

# Debian Lenny - Éléments de sécurisation

Debian GNU/Linux



Matthieu Vogelweith  
24 février 2009

# Résumé

Ce document a été rédigé en LaTeX en utilisant l'excellent Vim sous Debian GNU/Linux. Il est disponible aux formats [XHTML](#) et [PDF](#). Les sources LaTeX sont disponibles ici : [L<sup>A</sup>T<sub>E</sub>X](#)

# Licence

Copyright ©2009 Matthieu VOGELWEITH <matthieu@vogelweith.com>.

Vous avez le droit de copier, distribuer et/ou modifier ce document selon les termes de la GNU Free Documentation License, Version 1.3 ou ultérieure publiée par la Free Software Foundation ; avec aucune section inaltérable, aucun texte de première page de couverture, et aucun texte de dernière page de couverture. Une copie de la licence est disponible dans la page [GNU Free Documentation License](#).

# Table des matières

<b>Table des matières</b>	<b>3</b>
<b>1 Les bases</b>	<b>4</b>
1.1 Un système minimal . . . . .	4
1.2 Système de messagerie . . . . .	4
1.3 Pare feu . . . . .	4
<b>2 Surveillance des journaux</b>	<b>5</b>
2.1 Logcheck . . . . .	5
2.2 Personnalisation . . . . .	5
<b>3 Les mises à jour de sécurité</b>	<b>6</b>
3.1 Mises à jour APT . . . . .	6
3.2 Checkrestart . . . . .	6
3.3 Cron-apt . . . . .	7
3.4 La liste de diffusion Security . . . . .	7
<b>4 Intégrité du système</b>	<b>8</b>
4.1 Présentation . . . . .	8
4.2 debsums . . . . .	8
4.3 rkhunter . . . . .	8
4.4 integrit . . . . .	9
<b>5 Sécurité des services</b>	<b>10</b>
5.1 Généralités . . . . .	10
5.2 SSH . . . . .	10
<b>6 Références</b>	<b>11</b>

# Chapitre 1

## Les bases

### 1.1 Un système minimal

- Le script nécessaire installé.

### 1.2 Système de messagerie

- reception des alertes mails

### 1.3 Pare feu

En complément des éléments indiqués dans cette page, il est indispensable de protéger la machine par un pare feu adapté aux services qui tournent sur la machine. La mise en place d'un pare feu basé sur Shorewall est détaillée dans le document suivant : [1].

## Chapitre 2

# Surveillance des journaux

### 2.1 Logcheck

La surveillance des journaux est essentielle pour apprécier l'état d'un système. Cette surveillance est par contre très complexe dans le sens où il faut arriver à détecter simplement les messages critiques des messages d'informations. Pour cela il existe plusieurs outils qui vont "épurer" les journaux automatiquement pour ne remonter que les informations qui nécessitent une attention particulière. Parmi eux on peut distinguer Logcheck [2] qui est à la fois très puissant et très souple dans sa configuration. L'installation se fait avec la commande suivante :

```
# aptitude install logcheck logcheck-database
```

Le paquet supplémentaire **logcheck-database** installé avec la commande ci-dessus fournit un ensemble de règles permettant de filtrer les journaux. Pour chaque service, il fournit une ou plusieurs expressions régulières qui excluent les informations "non critique" des journaux.

### 2.2 Personnalisation

Il est tout à fait possible d'ajouter de nouvelles règles pour affiner le traitement des journaux. Par exemple, on peut estimer qu'il n'est pas intéressant de recevoir les lignes indiquant que Shorewall a "DROPPED" un paquet. Pour cela, il suffit de créer un fichier `/etc/logcheck/ignore.d.server/shorewall` contenant la ligne suivante :

```
^\w{3} [ :[:digit:]]{11} [._[:alnum:]-]+ kernel: \[[ 0-9\.]*\] Shorewall:[[:alnum:]]+:  
DROP:IN=
```

Ainsi, les journaux seront conservés dans le syslog mais ne seront pas reportés par logcheck dans l'alerte. Par ailleurs, voici un fichier contenant quelques règles utiles pour affiner le traitement des journaux que l'on peut mettre dans un fichier `/etc/logcheck/ignore.d.server/custom` : [3]

## Chapitre 3

# Les mises à jour de sécurité

### 3.1 Mises à jour APT

Dans `/etc/apt/sources.lists` :

```
# Security updates
deb http://security.debian.org/ lenny/updates main contrib non-free
```

Faire des mises à jour journalières, aidé par exemple de `cron-apt`.

### 3.2 Checkrestart

Après une mise à jour de sécurité, il est important de vérifier que tous les services impactés par ces mises à jour ont bien été redémarrés. Lors de la mise à jour d'une library par exemple, il est possible que des services utilisent encore l'ancienne version de la library jusqu'à ce qu'ils soient redémarrés.

Pour détecter ce type de problèmes, le paquet **debian-goodies** fournit l'utilitaire **checkrestart** qui va rechercher tous les services utilisant une version obsolète d'un librairie :

```
# aptitude install debian-goodies
# checkrestart
Found 12 processes using old versions of upgraded files
(1 distinct program)
(1 distinct packages)

Of these, 1 seem to contain init scripts which can be used to restart them:
The following packages seem to have init scripts that could be used
to restart them:
apache2-mpm-prefork:
  27676 /usr/sbin/apache2
  31279 /usr/sbin/apache2
  30910 /usr/sbin/apache2
  5565  /usr/sbin/apache2
  2047  /usr/sbin/apache2
  26909 /usr/sbin/apache2
  25558 /usr/sbin/apache2
  25991 /usr/sbin/apache2
  30891 /usr/sbin/apache2
  30628 /usr/sbin/apache2
  31289 /usr/sbin/apache2
  31288 /usr/sbin/apache2
```

```
These are the init scripts:  
/etc/init.d/apache2 restart
```

Dans l'exemple ci-dessus, `checkrestart` a détecté que Apache utilise une version obsolète d'un fichier mis à jour par APT. Après un redémarrage d'Apache, le commande reportera :

```
# checkrestart  
Found 0 processes using old versions of upgraded files
```

### 3.3 Cron-apt

Cron-APT est un outil qui permet de mettre à jour la liste des paquets disponibles et de télécharger les paquets à mettre à jour. L'outil permet d'exécuter de manière automatique n'importe quelle commande `apt-get` ou `aptitude` et de fournir un rapport sur l'exécution de la commande. Attention, utiliser `cron-apt` pour installer automatiquement les mises à jour est très dangereux !

La configuration de base permet de mettre à jour la liste des paquets toutes les nuits et de télécharger les nouveaux paquets de manière à accélérer la procédure de mise à jour qui sera faite manuellement par un administrateur. L'installation se fait tout simplement avec la commande suivante :

```
# aptitude install cron-apt
```

Par défaut, `cron-apt` fait déjà bien le boulot mais on peut modifier un peu la configuration pour utiliser **aptitude** au lieu de **apt-get** par exemple. Toute la configuration se fait dans le fichier `/etc/cron-apt/config` :

```
APTCOMMAND=/usr/bin/aptitude  
MAILTO="root"  
MAILON="upgrade"
```

De cette façon, l'utilisateur **root** recevra un mail à chaque fois qu'un paquet dispose d'une mise à jour dans les dépôts officiels ou de sécurité.

### 3.4 La liste de diffusion Security

Cron-APT permet d'être notifié à chaque nouvelle mise à jour disponible. Si l'on désire être prévenu en temps réel et obtenir plus de détails sur les mises à jours, un bon point de départ est de s'inscrire sur la liste de diffusion **debian-security-announce** [4].

## Chapitre 4

# Intégrité du système

### 4.1 Présentation

### 4.2 debsums

```
# aptitude install debsums
```

```
# debsums_init
```

```
# debsums | grep -v OK
```

Lancement en cron.daily ?

### 4.3 rkhunter

- Installation de rkhunter [5]

```
# aptitude install rkhunter
```

- Modification de la configuration pour correspondre à la configuration SSH réalisée ci-dessous.  
Dans /etc/rkhunter.conf :

```
ALLOW_SSH_ROOT_USER=no
```

- Mise à jour des bases

```
# rkhunter --update  
# rkhunter --propupd
```

## 4.4 integrit

- Installation de integrit [6]

```
# aptitude install integrit
```

- Configuration dans /etc/integrit/integrit.conf

```
root=/
known=/var/lib/integrit/known.cdb
current=/var/lib/integrit/current.cdb

!/dev
!/sys
!/home
!/proc
!/tmp
!/var
```

- Initialisation :

```
# integrit -C /etc/integrit/integrit.conf -u
# mv /var/lib/integrit/current.cdb /var/lib/integrit/known.cdb
# integrit -C /etc/integrit/integrit.conf -c
```

- Dans /etc/integrit/integrit.debian.conf

```
CONFIGS="/etc/integrit/integrit.conf"
```

Cron executée tous les jours.

## Chapitre 5

# Sécurité des services

### 5.1 Généralités

De manière générale, tous les services qui offrent un accès extérieur doivent être l'objet d'une attention particulière. L'idée première est de ne laisser transiter aucune information sensible en clair sur le réseau. Pour cela, la plupart des services proposent maintenant un support SSL qui permet de chiffrer les communications et de s'assurer de l'identité du service distant.

Par ailleurs, les différents services offrent souvent la possibilité d'être exécutés avec un utilisateur dédié. Cette fonctionnalité permet de cloisonner chaque service et doit être utilisée aussi souvent que possible pour limiter la portée d'une éventuelle corruption.

### 5.2 SSH

Le serveur **ssh** permet d'obtenir un contrôle total sur une machine et est un outil quasiment indispensable pour administrer les serveurs distants. Les possibilités offertes par ce service étant très vastes, une attention particulière doit être accordée lors de sa configuration. Initialement cette configuration est déjà complètement fonctionnelle, on peut simplement modifier quelques options pour améliorer la sécurité dans le fichier `/etc/ssh/sshd_config` :

```
PermitRootLogin no
X11Forwarding no
AllowUsers admin
```

Bien entendu, les modifications seront prises en compte après un re-démarrage du service :

```
# /etc/init.d/ssh restart
```

Notons qu'avec la configuration ci-dessus, seul l'utilisateur `admin` pourra se connecter en SSH.

Afin de lutter de manière efficace contre les attaques en "brute force", il est également possible de limiter le nombre de connexion SSH réalisée par secondes. Cette configuration doit être réalisée avec une macro `shorewall` comme indiqué dans le document dédié à ce service [1].

## Chapitre 6

# Références

- [1] Mise en place de shorewall. [www.vogelweith.com/debian\\_server/02\\_shorewall.php](http://www.vogelweith.com/debian_server/02_shorewall.php).
- [2] Logcheck. [www.logcheck.org](http://www.logcheck.org).
- [3] Personnalisation des règles logcheck. [www.vogelweith.com/downloads/logcheck\\_custom](http://www.vogelweith.com/downloads/logcheck_custom).
- [4] La liste debian security announce. [lists.debian.org/debian-security-announce/](http://lists.debian.org/debian-security-announce/).
- [5] Rootkit hunter. [rkhunter.sourceforge.net](http://rkhunter.sourceforge.net).
- [6] Integrit. [sourceforge.net/projects/integrit/](http://sourceforge.net/projects/integrit/).
- [7] Site officiel du projet debian. [www.debian.org](http://www.debian.org).
- [8] La page debian security. [www.debian.org/security/](http://www.debian.org/security/).