Utilisation de syslog pour la documentation de l'administration système

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 décembre 2005

https://www.bortzmeyer.org/doc-by-syslog.html

Sur tout site informatique un peu complexe, documenter les actions des administrateurs système est une tâche complexe. Idéalement, il faudrait qu'en plus d'installer, régler et réparer, l'administrateur système maintienne une épaisse documentation. Peu le font, parfois pour des mauvaises raisons (désir de garder ses petits secrets), parfois pour de bonnes (manque de temps). Pourquoi ne pas utiliser un outil déjà installé, syslog, pour pouvoir au moins effectuer le minimum de documentation ?

Merci à Sophie-Charlotte Barrière pour avoir imaginé cette technique.

Rien de plus agaçant que de passer des heures à déboguer un problème avant de s'apercvevoir qu'un collègue avait récemment fait un changement, sans le documenter. Bien sûr, il aurait dû le faire. Bien sûr, il aurait dû suivre les procédures ISO-quelquechose et rentrer dans le système de GED dix pages de textes pour dire simplement "j'ai ajouté un `/etc/logrotate.d/nsd` pour faire tourner les journaux". Mais n'y a t-il pas des solutions plus légères ?

Une raison que les administrateurs système donnent souvent à l'absence de documentation sur leurs actions est "Pas le temps", voire "Je le ferai demain" (ce qui n'arrive jamais car il y a d'autres choses à faire demain). Il faut donc une technique ultra-légère, et qui ne nécessite pas de changer de machine ou bien de lancer le seul navigateur Web avec lequel le CMS de documentation fonctionne.

syslog a toutes ces caractéristiques : il est très répandu, tout machine Unix l'a déjà. Il permet d'envoyer les évenements dans un fichier ou bien dans un programme ou encore être envoyé sur une machine centrale de traitement et d'achivage. Et il peut être appelé très rapidement avec le programme **logger**.

Enregistrer ses actions est donc aussi simple que de taper :

```
%  logger Ajout de /etc/logrotate.d/nsd
```

Et l'action sera enregistrée, avec le nom de la personne qui l'a effectue, et la date :

```
Nov 30 16:46:10 esther bortzmeyer: Ajout de /etc/logrotate.d/nsd
```

logger a plein d'options utiles. Par exemple, si l'action concerne la sécurité :

```
logger -p security.info Suppression de awstats
```

et, via sa configuration en `/etc/syslog.conf`, syslog va alors mettre le message dans un fichier différent et qu'on espère davantage lu. Il est important de soigner cet `/etc/syslog.conf` car ce n'est pas l'application qui décide du fichier ou système où le message va être enregistré, c'est le programme syslog.

On dispose ainsi d'un véritable journal des actions effectuées, qu'on peut ensuite consulter avec tail, grep ou l'excellent xlogmaster <http://www.gnu.org/software/xlogmaster/>. On peut aussi les trier avec Swatch <http://swatch.sourceforge.net/>.

Il peut être prudent de sauvegarder ce journal (tout Unix, par défaut, détruit régulièrement les vieux journaux, par exemple avec le programme logrotate).

Une autre solution pour trier facilement est d'avoir une facilité locale de syslog dédié à cette technique. Mettons qu'on utilise "local3", on peut alors définir un alias `alias logit="logger -p local3.info"` et une commande `logit Mise a jour du noyau` va alors automatiquement enregistrer avec cette facilité.