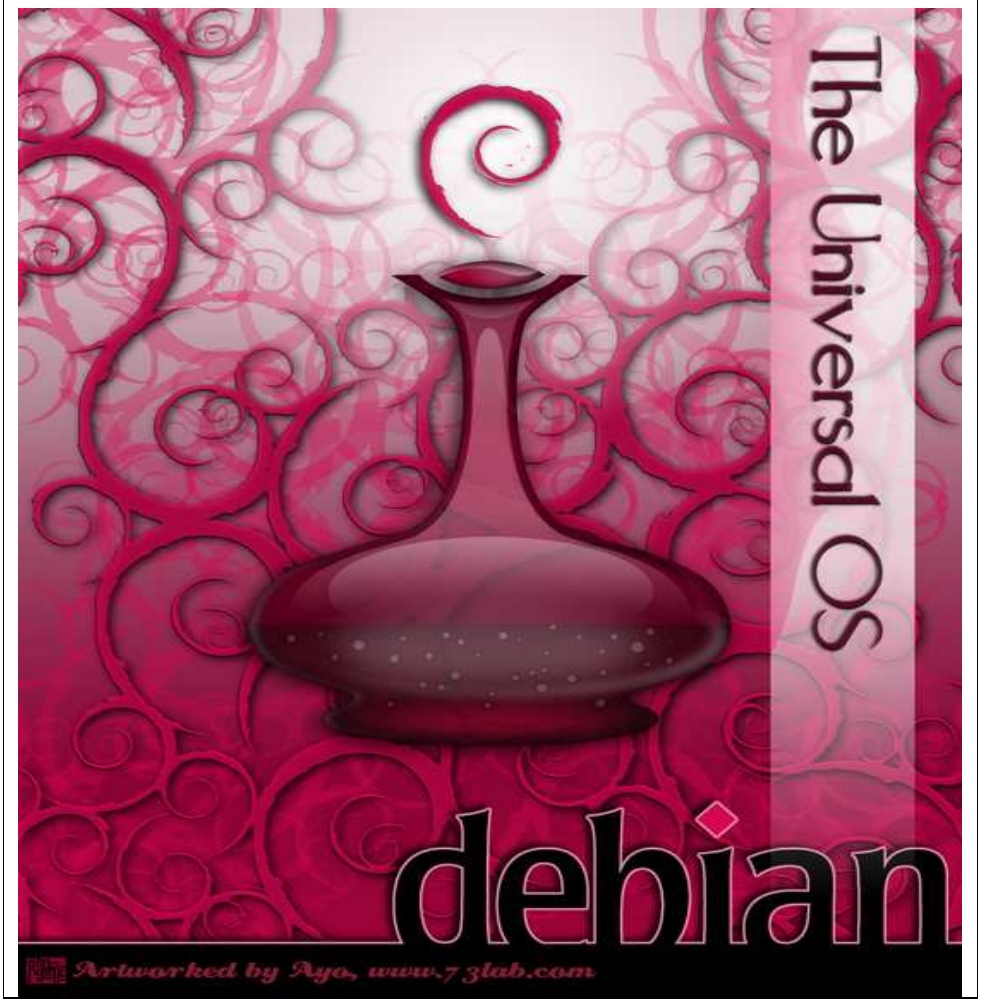
Mise en place du serveur

SYSLOG



Tables des matières

Ce serveur sert à centraliser les logs sensibles des serveurs Unix.

http://syslog

IP : X.X.X.X

http://unixlog.mondomaine.fr

IP : X.X.X.X

1 CONFIGURATION DE BASE :

➔ *Matérielle :* Serveur HP Proliant ML110 avec 1Go RAM, 2 HD de 160Go en RAID 1.

➔ *Logicielle :* Ubuntu Edgy eft 6.10 + Apache 2+ + PHP 5 + Phpmyadmin + MySQL-server + Syslog-ng + PhpSyslog-ng 2.8

2 PARTITIONNEMENT DU DISQUE :

- / (partition primaire) : 20 Go => la rendre amorçable
- /usr (partition logique) : 30 Go
- /var (partition logique) : 80 Go
- /home (partition logique) : 20 Go
- SWAP : 2Go

Ensuite installer la Ubuntu avec seulement l'interface graphique. Il ne faut pas installer les serveurs web, mail et bases de données lors de l'installation.
Seule chose importante lors de l'installation : il faut choisir un miroir de téléchargement pour les packages (programmes) Debian : ftp2.debian.org.

3 CONFIGURATION RESEAU :

Voici comment attribuer en commande une IP fixe et assurer la résolution de nom à notre serveur web qui sera situé en DMZ:

```
# vi /etc/network/interfaces
```

On y écrira les lignes suivantes :

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address X.X.X.X
netmask X.X.X.X
network X.X.X.X
gateway X.X.X.X
# dns
dns-nameservers X.X.X.X
dns-search mondomaine.fr
```

Puis il faut éditer le fichier resolv.conf :

```
#vi /etc/resolv.conf
```

Et y placer :

```
nameserver X.X.X.X
nameserver X.X.X.X
search mondomaine.fr
```

Redémarrer ensuite le service réseau pour prendre en compte les nouveaux paramètres avec :

```
# cd /etc/init.d
# ./networking restart
```

Vérifier l'attribution d'adresse et la résolution de nom avec :

```
# ifconfig -a
```

eth0 Lien encap:Ethernet HWaddr 00:1A:4B:B0:F3:43
inet adr:X.X.X.X Bcast:X.X.X.X Masque:X.X.X.X

```
# ping shiva
```

PING shiva.mondomaine.mondomaine.fr (194.254.145.149) 56(84) bytes of data.
64 bytes from shiva.systeme.mondomaine.fr (194.254.145.149): icmp_seq=1 ttl=64 time=4.67 ms

4 INSTALLATION DES SOFTWARES :

Ubuntu utilise l'outil APT et on peut configurer les sources de téléchargement (cd, http, ftp..) dans le fichier sources.list.
Par défaut, après l'installation, celui-ci utilise les sources du cédérom. Pour éviter des problèmes lors d'installations de packages, effectuer les manipulations suivantes en ouvrant un terminal (console) root depuis le bureau (on vous demandera le mdp) :

```
# vi /etc/apt/sources.list
```

Et commenter avec un **#** les lignes concernant le cédérom :

#deb cdrom:[Debian GNU/Linux 4.0 r1 _Etch_ - Official i386 DVD Binary-1 20070819-11:33]/ etch contrib main

deb http://fr.archive.ubuntu.com/ubuntu/ edgy main restricted
deb-src http://fr.archive.ubuntu.com/ubuntu/ edgy main restricted
deb http://ftp2.fr.debian.org/debian/ stable main
deb-src http://ftp2.fr.debian.org/debian/ stable main

Maintenant, on peut commencer à installer les logiciels :

4.1 Installation d'Apache 2

```
# apt-get install apache2 apache2-doc
```

4.2 Configuration d'Apache 2

Effectuer :

```
# vi /etc/apache2/apache2.conf
```

Avec la variable : **ServerName unixlog.mondomaine.fr**

N.B : A chaque changement de conf, effectuer :

```
# sudo /etc/init.d/apache2 reload
```

```
# apt-get install mysql-server
```

4.3 Installation de PHP 5

```
# apt-get install php5 libapache2-mod-php5 php5-mysql
```

Ensuite, pour tester la configuration de PHP, on peut créer un fichier phpinfo.php comme ceci :

```
# cd /var
# mkdir www   (on crée le répertoire web qui n'était pas présent par défaut)
# cd www
# vi phpinfo.php
```

Et on y met :

```
<?php
    phpinfo();
?>
```

On peut alors voir les informations ici : http://unixlog.mondomaine.fr/phpinfo.php

4.4 Installation de MySQL-server :

```
# apt-get install mysql-server
# sudo -i mysql_secure_installation
```

Il faut ensuite suivre un processus de configuration de mysql, qui va nous permettre de mettre un mot de passe root pour mysql, enlever l'utilisateur anonyme ainsi que la base de données test créés lors de l'installation ; choisir le mode d'administration mysql (locale ou distante), voir chapitre 4.9.

4.5 Installation de PhpMyAdmin

```
# apt-get install phpmyadmin php5-mcrypt
```

On peut ensuite se rendre a l'URL suivante:

http://syslog.mondomaine.fr/phpmyadmin

4.6 Installation de Syslog-ng

Vous devez au préalable activer le dépot universe ; l'installation de syslog-ng supprimera les paquets klogd et sysklogd, respectivement en charge de la journalisation des évènements liés au noyau et au reste du système. Idem pour le paquet ubuntu-minimal.

```
# sudo apt-get install syslog-ng
```

Editez ensuite le fichier **/etc/default/syslog-ng** et remplacer
#CONSOLE_LOG_LEVEL=0 par CONSOLE_LOG_LEVEL=1

Après avoir effectué ces changements, redémarrez syslog-ng avec la commande :

```
# sudo /etc/init.d/syslog-ng restart
```

4.7 Configuration de Syslog-ng

Le fichier de configuration par défaut est situé dans **/etc/syslog-ng/syslog-ng.conf**

Pour que syslog-ng accepte de recevoir des messages d'une machine distante, vous devez décommenter une ligne ; pour cela remplacer :

 # (this is equivalent to the "-r" syslogd flag)
 # udp();

Par

 # (this is equivalent to the "-r" syslogd flag)
udp();

4.8 Installation de PHP-Syslog-ng

Télécharger php-syslog-ng ici:

```
# cd /var/www
# wget http://php-syslog-ng.googlecode.com/files/php-syslog-ng-
2.9.3l.tgz
```

Décomprésser le fichier tar.gz

```
# tar –xvf php-syslog-ng-2.9.3l.tgz
```

Déplacer le dossier à l'intérieur du dossier apache2, par exemple:

```
# mv php-syslog-ng-2.9.3l phpsyslogng
```

4.9 Configuration de PHP-Syslog-ng

Le moyen le plus rapide est d'utiliser le fichier **dbsetup.sql** dans le répertoire 'scripts'. Éditer ce fichier et renseigner les mots de passe des 3 utilisateurs (sysloguser, syslogfeeder, syslogadmin) qui serons créés (en remplaçant PW_HERE). Le script créera une table pour les journaux et une pour l'authentification des utilisateurs, et affectera des droits sensiblement différents pour chaque utilisateur.

```
# cd /var/www/phpsyslogng/scripts
```

```
# vi dbsetup.sql
```

Et dans la section **create users** :

```
INSERT INTO user (Host, User, Password) VALUES
('localhost','sysloguser', password(' PW_HERE '));
INSERT INTO db (Host, Db, User) VALUES
('localhost','syslog','sysloguser');

INSERT INTO user (Host, User, Password) VALUES
('localhost','syslogfeeder', password(' PW_HERE '));
INSERT INTO db (Host, Db, User) VALUES
('localhost','syslog','syslogfeeder');

INSERT INTO user (Host, User, Password) VALUES
('localhost','syslogadmin',password(' PW_HERE '));
INSERT INTO db (Host, Db, User) VALUES
('localhost','syslog','syslogadmin');
COMMIT;
FLUSH PRIVILEGES;
```

Si vous effectuez d'autres changements comme changer le nom de la base de données ou des tables, assurez-vous de faire correspondre ces changements dans le fichier config.php.

Après avoir modifié le script dbsetup.sql exécuter le simplement avec la commande :

```
sudo mysql -u root -p < dbsetup.sql
```

Maintenant, nous devons entrer dans le fichier **/etc/syslog-ng/syslog-ng.conf** pour configurer l'outil.

Décommenter la ligne suivante pour recevoir des logs depuis des machines distantes:

udp();

Nous devons envoyer les logs dans la base de données **MySQL**.

Ajouter les lignes suivantes pour dire à syslog-ng où envoyer les données:

```
# pipe messages to /var/log/mysql.pipe to be processed by mysql

destination d_mysql {
pipe("/var/log/mysql.pipe"
template("INSERT INTO logs
(host, facility, priority, level, tag, datetime, program, msg)
VALUES ( '$HOST', '$FACILITY', '$PRIORITY', '$LEVEL', '$TAG', '$YEAR-
$MONTH-$DAY $HOUR:$MIN:$SEC','$PROGRAM', '$MSG' );\n") template-
escape(yes));
 };

# Ci-dessous, tous les sources des logs sont envoyés vers la base de
données MySQL.

log {
source(s_all);
destination(d_mysql);
 };
```

Vous pouvez trouver les lignes de configuration ci-dessus dans le fichier **.../"phpsyslog-ng directory"/scripts/syslog.conf**

5 SCRIPTS ET TACHES CRON

Nous devons pousser les logs dans la base de données avec un script bash:

Créer un nouveau fichier et insérer y la ligne ci-dessous, soyez attentif à sauver le fichier avec une extension .sh
Si vous ne vouler par créer le fichier, vous pouvez le trouver dans le dossier phpsyslog, puis **/scripts/syslog2mysql.sh.** (N'oubliez pas de configurer l'utilisateur et le mot de passe MySQL)

```
#!/bin/bash

if [ ! -e /var/log/mysql.pipe ]
then
mkfifo /var/log/mysql.pipe
fi
while [ -e /var/log/mysql.pipe ]
do
mysql    -u    syslogfeeder    --password=PASS_HERE    syslog    <
/var/log/mysql.pipe >/dev/null
done
```

Le script signifie que si le fichier mysql.pipe n'existe, il est créé. Ensuite, tant que le fichier mysql.pipe existes, ouvrir une connexion MySQL et envoyer les données en tampon dans la base de données.

Vous devez remplacer PASS_HERE par le mot de passe qui vous avez affecté à l'utilisateur 'syslogfeeder'. Vous voudrez aussi probablement que le script soit lancé automatiquement à chaque démarrage du serveur syslog-ng. Aussi, ajoutez un entrée dans inittab ou démarrez le script via init.d. Mais bien faire attention à lancer le script une fois que Mysql a démarré.

Avec un script init.d Ubuntu : Créez un fichier **syslog2mysql** dans /etc/init.d/

```
# cd /etc/init.d
# vi syslog2mysql
```

Ayant comme contenu :

```
#! /bin/sh

# Do NOT "set -e"

PATH=/usr/sbin:/usr/bin:/sbin:/bin
DESC="Fetch queries from syslog-ng to mysql db"
NAME=syslog2mysql
PIDFILE=/var/run/$NAME.pid
SCRIPTNAME=/etc/init.d/$NAME

# Exit if mysql client is not installed
[ -x "/usr/bin/mysql" ] || exit 0

# Load the VERBOSE setting and other rcS variables
[ -f /etc/default/rcS ] && . /etc/default/rcS

# Define LSB log_* functions.
# Depend on lsb-base (>= 3.0-6) to ensure that this file is present.
. /lib/lsb/init-functions

#
# Function that starts the daemon/service
#
do_start()
{
        [ ! -e /var/log/mysql.pipe ] && echo " (Creating $NAME
pipe)." && mkfifo /var/log/mysql.pipe
        if [ -e $PIDFILE ]; then
            if ps -p $(cat $PIDFILE) >/dev/null; then
                echo -n -e "\nError: $NAME seems to be already
running!"
                return 1
            else
                rm -f $PIDFILE
            fi
        fi
        {
            while [ -e /var/log/mysql.pipe ]
            do
                mysql -u syslogfeeder --password=PASS_HERE syslog <
/var/log/mysql.pipe >/dev/null
```

```
                sleep 1
            done
        } &
        echo $! > $PIDFILE
}

#
# Function that stops the daemon/service
#
do_stop()
{
        if [ -e $PIDFILE ]; then
            PID=$(cat $PIDFILE)
            if ps -p $PID >/dev/null; then
                # get PID of child
                CPID=$(pgrep -P $PID)
                # kill script
                kill $PID
                # kill child
                kill $CPID
                rm -f $PIDFILE
                return 0
            else
                echo -e "\nWarning: $NAME was not running."
                echo -n -e "\nCleaning PID file"
                rm -f $PIDFILE
                return 1
            fi
        else
            echo -n -e "\nWarning: $NAME was not running"
            return 1
        fi
}

case "$1" in
  start)
        [ "$VERBOSE" != no ] && log_daemon_msg "Starting $DESC"
"$NAME"
        do_start
        case "$?" in
                0|1) [ "$VERBOSE" != no ] && log_end_msg 0 ;;
                2) [ "$VERBOSE" != no ] && log_end_msg 1 ;;
        esac
        ;;
  stop)
        [ "$VERBOSE" != no ] && log_daemon_msg "Stopping $DESC"
"$NAME"
        do_stop
        case "$?" in
                0|1) [ "$VERBOSE" != no ] && log_end_msg 0 ;;
                2) [ "$VERBOSE" != no ] && log_end_msg 1 ;;
        esac
        ;;
  restart|force-reload)
        #
        # If the "reload" option is implemented then remove the
        # 'force-reload' alias
        #
```

```
        log_daemon_msg "Restarting $DESC" "$NAME"
        do_stop
        case "$?" in
          0|1)
                do_start
                case "$?" in
                        0) log_end_msg 0 ;;
                        1) log_end_msg 1 ;; # Old process is still
running
                        *) log_end_msg 1 ;; # Failed to start
                esac
                ;;
          *)
                # Failed to stop
                log_end_msg 1
                ;;
        esac
        ;;
  *)
        echo "Usage: $SCRIPTNAME {start|stop|restart|force-reload}"
>&2
        exit 3
        ;;
esac

:
```

Pensez à modifier le pwd de **syslogfeeder** dedans

Créez le lien pour lancer le script au démarrage

```
# sudo update-rc.d syslog2mysql defaults
```

Maintenant démarrez le service **syslog2mysql** :

```
# /etc/init.d/syslog2mysql start
```

Il est sage d'ajouter une ligne dans la **crontab** de root pour démarrer le script au démarrage du serveur.

Il est maintenant temps de redémarrer le démon syslog-ng et d'envoyer les logs dans la base de données :

```
# sudo /etc/init.d/syslog-ng restart
```

Si vous utilisez la base de données par défaut initialisée par le fichier dbsetup.sql, tout ce que vous avez à faire est d'entrer le mot de passe pour les utilisateurs sysloguser et syslogadmin, définir l'hote et le port du serveur de base de données s'il n'est pas sur le même serveur que le serveur web, et saisir une URL valide.

Sinon, parcourez le fichier config.php et configurez les paramètres dont vous avez besoin. Toutes les options sont expliquées dans le fichier.

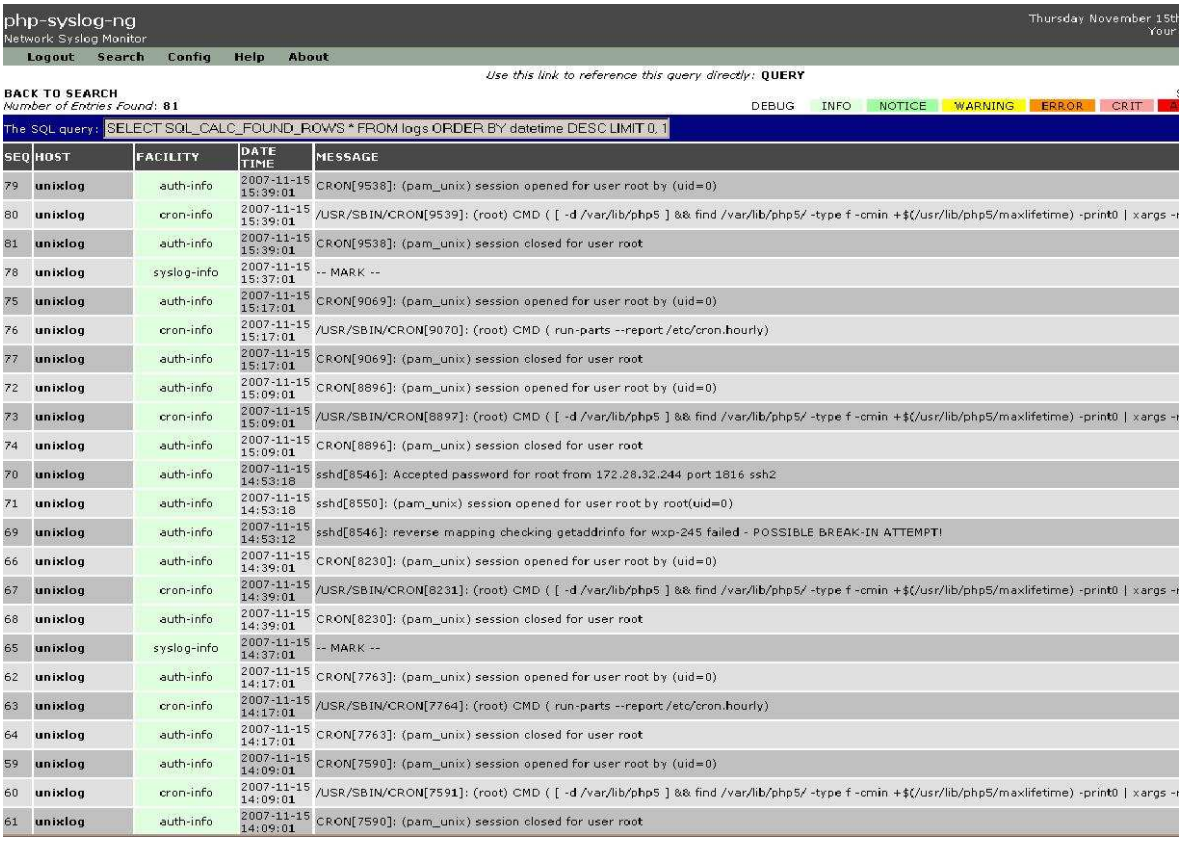
```
sudo vi /var/www/phpsyslogng/config/config.php
```

```
// BEGIN: DATABASE CONNECTION INFO
//==========================================================================
=====
// DBUSER is the name of the basic user.
define('DBUSER', 'sysloguser');

// DBUSERPW is DBUSER's database password.
define('DBUSERPW', PASS_HERE);

// DBADMIN is the name of the admin user.
define('DBADMIN', 'syslogadmin');

// DBADMINPW is DBADMIN's database password.
define('DBADMINPW', PASS_HERE);

// DBNAME is the name of the database you are using.
define('DBNAME', 'syslog');

// DBHOST is the host where the MySQL server is running.
define('DBHOST', 'localhost');

// DBPORT is the port where the MySQL server is listening.
// The default port is 3306.
define('DBPORT','3306');
```

php-syslog-ng est maintenant accessible à l'adresse : http://votre_webserver/phpsyslogng Un compte administrateur (admin) a été créé par dbsetup.sql avec le mot de passe admin.

Si après la connexion vous obtenez le message "Query failed: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1", c'est parce que votre base mysql n'est pas encore alimentée. Pour les plus pressés, vérifier que le fichier **syslog-ng.conf** est bien configuré **(cf paragraphe 4.9).**

Voici un apperçu de l'interface de phpsyslogng :



SEQ	HOST	FACILITY	DATE TIME	MESSAGE
79	unixlog	auth-info	2007-11-15 15:39:01	CRON[9538]: (pam_unix) session opened for user root by (uid=0)
80	unixlog	cron-info	2007-11-15 15:39:01	/USR/SBIN/CRON[9539]: (root) CMD ([-d /var/lib/php5] && find /var/lib/php5/ -type f -cmin +$(/usr/lib/php5/maxlifetime) -print0 | xargs -r
81	unixlog	auth-info	2007-11-15 15:39:01	CRON[9538]: (pam_unix) session closed for user root
78	unixlog	syslog-info	2007-11-15 15:37:01	-- MARK --
75	unixlog	auth-info	2007-11-15 15:17:01	CRON[9069]: (pam_unix) session opened for user root by (uid=0)
76	unixlog	cron-info	2007-11-15 15:17:01	/USR/SBIN/CRON[9070]: (root) CMD (run-parts --report /etc/cron.hourly)
77	unixlog	auth-info	2007-11-15 15:17:01	CRON[9069]: (pam_unix) session closed for user root
72	unixlog	auth-info	2007-11-15 15:09:01	CRON[8896]: (pam_unix) session opened for user root by (uid=0)
73	unixlog	cron-info	2007-11-15 15:09:01	/USR/SBIN/CRON[8897]: (root) CMD ([-d /var/lib/php5] && find /var/lib/php5/ -type f -cmin +$(/usr/lib/php5/maxlifetime) -print0 | xargs -r
74	unixlog	auth-info	2007-11-15 15:09:01	CRON[8896]: (pam_unix) session closed for user root
70	unixlog	auth-info	2007-11-15 14:53:18	sshd[8546]: Accepted password for root from 172.28.32.244 port 1816 ssh2
71	unixlog	auth-info	2007-11-15 14:53:18	sshd[8550]: (pam_unix) session opened for user root by root(uid=0)
69	unixlog	auth-info	2007-11-15 14:53:12	sshd[8546]: reverse mapping checking getaddrinfo for wxp-245 failed - POSSIBLE BREAK-IN ATTEMPT!
66	unixlog	auth-info	2007-11-15 14:39:01	CRON[8230]: (pam_unix) session opened for user root by (uid=0)
67	unixlog	cron-info	2007-11-15 14:39:01	/USR/SBIN/CRON[8231]: (root) CMD ([-d /var/lib/php5] && find /var/lib/php5/ -type f -cmin +$(/usr/lib/php5/maxlifetime) -print0 | xargs -r
68	unixlog	auth-info	2007-11-15 14:39:01	CRON[8230]: (pam_unix) session closed for user root
65	unixlog	syslog-info	2007-11-15 14:37:01	-- MARK --
62	unixlog	auth-info	2007-11-15 14:17:01	CRON[7763]: (pam_unix) session opened for user root by (uid=0)
63	unixlog	cron-info	2007-11-15 14:17:01	/USR/SBIN/CRON[7764]: (root) CMD (run-parts --report /etc/cron.hourly)
64	unixlog	auth-info	2007-11-15 14:17:01	CRON[7763]: (pam_unix) session closed for user root
59	unixlog	auth-info	2007-11-15 14:09:01	CRON[7590]: (pam_unix) session opened for user root by (uid=0)
60	unixlog	cron-info	2007-11-15 14:09:01	/USR/SBIN/CRON[7591]: (root) CMD ([-d /var/lib/php5] && find /var/lib/php5/ -type f -cmin +$(/usr/lib/php5/maxlifetime) -print0 | xargs -r
61	unixlog	auth-info	2007-11-15 14:09:01	CRON[7590]: (pam_unix) session closed for user root

Ouvrez le fichier .../**phpsyslogng/scripts/logrotate.php** et vérifier à la ligne 6, que la variable $APP_ROOT corresponde à ce que vous avez. Dans notre fichier de configuration:

$APP_ROOT = '/var/www/phpsyslogng';

Dans la partie "MISC FUNCTIONALITY" du fichier var/www/phpsyslogng/config/config.php, vous pouvez configurer des paramètres liés au fichier logrotate.php. Nous avons choisi de laisser les paramètres par défaut.
La dernière chose à faire est d'activer extention=mysql.so dans le fichier

```
# vi/etc/php5/cli/php.ini.
```

Rechercher la ligne avec **extension=mysql.so** et enlever le point virgule au début de la ligne.

```
extension=mysql.so
```

6 SCRIPTS ET TACHES CRON

Essayer de lancer le script **logrotate.php**:

```
# php5 /var/www/phpsyslogng/scripts/logrotate.php
```

Si vous avez quelque chose comme:

« ***Starting logrotate***
No DB link »

Cela veut dire que **extension=mysql.so** n'est pas décommenté dans le fichier **php.ini**.

Si tous est okay, vous devriez voir quelque chose comme ceci:

Starting logrotate
2006-07-29 22:42:50
Log rotate ended successfully

La dernière chose à faire est d'ajouter ce script dans un cron mensuel par exemple.
Il faut faire attention que seulement root peut accéder au fichier.

```
# chmod 700 /var/www/phpsyslogng/scripts/logrotate.php
# chown root:root /var/www/phpsyslogng/scripts/logrotate.php

# crontab -e -u root 00 22 * * 0 php
/var/www/phpsyslogng/scripts/logrotate.php
```

Ici, la rotation des logs se fera tout les lundis (0) à 22h00

```
# m h  dom mon dow   command
00 22 * * 0 php /var/www/phpsyslogng/scripts/logrotate.php
```

7 INSTALLATION D'UN CLIENT SYSLOG UNIX

Pour envoyer des logs depuis une machine Linux vers un serveur log, vous pouvez soit utiliser syslogd qui est le syslog par défaut sur une machine Linux ou syslog-ng.

-**syslogd**

Ouvrir le fichier **/etc/syslogd.conf**. Vous devez utiliser la syntaxe suivante:

facility.priorité ***destination***

Voici quelques exemples:

***.* 10.58.1.1**	# tous les logs sont déviés vers 10.58.1.1
kern.alert 10.2.5.8	# les messages "alert" et "emergencies" (urgence) généré par le noyau (kernel) sont envoyés vers 10.2.5.8.

Redémarrer le serveur:

```
etc/init.d/sysklogd restart
```

- **syslog-ng**

```
# apt-get install syslog-ng
```

La configuration du client syslog-ng est un peu plus difficile que celle de syslogd mais par contre elle offre bien plus de possibilités. Par exemple, l'utilisation de filtres, l'envoi de logs sur TCP ou encore l'envoi de logs encryptés vers le serveur.

Voyons comment configurer le client syslog-ng:
Ouvrez le fichier de configuration **/etc/syslog-ng/syslog-ng.conf**
La syntaxe est la suivante, elle se comprend par elle-même:

```
log
{
source(nom_de_la_source);
filter(nom_du_filtre);
destination(nom_de_la_destination);
};
```

Voici quelques exemples:

7.1 Tous les logs sont envoyés vers le serveur de log 10.13.44.44.

```
source s_all {
internal();
unix-stream("/dev/log");
file("/proc/kmsg" log_prefix("kernel: "));
udp();
};

destination d1 { udp("10.13.44.44"); };

log
{
source(s_all);
destination(d1);
};
```

La variable d1 représente ici un alias pour l'adresse 10.13.44.44

7.2 L'utilisation des Filtres

Dans ce deuxième exemple, nous utilisons un filtre pour séléctionner quelles logs seront envoyés vers le serveur. Le filtre inclus les messages de niveau "notice", "alert" et "error". En même temps, les messages doivent provenir de la "facility" kernel, en d'autres termes venir du noyau.
Pour plus d'informations à propos de la syntaxe du message, regarder le site web linode.com .

Les logs sont envoyés sur TCP port 54321 au lieu de sur UDP port 514, qui est le paramétrage par défaut.

Bien sûr, si vous voulez changer le port utiliser pour envoyer les logs, le collecteur de log doit être capable d'écouter à ce port.

```
source s_all {
internal();
unix-stream("/dev/log");
file("/proc/kmsg" log_prefix("kernel: "));
udp();
};

filter filtre1 { level(notice, alert, errot) and facility(kern); };

destination d1 { tcp("10.15.61.1" port (54321)); };

log
{
source(s_all);
filter(filtre1);
destination(d1);
};
```

N'oubliez pas d'ouvrir le port TCP 54321 sur le serveur syslog. Le port doit être déclaré dans une définition de source dans le fichier **/etc/syslog-ng/syslog-ng.conf** (du serveur de log, pas le client). Voici un exemple:

```
source s_all {
internal();
unix-stream("/dev/log");
file("/proc/kmsg" log_prefix("kernel: "));
udp();
tcp(port(54321));
};
```

Dans l'exemple illustré ci-dessus, le serveur syslog peut écouter à la fois sur les ports UDP 514 et TCP 54321.

8 INSTALLATION D'UN CLIENT SYSLOG WINDOWS

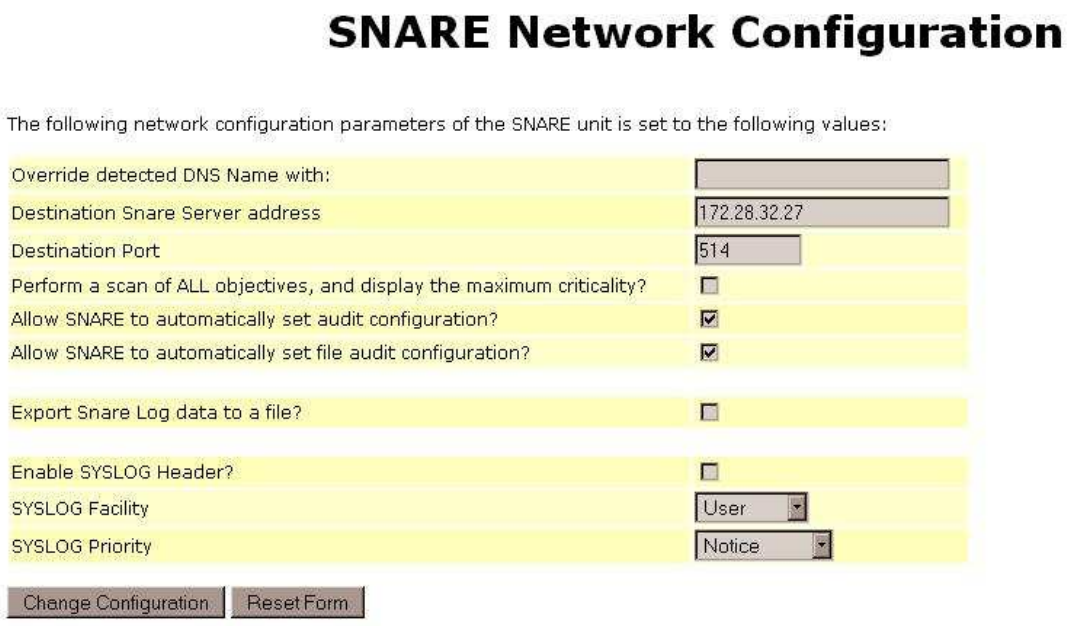
Se rendre sur le site d'interselect alliance :

http://www.intersectalliance.com/projects/SnareWindows/index.html

Et télécharger l'agent snare pour windows.

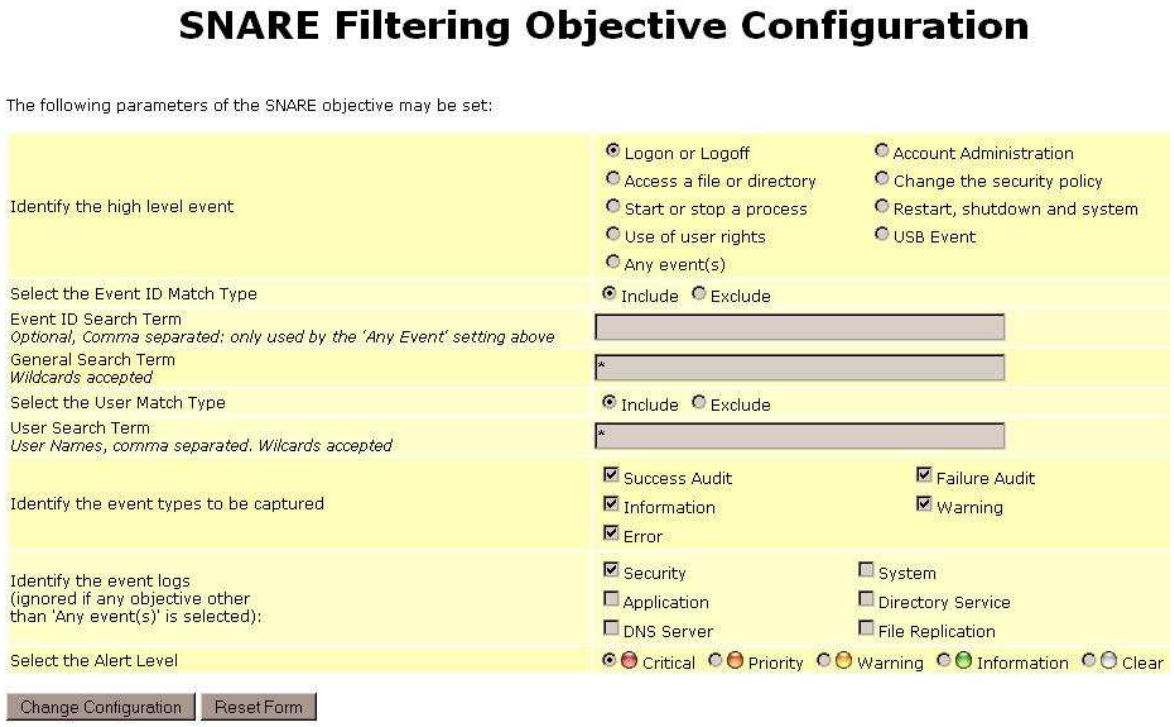
Installer ensuite celui-ci, et le configurer comme ceci :

8.1 Configuration Réseau :



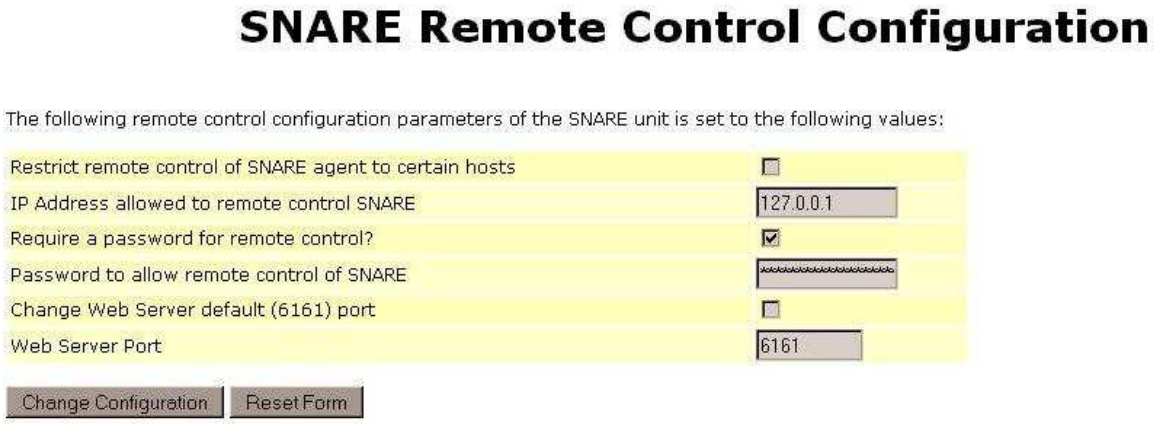
Il faut ici définir l'adresse et le port (514) d'écoute du serveur syslog

8.2 Configuration d'un filtre de logs :



A configurer selon les priorités voulues. Dans notre cas, nous privilègierons seulement les logs de type Error ou Warning.

8.3 Configuration de contrôle distant du démon syslog (agent snare)



8.4 Appeçu des évènements du client Windows avant l'envoi des logs :

Current Events

	Date	System	Event Count	EventID	Source	UserName	UserType	ReturnCode	Strings
	Mon Nov 12 11:50:05 2007	WXP-245.cndp.lan	102	538 (Ouverture/Fermeture de session)	Security	SYSTEM	User	Success Audit	Fermeture de la session utilisateur : Utilisateur : WXP-245$ Domaine : CNDP Id. de la session : (0x0,0x29D653) Type de session : 3
	Mon Nov 12 11:50:05 2007	WXP-245.cndp.lan	101	540 (Ouverture/Fermeture de session)	Security	SYSTEM	User	Success Audit	Ouverture de session réseau réussie : Utilisateur : WXP-245$ Domaine : CNDP Id. de la session : (0x0,0x29D653) Type de session : 3 Processus de session : Kerberos Package d'authentification : Kerberos Nom de la station de travail : GUID d'ouv. de session : {f4adf4cb-dba3-118a-f860-b59245bedc1c}
	Mon Nov 12 11:49:42 2007	WXP-245.cndp.lan	100	7036 (None)	Service Control Manager	Unknown User	N/A	Information	Le service Acquisition d'image Windows (WIA) est entré dans l'état : en cours d'exécution.
	Mon Nov 12 11:49:42 2007	WXP-245.cndp.lan	99	7035 (None)	Service Control Manager	SYSTEM	User	Information	Un contrôle Démarrer a correctement été envoyé au service Acquisition d'image Windows (WIA).
	Mon Nov 12 11:47:54 2007	WXP-245.cndp.lan	98	538 (Ouverture/Fermeture de session)	Security	julien.tehery	User	Success Audit	Fermeture de la session utilisateur : Utilisateur : julien.tehery Domaine : CNDP Id. de la session : (0x0,0x28AC9D) Type de session : 7
	Mon Nov 12 11:47:54 2007	WXP-245.cndp.lan	97	528 (Ouverture/Fermeture de session)	Security	julien.tehery	User	Success Audit	Ouverture de session réseau réussie : Utilisateur : julien.tehery Domaine : CNDP Id. de la session : (0x0,0x28AC9D) Type de session : 7 Processus de session : User32 Package d'authentification : Negotiate Station de travail : WXP-245 GUID d'ouv. de session : {be6db685-d1b6-1e5e-aa43-a3471d171184}
	Mon Nov 12 11:35:08 2007	WXP-245.cndp.lan	96	538 (Ouverture/Fermeture de session)	Security	julien.tehery	User	Success Audit	Fermeture de la session utilisateur : Utilisateur : julien.tehery Domaine : CNDP Id. de la session : (0x0,0x277363) Type de session : 7
	Mon Nov 12 11:35:08 2007	WXP-245.cndp.lan	95	528 (Ouverture/Fermeture de session)	Security	julien.tehery	User	Success Audit	Ouverture de session réseau réussie : Utilisateur : julien.tehery Domaine : CNDP Id. de la session : (0x0,0x277363) Type de session : 7 Processus de session : User32 Package d'authentification : Negotiate Station de travail : WXP-245 GUID d'ouv. de session : {25917525-2ed1-d5d4-12d7-995a22696566}
	Mon Nov 12 11:35:03 2007	WXP-245.cndp.lan	94	529 (Ouverture/Fermeture de session)	Security	SYSTEM	User	Failure Audit	Échec de l'ouverture de session : Raison : Nom d'utilisateur inconnu ou mot de passe incorrect Nom de l'utilisateur : julien.tehery@cndp.fr Domaine : Type de session : 7 Processus d'ouv. de session : User32 Package d'authentification : Negotiate Nom de station de travail : WXP-245