Chapitre VIII : Journalisation des événements

Eric Leclercq

Département IEM
http://ufrsciencestech.u-bourgogne.fr
http://ludique.u-bourgogne.fr/~leclercq

5 mars 2018

Aperçu

- La journalisation est une partie extrêmement importante de la sécurité d'un système
- C'est un complément à la protection réalisée par filtrage
- C'est un des piliers de la détection d'intrusions
- Une bonne gestion de la journalisation couplée à un mécanisme d'alerte/réponse automatique peut :
  - permettre une détection rapide des problèmes
  - faciliter l'étude des intrusions (ou des tentatives) éventuelles

Journalisation et aspects légaux

- La CNIL considère les logs (journaux) comme relevant du fonctionnement normal d'un prestataire informatique (qu'il soit public ou privé)
- Par conséquent ils ne sont donc pas soumis à déclaration à la CNIL
- `http://listes.cru.fr/droit-net/` propose une FAQ concernant les logs
- Les informations collectées à l'insu d'une personne ne peuvent être utilisées contre elle
- Il est donc préférable de clairement spécifier l'existence des logs dans une charte.

Architecture pour l'archivage des journaux

L'enregistrement des événements système est géré par deux programmes : `klogd` et `syslogd`. `syslogd` réaliser la plus grosse partie du travail en triant et en écrivant les messages dans des fichiers spécifiques.

- Une solution semi-centralisée est une bonne stratégie (serveur syslog) :
  - déporter une copie des logs
  - utilisér une machine spécialisée dans la gestion des traces
- une machine standard, dotée d'une bonne capacité disque (100Go) et surtout protégée des intrusions par la mise en place minimale de service de filtrage
- installer sur cette machine des outils de surveillance permettant d'avertir automatiquement les administrateurs (script de consultation des log, crontab, mail)
- installer un service d'archivage, un outil de statistiques et un service de sauvegarde

Architecture côté serveur

- Il est possible de mettre en place plusieurs serveurs syslog
- Il suffira alors de les ajouter aux lignes des fichiers de configuration
- Avec un petit serveur Linux les services offerts peuvent se limiter à :
  - ssh pour une connexion distante
  - `syslogd` (le démon syslog) :
    - attention `syslogd` effectue une synchronisation sur le disque à chaque écriture, ce qui le rend particulièrement consommateur de CPU
    - utiliser un tiret devant les nom de fichier pour eviter la synchronisation à chaque écriture mais veiller à mettre en place un système de fichier journalisé (ext3, xfs etc.)
  - syslog-ng est une version améliorée de syslog `http://www.balabit.hu/en/products/syslog-ng/`
  - synchronisation des horloges avec un client NTP
  - un interpréteur PERL (pour les scripts calculant les statistiques)

Architecture côté serveur

- Parmi les outils de surveillance des logs on peut noter :
  - LogSurfer `http://www.cert.dfn.de/eng/logsurf/`
  - Swatch scripts PERL en mode console
- un outil d'archivage qui compressera les logs générés à intervalle régulier (avec renommage afin de faciliter les recherches) : `logrotate` permet de réaliser ces actions
- Il existe cependant des outils spécialisés pour exploiter , synthétiser les logs des application les plus connues (awstat pour Apache, sag pour les journaux de squid).

Architecture côté client

- pour les machines Unix une configuration spécifique du démon `syslogd` est à définir
  - elle doit être suffisamment complète pour permettre d'avoir les renseigments nécessaires au but recherché
  - elle ne doit pas saturer des fichiers
  - ajouter ou modifier les lignes dans le fichier `/etc/syslog.conf` comme par exemple `*.kern @serveur.syslog.org`
- pour les machines Windows NT il est possible d'utiliser BackLog
- pour les switch, les routeurs (CISCO le propose) et les imprimantes

Configuration générale

- la configuration se fait via le fichier `/etc/syslog.conf`
- les lignes sont de la forme `facility.level action` ou `outil.niveau destination`
- le caractère `*` est utilisable pour les outils et les niveaux
- le lancement du démon syslog peut se faire avec `-r` pour autoriser ou non les connexions distantes
- `/etc/sysconfig/syslog` et `/etc/init.d/syslog`

```
auth,authpriv.*                                         /var/log/auth
auth,authpriv.*                                         @194.206.63.157

local7.*  /var/log/dhcpd.log

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure
authpriv.*                                              @194.206.63.157
# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog
```

Structure du fichier (outils) 1

- `auth` : informations concernant l'authentification (forme dépréciée, utiliser authpriv)
- `authpriv` : informations d'authentification (peut contenir des données comme le login et d'autres informations plus précises)
- `console` : messages à destination de `/dev/console` émis par le noyau ou par un pilote
- `cron` : messages de service `cron` ou `at`
- `daemon` : messages de démons commes `inetd`, `xinetd`, etc.
- `ftp` : messages du démon ftp
- `kern` : message du noyau (sur les systèmes Linux). Généralement ces messages sont passés en premier lieux à `klogd`
- `lpr` : messages des systèmes d'impression lpd, LPRng, etc.
- `mail` : message en provenance des démons de gestion du courrier comme `sendmail` ou `postfix`

Structure du fichier (outils) 2

- `mark` : commande interne pour générer des *timestamps*
- `news` : messages spécifiques de démon NNTP comme innd ou leafnode
- `security` : messages provennant de sous-systèmes assurant la sécurité (BSD)
- `syslog` : message provennant du démon syslog
- `user` : messages générés par des programmes utilisateurs
- `uucp` : messages du système UUCP
- `local0-local7` : Facilities used by customized programs (ie. in some programs you can tell it via a configuration file what facility to use, so you may opt to have OpenLDAP log to local0, OpenSSH to log to local1, and so forth)
- `*` : All facilities except mark

Structure du fichier (niveaux) 1

- `emerg` : The system is unusable
- `alert` : A condition exists that needs to corrected immediately
- `crit` : An error condition that indicates a program or subsystem may no longer be useable
- `err` : An error condition that indicates a component of a program or subsystem may no longer be useable
- `warning` : A warning message
- `notice` : A normal condition with significance
- `info` : An informational message
- `debug` : A debug message, usually a message that does not indicate any problems or have any normal significance
- `none` : No level, usually used as a facility exemption when using the wildcard
- `*` : All levels, except none

Structure du fichier (actions) 1

- `file or device` : The absolute pathname to a file (ie. /var/log/messages).
- The message will be written to the specified file. You can also use the full path to a device such as /dev/console, /dev/tty1, or /dev/lp0, etc.
- This can be useful for writing to a serial port, printer, or specific console. On Linux systems, you can prefix a file with the "-" character to tell syslog not to sync the file after every logging, which can have some performance benefits, but may also result in missing messages in the event of a system crash.
- `@hostname` : Messages are sent to specified hostname. The remote syslogd must be able to receive remote messages and must be configured for the selected facility.level being sent.

Structure du fichier (actions) 2

- `username` : Sends the message to the specified user(s) using write, provided they are logged in. Multiple users can be specified by using a comma-separated list (ie. root,vdanen,joe. To write to everyone, use "*".
- `named pipe` : The absolute path to a FIFO file (created with mkfifo), preceeded with the pipe (—) symbol. This tells syslog to write into the FIFO (pipe), and other programs like swatch can read from the FIFO and act on the message.