Version : **2020.01**

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

SO206 - Gestion de la Journalisation

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

Il est conseillé de déplacer le point de montage du répertoire **/var/adm** sur une tranche 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 tranche 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.

Gestion des journaux

Journalisation du Système

/var/sadm/system/logs

Ces répertoire contient les journaux générés par le processus d'installation de Solaris.

```
# ls /var/sadm/system/logs
begin.log                       install_launch.log_2019_11_29_1344
begin.log_2019_11_29            install_log
```

```
finish.log                          sysidtool.log
finish.log_2019_11_29
# cat /var/sadm/system/logs/begin.log
Executing begin script "install_begin"...
Begin script install_begin execution completed.
```

/var/adm/messages

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

```
# head /var/adm/messages
Nov 29 13:46:34 unknown genunix: [ID 672855 kern.notice] syncing file systems...
Nov 29 13:46:34 unknown genunix: [ID 904073 kern.notice]  done
Nov 29 13:26:09 unknown genunix: [ID 540533 kern.notice] ^MSunOS Release 5.10 Version Generic_147148-26 64-bit
Nov 29 13:26:09 unknown genunix: [ID 700403 kern.notice] Copyright (c) 1983, 2013, Oracle and/or its affiliates.
All rights reserved.
Nov 29 13:26:09 unknown unix: [ID 223955 kern.info] x86_feature: lgpg
Nov 29 13:26:09 unknown unix: [ID 223955 kern.info] x86_feature: tsc
Nov 29 13:26:09 unknown unix: [ID 223955 kern.info] x86_feature: msr
Nov 29 13:26:09 unknown unix: [ID 223955 kern.info] x86_feature: mtrr
Nov 29 13:26:09 unknown unix: [ID 223955 kern.info] x86_feature: pge
Nov 29 13:26:09 unknown unix: [ID 223955 kern.info] x86_feature: cmov
```

La commande /usr/sbin/dmesg

Les messages générés pendant le démarrage du système peuvent être visualisés grâce à la commande **dmesg** :

```
# dmesg | more

Tue Jan 14 13:45:26 CET 2020
Nov 30 06:22:09 solaris.i2tch.loc pseudo: [ID 129642 kern.info] pseudo-device: systrace0
```

```
Nov 30 06:22:09 solaris.i2tch.loc genunix: [ID 936769 kern.info] systrace0 is /pseudo/systrace@0
Nov 30 06:22:09 solaris.i2tch.loc pseudo: [ID 129642 kern.info] pseudo-device: fbt0
Nov 30 06:22:09 solaris.i2tch.loc genunix: [ID 936769 kern.info] fbt0 is /pseudo/fbt@0
Nov 30 06:22:09 solaris.i2tch.loc pseudo: [ID 129642 kern.info] pseudo-device: sdt0
Nov 30 06:22:09 solaris.i2tch.loc genunix: [ID 936769 kern.info] sdt0 is /pseudo/sdt@0
Nov 30 06:22:09 solaris.i2tch.loc pseudo: [ID 129642 kern.info] pseudo-device: fasttrap0
Nov 30 06:22:09 solaris.i2tch.loc genunix: [ID 936769 kern.info] fasttrap0 is /pseudo/fasttrap@0
Nov 30 06:22:09 solaris.i2tch.loc pseudo: [ID 129642 kern.info] pseudo-device: fcsm0
Nov 30 06:22:09 solaris.i2tch.loc genunix: [ID 936769 kern.info] fcsm0 is /pseudo/fcsm@0
--More--
```

Journalisation des Services

/var/svc/log

Ce répertoire contient les journaux des services :

```
# ls /var/svc/log | more
application-cde-printinfo:default.log
application-database-postgresql:version_81.log
application-database-postgresql:version_82.log
application-database-postgresql:version_82_64bit.log
application-database-postgresql_83:default_32bit.log
application-database-postgresql_83:default_64bit.log
application-font-fc-cache:default.log
application-gdm2-login:default.log
application-graphical-login-cde-login:default.log
application-management-dmi:default.log
application-management-ocm:default.log
application-management-seaport:default.log
application-management-sma:default.log
application-management-snmpdx:default.log
```

```
application-management-wbem:default.log
application-management-webmin:default.log
application-opengl-ogl-select:default.log
application-print-ipp-listener:default.log
application-print-ppd-cache-update:default.log
application-print-server:default.log
application-stosreg:default.log
milestone-devices:default.log
--More--
```

Journalisation Sécuritaire

/var/adm/sulog

Ce fichier contient la journalisation de l'utilisation de la commande **su** :

```
# tail /var/adm/sulog
SU 11/30 05:27 + console LOGIN-root
```

/var/adm/wtmpx

La commande **last** indique les dates et heures des dernières connexions des utilisateurs lues à partir du fichier binaire **/var/adm/wtmpx** :

```
# last
root      pts/2        2.2.0.10.rev.sfr Tue Jan 14 12:45   still logged in
root      sshd         2.2.0.10.rev.sfr Tue Jan 14 12:45   still logged in
reboot    system boot                   Tue Jan 14 12:44
reboot    system down                   Sat Nov 30 06:23
root      console      :0               Sat Nov 30 06:23 - down  (45+06:21)
root      pts/2        2.2.0.10.rev.sfr Sat Nov 30 06:22 - 06:23  (00:00)
root      sshd         2.2.0.10.rev.sfr Sat Nov 30 06:22 - 06:23  (00:00)
```

```
root      pts/2        2.2.0.10.rev.sfr Sat Nov 30 06:22 - 06:22  (00:00)
root      sshd         2.2.0.10.rev.sfr Sat Nov 30 06:22 - 06:22  (00:00)
reboot    system boot                   Sat Nov 30 06:22
reboot    system down                   Sat Nov 30 06:21
root      pts/3        :0.0             Sat Nov 30 06:20 - down   (00:01)
root      console      :0               Sat Nov 30 06:20 - down   (00:01)
reboot    system boot                   Sat Nov 30 06:19
reboot    system down                   Sat Nov 30 06:18
root      pts/3        :0.0             Sat Nov 30 06:17 - 06:17  (00:00)
root      console      :0               Sat Nov 30 06:17 - down   (00:02)
reboot    system boot                   Sat Nov 30 06:14
reboot    system down                   Sat Nov 30 06:14
root      pts/3        :0.0             Sat Nov 30 05:28 - down   (00:45)
root      console      :0               Sat Nov 30 05:28 - down   (00:45)
reboot    system boot                   Sat Nov 30 05:28
reboot    system down                   Sat Nov 30 05:27
reboot    system boot                   Fri Nov 29 17:41
reboot    system down                   Fri Nov 29 14:19
root      console      :0               Fri Nov 29 13:30 - down   (04:10)
reboot    system boot                   Fri Nov 29 13:26

wtmp begins Fri Nov 29 13:26
```

/var/adm/utmpx

La commande **whodo** indique qui fait quoi sur le système à l'instant **t**. L'information provient des fichiers **/var/adm/utmpx** et **/proc/<pid>** :

```
# whodo
Tue Jan 14 13:47:32 CET 2020
solaris.i2tch.loc

pts/2        root     12:45
    pts/2          822    0:00 sh
```

```
    pts/2          952    0:00 whodo
```

syslogd

Syslog

Syslog centralise les journaux du système grâce au daemon **syslogd**. Chaque daemon qui le souhaite peut communiquer avec syslogd via le port **514/udp** ou via une **socket unix**. Les messages de journalisation envoyés à syslogd sont taggés avec un **sous-système applicatif** et une **priorite**.

```
# cat /etc/services | grep 514/udp
syslog          514/udp
```

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

- ignorer les informations
- envoyer les informations à un syslogd sur une autre machine
- inscrire les informations dans un fichier sur disque
- transmettre les informations à un utilisateur
- transmettre les informations à tous les utilisateurs
- transmettre les informations à une application liée à syslogd via un tube

Sous-systèmes applicatifs

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

Sous-système applicatif	Description
auth	Message de sécurité / autorisation
security	Message de sécurité / autorisation
auth-priv	Message de sécurité / autorisation privé
cron	Message de cron ou at

Sous-système applicatif	Description
daemon	Message d'un daemon
ftp	Message du daemon ftp
kern	Message du noyau
local0 - local7	Message d'une application
lpr	Message du système d'impression
mail	Message du système de mail
news	Message du système de news
syslog	Message interne de syslogd
user	Message utilisateur
uucp	Message du système UUCP
mark	Message interne

Priorités

La priorité détermine l'importance des informations :

Priorité	Description
emerg	Système inutilisable
panic	Système inutilisable
alert	Action immédiate requise
crit	Condition critique atteinte
err (error)	Erreurs rencontrées
warn (warning)	Avertissements présentés
notice	Condition normale - message important
info	Condition normale - message simple
debug	Condition normale - message de débogage

/etc/syslog.conf

syslogd est configuré par le fichier **/etc/syslog.conf** :

```
# cat /etc/syslog.conf
#ident  "@(#)syslog.conf        1.5     98/12/14 SMI"   /* SunOS 5.0 */
#
# Copyright (c) 1991-1998 by Sun Microsystems, Inc.
# All rights reserved.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words.  Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice                   /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit        /var/adm/messages

*.alert;kern.err;daemon.err                     operator
*.alert                                         root

*.emerg                                         *

# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
#auth.notice                    ifdef(`LOGHOST', /var/log/authlog, @loghost)

mail.debug                      ifdef(`LOGHOST', /var/log/syslog, @loghost)

#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
ifdef(`LOGHOST', ,
user.err                                        /dev/sysmsg
user.err                                        /var/adm/messages
user.alert                                      `root, operator'
```

```
user.emerg                                          *
)
```

La syntaxe du fichier **/etc/syslog.conf** est la 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 : ***.emerg**.

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 : **root, operator**.

n Sélecteurs avec la même Action

Une Action peut s'appliquer à plusieurs Sélecteurs en les séparant par le caractère **;**, par exemple : ***.alert;kern.err;daemon.err**.

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

/usr/bin/logger

La commande **/usr/bin/logger** permet d'intégrer des informations dans syslog. 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 :

```
# logger -p user.err Unix est super
```

Consultez ensuite le fichier **/var/adm/messages**. Vous obtiendrez un résultat similaire à celui-ci :

```
# tail /var/adm/messages
```

```
# tail /var/adm/messages
Jan 14 12:44:54 solaris.i2tch.loc pseudo: [ID 129642 kern.info] pseudo-device: vol0
Jan 14 12:44:54 solaris.i2tch.loc genunix: [ID 936769 kern.info] vol0 is /pseudo/vol@0
Jan 14 12:44:54 solaris.i2tch.loc pseudo: [ID 129642 kern.info] pseudo-device: rsm0
Jan 14 12:44:54 solaris.i2tch.loc genunix: [ID 936769 kern.info] rsm0 is /pseudo/rsm@0
Jan 14 12:44:54 solaris.i2tch.loc pseudo: [ID 129642 kern.info] pseudo-device: pool0
Jan 14 12:44:54 solaris.i2tch.loc genunix: [ID 936769 kern.info] pool0 is /pseudo/pool@0
Jan 14 12:44:54 solaris.i2tch.loc ipf: [ID 774698 kern.info] IP Filter: v4.1.9, running.
Jan 14 12:44:56 solaris.i2tch.loc syslogd: line 24: WARNING: loghost could not be resolved
Jan 14 13:49:42 solaris.i2tch.loc root: [ID 702911 user.error] Unix est super
Jan 14 13:49:42 solaris.i2tch.loc root: [ID 702911 user.error] Unix est super
```

/usr/sbin/logadm

Les fichiers journaux grossissent régulièrement. Le programme **/usr/sbin/logadm** est utilisé pour effectuer des rotations de ces fichiers selon la configuration contenue dans le fichier **/etc/logadm.conf**.

Visualisez le fichier **/etc/logadm.conf** :

```
# cat /etc/logadm.conf
# Copyright (c) 2001, 2010, Oracle and/or its affiliates. All rights reserved.
#
#ident  "@(#)logadm.conf        1.8     10/04/12 SMI"
#
# logadm.conf
#
# Default settings for system log file management.
# The -w option to logadm(1M) is the preferred way to write to this file,
# but if you do edit it by hand, use "logadm -V" to check it for errors.
#
# The format of lines in this file is:
#       <logname> <options>
```

```
# For each logname listed here, the default options to logadm
# are given.  Options given on the logadm command line override
# the defaults contained in this file.
#
# logadm typically runs early every morning via an entry in
# root's crontab (see crontab(1)).
#
/var/log/syslog -C 8 -a 'kill -HUP `cat /var/run/syslog.pid`'
/var/adm/messages -C 4 -a 'kill -HUP `cat /var/run/syslog.pid`'
/var/cron/log -c -s 512k -t /var/cron/olog
/var/lp/logs/lpsched -C 2 -N -t '$file.$N'
/var/fm/fmd/errlog -N -s 2m -M '/usr/sbin/fmadm -q rotate errlog && mv /var/fm/fmd/errlog.0- $nfile'
/var/fm/fmd/fltlog -N -A 6m -s 10m -M '/usr/sbin/fmadm -q rotate fltlog && mv /var/fm/fmd/fltlog.0- $nfile'
smf_logs /var/svc/log/*.log -C 8 -s 1m -c
#
# The entry below is used by turnacct(1M)
#
/var/adm/pacct -C 0 -N -a '/usr/lib/acct/accton pacct' -g adm -m 664 -o adm -p never
#
# The entry below manages the Dynamic Resource Pools daemon (poold(1M)) logfile.
#
/var/log/pool/poold -N -s 512k -a 'pkill -HUP poold; true'
```

Dans ce fichier, le format de chaque ligne est :

```
nomjournal [espace] options
```

Les options les plus importantes de la commande sont :

Option	**Explication**
-C	Suppression des anciens fichiers de journalisation jusqu'à ce qu'il ne reste que **C** fichiers. Cette option définit donc le nombre d'anciens fichiers de journalisation à garder sur disque
-a	Exécuter la commande qui suit après la rotation de journal
-s	La rotation n'a lieu que si la taille du fichier de journalisation est égale ou supérieur à la valeur indiquée

Option	Explication
-P	La rotation n'a lieu qu'après la période indiquée

En règle générale, le renommage d'un fichier journal lors de la rotation de celui-ci suit une règle spécifique. Prenons l'exemple d'un fichier de journal nommé ***journal*** :

nom	Description
journal	Le fichier journal courant
journal.0	Le fichier journal avant la dernière rotation
journal.1	Le fichier journal avant l-avant-dernière rotation
