Journalisation d’un pare-feu avec MySQL — une méthode rapide et simple

Gazette Linux n°121 — Décembre 2005

Anonymous

Article paru dans le n°121 de la Gazette Linux de décembre 2005.
Traduction française par Deny <deny CHEZ: monaco POINT net>.
Relecture de la traduction française par Joëlle Cornavin <jcornavi CHEZ club TIRET internet POINT fr>.

Table des matières

La sécurité est un voyage, non une destination. Un grand pas vers la bonne direction consiste à passer en revue et à analyser de façon régulière vos journaux de pare-feu et vos messages syslog. Malheureusement, les fichiers journaux en texte clair produits par syslog ne sont pas dans une forme aisément analysée. En outre, à moins que vous n’employiez syslog-ng, vos journaux de pare-feu sont probablement dispersés parmi les nombreux fichiers journaux des messages du système.

Cet article vous montrera comment déplacer vos fichiers journaux de pare-feu depuis des fichiers texte syslog vers une base de données MySQL en 10 minutes ou presque. Les exemples suivants ont été réalisés sur un système SuSE 10.0®, mais vous pouvez facilement les adapter pour d’autres distributions.

1. Vérification de la configuration du noyau

Vous pouvez sauter cette étape si vous utilisez le noyau par défaut de la SuSE 10.0®. Les noyaux d'origine fournis avec la plupart des distributions devraient fonctionner sans problème, mais vous devrez vous assurer que vous avez compilé votre noyau avec les options `CONFIG_NETFILTER`, `CONFIG_IP_NF_IPTABLES`,`CONFIG_IP_NF_FILTER` et `CONFIG_IP_NF_TARGET_ULOG`. La plupart des pare-feux auront également besoin de `CONFIG_IP_NF_CONNTRACK`, `CONFIG_IP_NF_FTP` et de `CONFIG_IP_NF_IRC`.

Si vous avez un fichier appelé `/proc/config.gz`, cela signifie que votre noyau a été compilé avec l'option `IKCONFIG`. Comme `/proc/config.gz` est la version compressée du fichier `.config` qui a été utilisé pour générer le noyau, vous pouvez vérifier si vous avez les options nécessaires pour netfilter et ulog à l'aide de cette commande :

S'ils ne sont pas activés en tant que modules ou compilés dans le noyau, vous devrez les changer et recompiler le noyau. Dans menuconfig, activez les options suivantes :

Vous pourriez également être amené à vérifier que iptables est compilé avec la prise en charge de ulog.

2. Installation de MySQL

Vous pouvez aller directement section 2.1. si vous avez déjà MySQL installé. Autrement :

Si vous utilisez SuSE® et que apt4rpm (http://linux01.gwdg.de/apt4rpm/) n'est pas installé sur votre système, je vous recommande fortement de l'installer, car il simplifiera considérablement la gestion de vos paquetages.

Vous devez également choisir un mot de passe pour l'utilisateur *root* de MySQL :

2.1. Initialisation de la base de données

Saisissez :

puis votre mot de passe à l'invite. Une fois connecté dans votre base de données MySQL, saisissez les commandes suivantes pour préparer la base de données à recevoir les journaux de pare-feu provenant de ulog.

Que s'est-il donc produit ici ?

- Nous avons créé une base de données ulogdb pour y héberger nos fichiers journaux.
- Nous avons exécuté le scriptSQL ulogd.mysqldump, préparant la base de données pour nulog-php. Il permet de stocker plus d'informations que la table MySQL fournie avec ulogd, et vous pouvez le trouver dans le répertoire de scripts de nulog-php ou ici (outils/lg121-A/ulogd.mysqldump).
- Nous avons créé un utilisateur « ulogd » (avec comme mot de passe « ulogpass ») pour avoir un accès en lecture/écriture à cette base de données. Je vous recommande vivement de saisir un mot de passe différent de celui qu'emploie cet exemple.

3. Installation de ulogd

Installez le démon de journalisation ulogd :

3.1. Configuration de `ulogd.conf`

Éditez `/etc/ulogd.conf` pour faire correspondre ce que nous avons mis en place précédemment :

Remplacez le mot de passe ***`ulogpass`*** par le mot de passe que vous avez fixé dans la commande **GRANT** dans votre base de données MySQL. À présent, décommentez la ligne suivante pour envoyer les données à MySQL :

et commentez les deux lignes suivantes pour interdire la journalisation dans un fichier texte :

Redémarrez maintenant le démon ulogd et réglez-le pour qu'il soit automatiquement démarré au moment de l'amorçage avec chkconfig :

4. Redirection de la journalisation de iptables

La commande **sed** suivante commute toutes vos règles iptables pour les journaliser via ULOG. Nous supposerons que vous stockez votre ensemble de règles iptables dans un fichier appelé « iptables » (habituellement dans `/etc/sysconfig/` ou `/var/lib/`) :

Votre configuration est à présent terminée ! Tous les journaux provenant de votre pare-feu sont à présent consignés dans votre base de données MySQL. N'oubliez pas de mettre à jour votre script de démarrage de pare-feu de façon à ce que les nouvelles règles iptables soient prises en compte.

5. Importation de vos anciens journaux

Jusqu'ici, tout se déroule bien, mais vous aimeriez probablement avoir vos anciens journaux dans MySQL également. Voici un petit script perl (outils/lg121-A/nf2mysql.pl.txt) pour vous permettre d'importer vos anciens fichiers journaux texte dans MySQL. Certaines des expressions régulières sont réutilisées depuis adcfw-log (http://adcfw-log.sourceforge.net/). Vous pouvez habituellement trouver vos journaux netfilter dans `/var/log/`*`firewall-XXXXXX.gz`* ou `/var/log/`*`messages-XXXXXX.gz`*. Pour importer :

Répétez cette procédure pour chacun de vos autres fichiers journaux. Pour convertir un fichier journal actuel (ou un autre fichier journal décompressé) tel que `/var/log/messages` ou `/var/log/firewall` :

C'est tout !

6. Analyse des résultats

Pour analyser vos journaux dans MySQL, vous pouvez faire appel à nulog (http://www.inl.fr/Nulog.html) ou webfwlog (http://webfwlog.sourceforge.net/).

7. Liens

Cet article a été en partie inspiré par cet article (http://www.wikilearning.com/logear_netfilter_en_una_base_de_datos-wkccp-673-1.htm) (disponible uniquement en espagnol).

La page originale de ulog se trouve ici (http://gnumonks.org/gnumonks/projects/project_details?p_id=1).

Si vous souhaitez approfondir et journaliser tous les messages système dans MySQL, jetez un coup d’œil à ce wiki : http://gentoo-wiki.com/HOWTO_setup_PHP-Syslog-NG.

Voici (http://www.computerworld.com/printthis/2005/0,4814,105905,00.html) une raison d’abandonner la journalisation habituelle depuis un fichier texte.

Si vous n’avez pas déjà votre iptables configuré, vous pouvez facilement construire un ensemble de règles satisfaisant avec shorewall (http://www.shorewall.net/), firehol (http://firehol.sourceforge.net/) ou firestarter (http://www.fs-security.com/).

> A. N. Onymous écrit pour la LG depuis ses débuts — généralement en s’introduisant furtivement de nuit et en laissant divers articles sur le bureau du rédacteur en chef. Un homme (une femme ?) mystérieux(se), ne demandant aucun remerciement et se cachant dans l’obscurité... probablement cela a-t-il un rapport avec un immense trésor dans un ancien temple maya et une belle femme aux yeux sombres avec un serpent tatoué ondulant vers le bas de sa hanche gauche. Ou peut-être est-il jaloux de son intimité. Quoi qu’il en soit, nous lui sommes reconnaissants pour sa contribution.
>
> — Ben