Nom : Romain Quarré
Section : 5I option Sécurité Réseaux
Système : Ubuntu 8.10 **noyau** 2.6.27-11-generic
Daemon utilisé : Syslogd 1.5-2
Shell utilisé : Bash version 3.2.39(1)

Administration et sécurité sous Unix

Le démon Syslogd

Sommaire

INTRODUCTION

La journalisation est une part extrêmement importante de la sécurité et c'est un des seuls outils à notre disposition pour la surveillance du système. Elle est un complément à la protection et c'est un des piliers de la détection d'intrusion. On ne peut se contenter d'une détection d'intrusion cantonnée à l'entrée du réseau. Les pirates réussissent parfois à entrer, ou ils peuvent être internes à l'organisme. Une bonne gestion de la journalisation couplée à un logiciel de réponse automatique va permettre une détection rapide des problèmes et faciliter l'étude post-mortem de l'intrusion.
La journalisation sert toutefois essentiellement à la surveillance du système. C'est le principal outil dont dispose l'administrateur. Il faut toutefois trouver le bon compromis, car la journalisation utilise des ressources CPU et disque. Une journalisation importante est parfois nécessaire lors de l'implantation d'un nouveau service, mais il faut bien vérifier qu'elle est nécessaire par la suite. On notera également que la journalisation des événements sert également a des fins de statistiques ou de facturation. Sur les systèmes UNIX/Linux il existe un démon principal gérant la journalisation d'événement. C'est le démon **Syslogd.** Ce démon reçoit des messages événementiels de la part de clients (locaux ou distants) Syslog (par exemple named, sendmail, etc..) ou du démon **Klogd** qui est chargé d'écouter les messages du noyau et de les envoyer au démon Syslogd pour que celui-ci les journalise suivant son fichier de configuration. Dans ce dossier nous nous focaliserons principalement sur l'étude du démon Syslogd (communément appelé Syslog). Klogd ne sera donc pas étudié dans les détails. Au niveau réseau, on précisera que le démon Syslog est un processus de niveau applicatif (couche 7 modèle OSI) utilisant comme port quand le serveur syslog est configuré pour écouter sur le réseau le port UDP 514 (protocole Syslog).

INSTALLATION

Sur la plupart des distributions UNIX/LINUX, Syslogd (et ses sous programmes dépendants tels que Klogd) sont installés de base avec la distribution. (C'est donc biensur le cas avec la version d'Ubuntu précisée dans l'entête sur la page d'accueil). Néanmoins, s' il y a un problème il est toujours possible de désinstaller Syslog et de le réinstaller. Je vais expliquer différente manière possible d'installer (réinstaller) Syslogd.

Installer,désinstaller ou réinstaller Syslog

Synaptic : Sous Ubuntu via Synaptic (substitut graphique d'aptitude)si la machine dispose d'un serveur X11, choisir la réinstallation, suppression totale (avec les fichiers de configuration) ou partielle (les fichiers de configuration restent).

Aptitude en mode shell :

Pour supprimer toute trace précédente : **sudo apt-get remove sysklogd**
Pour installer le paquet syslogd et ses dépendances : **sudo apt-get install/reinstall sysklogd**

On peut également installer le paquet avec tout autre gestionnaire de paquet (dpkg,yum,rpm,etc..). Le dépôt qui contient le paquet est en général présent dans le sources.list. Dans le cas d'une compilation en utilisant les fichiers sources, on peut installer le programme après l'avoir dezipé en tapant la liste de commande suivantes :

./configure
Make
Make install

Une fois le programme installé, on peut vérifier sa présence suivant son mode d'installation en tappant

```
romain@pc-rom1:~$ dpkg -l | grep sysklog
ii  sysklogd                      1.5-2ubuntu6                    System Logging Daemon
romain@pc-rom1:~$
```

Pour les systèmes debian. Ou encore :

```
romain@pc-rom1:~$ aptitude show sysklogd
Paquet : sysklogd
État: installé
Automatiquement installé: non
Version : 1.5-2ubuntu6
```

Chaque gestionnaire de paquet offre des options pour vérifier pour vérifier si un paquet est installé ou non. Dans le cas d'une installation via la compilation, on peut rechercher des traces de fichiers (scripts,binaires, etc) en faisant un find ou un locate (mettre avant la base de donnée des fichiers installés a jour avec la commande updatedb). Il est également interessant de regarder quels fichiers sont installés par le paquet à l'aide de la commande dpkg –L sysklogd.

CONFIGURATION ET FONCTIONNEMENT

Une fois le programme syslog installé, on peut vérifier s'il est actif ou non en tappant :

```
romain@pc-rom1:~$ ps -ef | grep log
syslog    4254     1  0 12:19 ?        00:00:01 /sbin/syslogd -u syslog
root      4295     1  0 12:19 ?        00:00:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
klog      4297     1  0 12:19 ?        00:00:00 /sbin/klogd -P /var/run/klogd/kmsg
```

On voit bien que le binaire syslogd (lancé par le script de démarrage sysklogd) est actif en mémoire et a comme PID 4254.

Le programme Syslogd est en général lancé au démarrage tout comme le programme klogd (qui travaille en général avec syslogd). Tous deux sont présents dans les répertoires rcX.d/ sous forme de liens vers les scripts de démarrage des services (S10syslogd).
Nous allons à présent expliquer et détailler le fonctionnement du service syslogd. Le binaire syslogd présent comme montré dans la précédente capture dans **/sbin/** est lancé par le script de démarrage **/etc/init.d/sysklogd** lorsque celui-ci est invoqué avec un argument de type start ou restart. Au démarrage du programme, le fichier de configuration **/etc/syslog.conf** qui est le fichier de configuration principal de syslogd est lu. Nous aborderons un peu plus tard ce fichier de configuration. La liste des bibliothèques utilisées par le démon s'obtient grâce à la commande **ldd** dont nous n'allons pas afficher le résultat ici, celui-ci n'ayant que peu d'intérêt.

Le paquet (ou fichiers installés après une compilation) sysklogd contient un certain nombre de fichiers (binaires, fichiers de configurations, fichier de documentations, etc..) qui vont être listés et expliqués pour certain pour mieux comprendre le fonctionnement global. En tapant dpkg –L sysklogd on obtient la liste des fichiers installés avec le paquet. On peut voir les fichiers :

```
/etc/cron.daily/sysklogd
/etc/cron.weekly/sysklogd
/etc/default/syslogd
/etc/init.d/sysklogd
/etc/syslog.conf
/sbin/syslogd
/usr/sbin/syslog-facility
/usr/sbin/syslogd-listfiles
/usr/share/doc/sysklogd/changelog.Debian.gz
/usr/share/doc/sysklogd/changelog.gz
/usr/share/doc/sysklogd/copyright
/usr/share/doc/sysklogd/readme.txt.gz
/usr/share/man/man5/syslog.conf.5.gz
/usr/share/man/man8/sysklogd.8.gz
/usr/share/man/man8/syslog-facility.8.gz
/usr/share/man/man8/syslogd-listfiles.8.gz
/usr/share/man/man8/syslogd.8.gz
/usr/share/sysklogd/dummy
```

On voit dans l'ensemble de ces fichiers outre le binaire principal /sbin/syslogd le fichier binaire **/usr/sbin/syslogd-listfiles** et /**usr/sbin/syslog-facility**. Ils constituent les 3 fichiers binaires de l'ensemble syslog.
Le binaire syslogd-listfiles a pour but de sélectionner le fichier de logs le plus adapté a une rotation (en général le fichier le plus volumineux) dans les fichiers de logs listés dans /etc/syslog.conf. Ce binaire est lancé par les scripts **/etc/cron.daily/sysklogd et /etc/cron.weekly/sysklogd** qui s'exécutent a période constante. Le fichier binaire **syslog-facility** sert a installer ou désinstaller une nouvelle priorité a un message dans le fichier de configuration syslog.conf.

Il est à noter que le démon syslogd par défaut n'écoute PAS sur le réseau et reçoit donc des messages événementiels en local à l'aide d'une socket Unix domain. Cette socket est en réalité un fichier spécial appelé FIFO se comportant comme une liste d'attente dans lequel le démon va lire. Il s'agit en réalité du fichier **`/dev/log`**. Un programme C peut donc envoyer des messages à Syslogd en écrivant directement dans ce fichier. Il est cependant possible de modifier le comportement par défaut du processus en lui demandant d'écouter les messages sur le réseau via le protocole syslog en utilisant le port UDP 514. Pour configurer cela, on aura besoin de rajouter l'option –r lors du lancement du script de démarrage sysklogd ou alors, on modifie le fichier de configuration **/etc/default/syslogd** ou le script /etc/init.d/sysklogd en rajoutant l'option –r à la variable SYSLOGD

```
#! /bin/sh
# /etc/init.d/sysklogd: start the system log daemon.
PATH=/bin:/usr/bin:/sbin:/usr/sbin
pidfile=/var/run/syslogd.pid
binpath=/sbin/syslogd
test -x $binpath || exit 0
# Options for start/restart the daemons
#   For remote UDP logging use SYSLOGD="-r"
#
SYSLOGD="-r"
```

Pour modifier les fichiers de configuration qui appartiennent à root, il faut obligatoirement avoir les droits de super-utilisateur. Les fichiers de configuration ont les droits de lecture uniquement pour tout le monde sauf root qui a en plus les droits d'ecriture. Les fichiers de configuration cron ont tous les droits en mode root, le droit x en plus pour les utilisateurs du groupe root, et les autres n'ont toujours que le droit r. Pour ce qui concerne les binaires et les fichiers scripts, root a toujours tous les droits, les membres du groupe root ont les droits x et r et les autres n'ont que le droit d'execution.

Nous allons maintenant étudier le fichier de configuration du démon syslogd. Lors de son lancement, **syslogd** lit le fichier /etc/syslog.conf, et en déduit dans quel fichier doit être enregistré chaque message. Chacun d'eux est composé de trois parties distinctes : la priorité, le service et le texte qui devra être enregistré dans l'historique. C'est en fonction de la priorité du message et du service qui l'a généré que syslog déterminera dans quel fichier enregistrer le message. Dans syslog.conf, on définit donc ce que l'on veut tracer, le niveau de traçabilité et où on doit envoyer la trace.

Exemple : `mail.info /var/log/mail.info`

Chaque ligne est de la forme :

```
Service.Priorité Destination
```

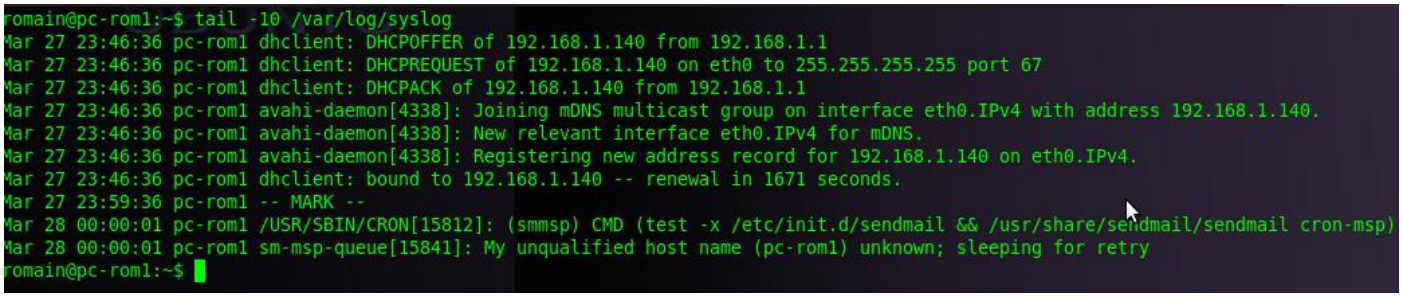
- Service correspond au type de programme (Démon, Noyau,...) et doit être l'un de ces mots-clés : auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, security (identique à auth), syslog, user, uucp et local0 à local7.
- Priorité représente le niveau de gravité du message et doit être l'un de ces mots clés : debug, info, notice,

warning, warn (identique à warning), err, error (identique à err), crit, alert, emerg, panic (identique à emerg). ATTENTION : En indiquant un niveau, syslog enverra les messages de ce niveau et tous les messages des niveaux plus importants. Donc en mettant « debug », syslog enverra tous les messages (de debug à panic).

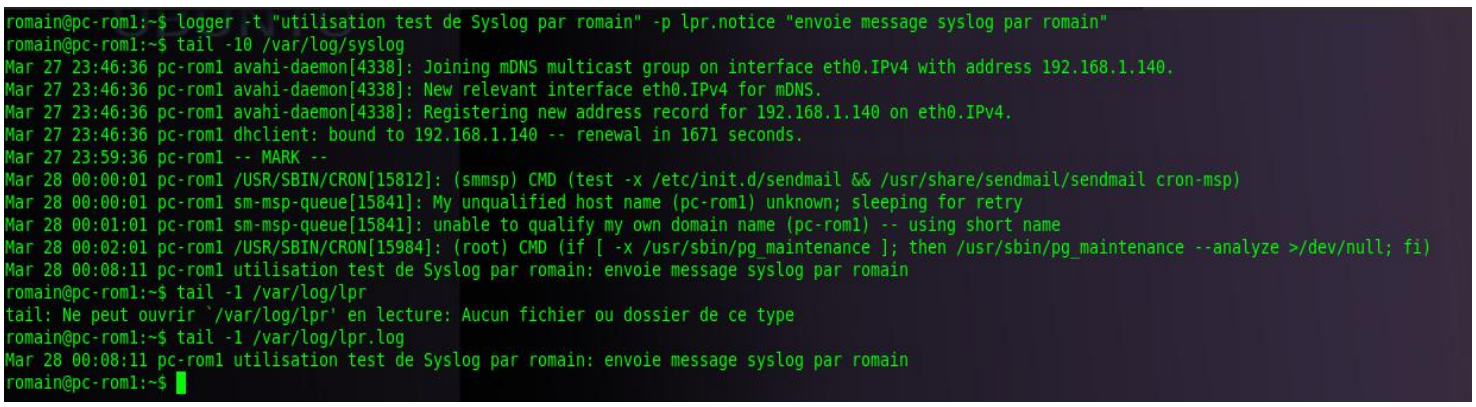
- Destination représente la destination du message et peut être un chemin vers un fichier texte (ex : /var/log/mail.info) ou le nom d'une console pour envoyer les messages à l'écran (ex : /dev/tty8) ou un autre serveur (ex : @MonAutreServeur).

Remarque : Chaque programme détermine les « Services » et les « Priorités » qu'il utilise et il est rarement possible de les modifier. Par exemple, les programmes Postfix et Fetchmail utilisent la Service « mail ».
Ne pas oublier qu'après chaque modification d'un fichier de configuration, il faut relancer le script de démarrage du service pour que les changements soient pris en compte.

Le service syslog enregistre les logs qu'il reçoit en fonction des paramètres présents dans syslog.conf. Ainsi, tous les logs sauf les logs d'authentification seront présents dans le fichier /var/log/syslog et seront également répartis grace au démon dans d'autres fichiers de logs correspondant a un meme service et a un niveau de criticité. Pour exemple, voici la liste des 10 derniers logs présents dans /var/log/syslog.conf



Afin de vérifier le bon fonctionnement du service, on peut déjà taper la commande /etc/init.d/sysklogd status qui devrait retourner « syslogd is running ». Ensuite, on dispose de la commande « logger » qui nous permet d'envoyer a la demande un message a syslog. La vérification du contenu des fichiers de log nous prouvera si le fichier a été reçu ou non, donc si le démon fonctionne correctement. Cet exemple est illustré dans la capture suivante ou l'on peut s'apercevoir que j'envoie un message de type lpr (service d'impression) au démon syslog à l'aide de la commande logger. On peut vérifier que le message est bien présent dans /var/log/syslog et dans le fichier de le fichier de log concerné /var/log/lpr.log



On peut donc conclure d'après ce test que localement le démon syslogd fonctionne correctement. Penchons nous maintenant sur le cas ou le démon écoutera sur le réseau via le port UDP 514 afin de centraliser les logs que lui forwardent les autres ordinateurs. Il va falloir modifier le fichier de configuration syslog.conf comme expliqué précédemment et ajouter à la variable SYSLOGD la valeur ' –r ' puis relancer le service. Pour le poste qui génèrera le message, il faudra configurer dans syslog.conf pour le service lpr, non pas un chemin local mais l'adresse IP de la machine qui centralisera les logs. Refaisons la même expérience à partir d'un autre poste du réseau

```
romain@pc-rom1:~$ sudo /etc/init.d/sysklogd restart
 * Restarting system log daemon...
romain@pc-rom1:~$ sudo nmap -sU 127.0.0.1

Starting Nmap 4.62 ( http://nmap.org ) at 2009-03-28 00:52 CET
Interesting ports on localhost (127.0.0.1):
Not shown: 1483 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
514/udp  open|filtered syslog
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 1.421 seconds
romain@pc-rom1:~$
```

Le port UDP 514 est a présent ouvert car le démon syslogd est maintenant en écoute de message sur le réseau. Un nmap sans avoir mis l'option –r dans la variable SYSLOGD du fichier /etc/default/syslogd n'aurait pas indique le port 514 en ouvert mais en fermé. Sur la machine (famille-server.home) qui va envoyer le message lpr au serveur syslog (pc-rom1) on a configuré dans /etc/syslog.conf en face du champs lpr.* la valeur de l'adresse IP de la machine a qui envoyer le message (a la place du fichier local /var/log/lpr.log) soit @192.168.1.140 (ip du serveur syslog). Puis je redémarre le service puis tape la meme commande que précédemment avec la commande logger sur le pc distant. Voici la trace de /var/log/syslog du serveur montrant que le démon syslog a bien receptionné le message forwardé par famille-server.home

```
romain@pc-rom1:~$ tail -5 /var/log/syslog
Mar 28 00:52:53 pc-rom1 syslogd 1.5.0#2ubuntu6: restart (remote reception).
Mar 28 01:00:01 pc-rom1 /USR/SBIN/CRON[17104]: (smmsp) CMD (test -x /etc/init.d/sendmail && /usr/share/sendmail/sendmail cron-msp)
Mar 28 01:00:02 pc-rom1 sm-msp-queue[17132]: My unqualified host name (pc-rom1) unknown; sleeping for retry
Mar 28 01:01:02 pc-rom1 sm-msp-queue[17132]: unable to qualify my own domain name (pc-rom1) -- using short name
Mar 28 01:06:47 famille-serveur.home utilisation réseau syslog: envoie message lpr via reseau
romain@pc-rom1:~$
```

On voit bien a la dernière ligne que le serveur a bien réceptionné le message du client distant famille-server.home. Ces 2 exemples ont donc démontré l'utilisation du démon syslogd via une utilisation locale ou via le réseau. Ces tests attestent du bon fonctionnement du service.

SECURITE

La première des règles de sécurité est d'avoir les démons mis à jour pour corriger d'éventuels bugs. En effet, si un démon plante, on a un défaut de disponibilité de service (la disponibilité étant un des piliers de la sécurité). De la même manière, les programmes étant conçu par des humains ne sont pas exempt de failles qu'un individu maicieux pourra exploiter (nous en donnerons une liste non exhaustive dans la suite de cette documentation). Ainsi pour réaliser la mise a jour d'un démon, on peut utiliser la commande :

Apt-get install sysklogd

Si le paquet est la dernière version disponible, le résultat de la commande le notifiera sinon le paquet sera mis a jour. Pour connaitre la version d'un paquet on peut taper la commande : **aptitude show sysklogd.** On peut ensuite comparer la version de son paquet avec ce qui se trouve sur internet par exemple.

Il y une possibilité que le démon syslogd soit utilisé comme passage pour une attaque de déni de service. Un programme(ur) malicieux pourrait très simplement noyer le démon syslogd avec des messages, ce qui conduirait les journaux à remplir toute la place restante du système de fichiers. Activer la journalisation à travers la socket de domaine internet exposera le système à des risques extérieurs vis-à-vis des programmes ou des utilisateurs de la machine locale.

Il y a de nombreuses méthodes pour protéger cette machine :

1. Implémenter le pare-feu du noyau pour limiter les hôtes ou les réseaux ayant accès à la socket 514/UDP.

2. La journalisation peut être dirigée vers un système de fichiers isolé ou non-racine qui, s'il est plein, n'impactera pas la machine.

3. Le système de fichiers ext2 peut être utilisé en le configurant pour limiter un certain pourcentage du système de fichier pour une utilisation par root seulement. REMARQUEZ que cela obligera à lancer syslogd comme processus non root. REMARQUEZ AUSSI que cela empêchera l'utilisation de la journalisation distante, puisque syslog sera incapable de lier la socket 514/UDP.

4. Désactiver la socket de domaine internet limitera les risques sur la machine locale.

Pour palier aux quelques problèmes de sécurité que propose le démon syslogd, on trouve des améliorations de ce démon appelés syslog -ng ou on trouve encore le démon rsyslog

REFERENCES

http://fr.wikipedia.org/wiki/Syslog Informations générales sur le service

http://www.karlesnine.com/tag/syslogd Manuel francais de Syslogd

http://www.coagul.org/spip.php?article210 Configuration de syslogd (syslog.conf)