for local system logging (e.g. via logger command)
$ModLoad imklog.so   # kernel logging (may be also provided by /sbin/klogd)

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

###
#
# print most on tty10 and on the xconsole pipe
#
kern.warning;*.err;authpriv.none     /dev/tty10;RSYSLOG_TraditionalFileFormat
```

```
kern.warning;*.err;authpriv.none    |/dev/xconsole;RSYSLOG_TraditionalFileFormat
*.emerg                 *

# 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 $msg contains 'OUT=') then \
    -/var/log/firewall;RSYSLOG_TraditionalFileFormat
if  ($syslogfacility-text == 'kern') and \
    ($msg contains 'IN=' and $msg contains 'OUT=') then \
    ~

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

#
# NetworkManager into separate file and stop their further processing
#
```

```
if      ($programname == 'NetworkManager') or \
    ($programname startswith 'nm-') then \
    -/var/log/NetworkManager;RSYSLOG_TraditionalFileFormat
if      ($programname == 'NetworkManager') or \
    ($programname startswith 'nm-') then \
    ~

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

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

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

#
# the rest in one file
#
```

```
*.*;mail.none;news.none         -/var/log/messages;RSYSLOG_TraditionalFileFormat

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

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

###
```

/etc/rsyslog.conf

```
opensuse:~ # cat /etc/rsyslog.conf
##
## 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.
## [The modules are linked against libraries installed bellow of /usr
##  thus also installed in /usr/lib*/rsyslog because of this.]
##
## You can change it by adding network-remotefs to the Required-Start
## and Required-Stop LSB init tags in the /etc/init.d/syslog script.
##

#
```

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

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

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

$ModLoad imuxsock.so   # provides support for local system logging (e.g. via logger command)
                       # reduce dupplicate log messages (last message repeated n times)
$RepeatedMsgReduction on

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



#
# Use traditional log format by default. To change it for a single
# file, append ";RSYSLOG_TraditionalFileFormat" to the filename.
#
$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 /var/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                  *

# 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
&   ~


#
# 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
&   ~


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


#
# 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

###
```

/etc/rsyslog.d/remote.conf

```
opensuse:~ # cat /etc/rsyslog.d/remote.conf
##
## 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.
## [The modules are linked against libraries installed bellow of /usr
##  thus also installed in /usr/lib*/rsyslog because of this.]
##
## You can change it by adding network-remotefs to the Required-Start
## and Required-Stop LSB init tags in the /etc/init.d/syslog script.
##


# Remote Logging (we use TCP for reliable delivery)
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/spool/rsyslog # where to place spool files
#$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
# 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
# Note: as of now, you need to use the -t command line option to
# enable TCP reception (e.g. -t514 to run a server at port 514/tcp)
# This will change in later v3 releases.

# UDP Syslog Server:
#$ModLoad imudp.so  # provides UDP syslog reception
#$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
```

Dans ces trois fichiers nous pouvons identifier plusieurs sections :

- **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 à partir de serveurs rsyslog distants en utilisant le protocole **UDP**
$ModLoad imtcp.so	Active la réception de messages à partir de serveurs rsyslog distants en utilisant le protocole **TCP**

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

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

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

$ModLoad imuxsock.so   # provides support for local system logging (e.g. via logger command)
                       # reduce dupplicate log messages (last message repeated n times)
$RepeatedMsgReduction on

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

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 :

```
...
# UDP Syslog Server:
$ModLoad imudp.so  # provides UDP syslog reception
$UDPServerRun 514 # start a UDP syslog server at standard port 514
...
```

<note important> Les deux directives **$ModLoad imudp.so** et **$UDPServerRun 514** crée un **Écouteur** sur le port UDP/514. Le port 514 est le port standard pour un Écouteur de rsyslog. Dans le cas de la création d'un Écouteur TCP, il est nécessaire de décommenter la directive **$ModLoad imtcp.so** dans le fichier **/etc/rsyslog.d/remote.conf et** de fixer la valeur de la directive **RSYSLOGD_PARAMS** à **“-t514”** dans le fichier **/etc/default/syslog**. </note>

Pour envoyer l'ensemble des traces de journalisation vers un serveur rsyslog distant, il convient de modifier les lignes suivantes dans le fichier

/etc/rsyslog.d/remote.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. </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 :

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

Consultez la fin de votre syslog :

```
opensuse:~ # tail /var/log/messages
Apr 23 13:38:01 opensuse /USR/SBIN/CRON[11352]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 23 13:39:01 opensuse /USR/SBIN/CRON[11359]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 23 13:39:31 opensuse dhclient: XMT: Solicit on eth0, interval 124560ms.
Apr 23 13:40:01 opensuse /USR/SBIN/CRON[11366]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 23 13:41:01 opensuse /USR/SBIN/CRON[11373]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 23 13:41:35 opensuse dhclient: XMT: Solicit on eth0, interval 108800ms.
Apr 23 13:42:01 opensuse /USR/SBIN/CRON[11380]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 23 13:43:01 opensuse /USR/SBIN/CRON[11387]: (trainee) CMD (/bin/pwd > pwd.txt)
Apr 23 13:43:20 opensuse trainee: Linux est super
Apr 23 13:43:24 opensuse dhclient: XMT: Solicit on eth0, interval 129130ms.
```

Options de la commande

Les options de la commande logger sont :

```
opensuse:~ # logger --help
logger: invalid option -- '-'
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** :

```
opensuse:~ # 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/bzip2
uncompresscmd /usr/bin/bunzip2

# former versions had to have the compressext set accordingly
#compressext .bz2

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

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 :

```
opensuse:~ # 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

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

~~DISCUSSION:off~~

Donner votre Avis

{(rater>id=opensuse_11_l114|name=cette page|type=rate|trace=user|tracedetails=1)}