

Surveillance du serveur

Debian GNU/Linux



Matthieu Vogelweith

10 juillet 2008

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^AT_EX](#)

Licence

Copyright ©2008 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 1.2 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

Table des matières	3
1 Surveillance des logs	4
1.1 logcheck	4
2 Alertes de sécurité	5
2.1 Chkrootkit	5
2.2 rkhunter	5
3 SNMP	6
3.1 Installation	6
3.2 Premier test	6
4 Surveillance avec Nagios	7
4.1 Installation	7
5 Supervision avec CACTI	8
5.1 Installation	8
5.2 Monitoring matériel	8
5.2.1 Trafic réseau	8
5.2.2 Températures	8
5.3 Monitoring des services	8
5.3.1 Postfix	8
6 Références	10

Chapitre 1

Surveillance des logs

1.1 logcheck

- Installation

```
# aptitude install logcheck
```

Chapitre 2

Alertes de sécurité

2.1 Chkrootkit

- Installation

```
# aptitude install chkrootkit
```

- Analyse journalière et envoi des rapports par mail (/etc/cron.d/chkrootkit)

```
#  
# Chkrootkit alerts  
#  
# m h dom mon dow user  command  
0 6 * * * root    /usr/sbin/chkrootkit -n -q | mail -s "Daily chkrootkit report "  
    rootkitalert
```

- Alias dans /etc/aliases

```
rootkitalert: root
```

2.2 rkhunter

- Installation

```
# aptitude install rkhunter
```

Chapitre 3

SNMP

3.1 Installation

```
# aptitude install snmpd
```

Edition de /etc/default/snmpd pour enlever 127.0.0.1 de la variable SNMPDOPTS

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid'
```

Edition de /etc/snmp/snmpd.conf

```
#com2sec paranoid default public
com2sec readonly default public
```

Re-démarrage du service

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

3.2 Premier test

- installation du client et des outils SNMP

```
# aptitude install snmp
```

- affichage des informations disponibles

```
# snmpwalk -v 2c -c public localhost
```

Chapitre 4

Surveillance avec Nagios

4.1 Installation

```
# aptitude install nagios2
```

Chapitre 5

Supervision avec CACTI

Cacti est un logiciel de supervision réseau basé sur la puissance de stockage de données de RRDTOOL.

5.1 Installation

Installation avec le serveur MySQL et PHP5

```
# aptitude install cacti libapache2-mod-php5 php5-mysql php5-snmp php5-cli mysql-server
```

Comme indiqué précédemment, Cacti utilise une base de donnée pour ... Il est possible de faire toute la configuration de la base avec dbconfig lors de la post-installation du paquet. Pour cela il suffit de répondre aux questionx de debconf en suivant les instructions ci-dessous :

- Configure database for cacti with dbconfig-common ? -> Yes
- Password of your database's administrative user : xx
- MySQL application password for cacti : xx
- Password confirmation : xx
- Webserver type : Apache2

5.2 Monitoring matériel

5.2.1 Traffic réseau

5.2.2 Températures

5.3 Monitoring des services

5.3.1 Postfix

- + Récupération de l'archive mailgraph-cacti.zip
- + Sur la machine ou tourne Postfix
- + installation de mailgraph

```
apt-get install mailgraph
mv /usr/sbin/mailgraph.pl /usr/sbin/mailgraph.pl.orig
unzip mailgraph-cacti.zip
cd mailgraph-cacti
cp mailgraph.pl /usr/local/sbin/
cp postfixstats.sh /usr/local/bin/
```

+ Dans le fichier snmpd.conf

```
exec mailcount /usr/bin/postfixstats.sh
```

+ Redemarrage de snmpd

```
/etc/init.d/snmpd restart
```

+ Creation des fichiers temp de compteur

```
touch /var/tmp/mailreceived
touch /var/tmp/mailed
touch /var/tmp/mailrejected
touch /var/tmp/mailbounced
touch /var/tmp/mailspam
touch /var/tmp/mailvirus
```

+ Modification du script d'init

```
I5 : DAEMON="/usr/local/sbin/mailgraph.pl"
```

```
I16 : test -x $DAEMON || exit 0
```

+ Redemarrage de mailgraph

```
/etc/init.d/mailgraph restart
```

+ Sur la machine ou tourne Cacti

+ Copie du script

```
cp postfixcheck.pl /usr/share/cacti/site/scripts/
```

+ Ajout du template cacti_graph_template_postfix_processing.xml dans cacti + Ajout du graph pour le bon host

Chapitre 6

Références