Chassat

Thomas

**Installation d’un serveur de logs avec Loganalyser et Rsyslog**

**Introduction :** Cette documentation va vous permettre d'installer et configurer un serveur de centralisation des logs. Rsyslog est un logiciel libre utilisé sur des systèmes d'exploitation de type Unix transférant les messages des journaux d'événements sur un réseau IP. Rsyslog implémente le protocole basique syslog qui centralise les journaux d'événements, permettant de repérer plus rapidement et efficacement les défaillances d'ordinateurs présents sur un réseau. Il présente la particularité d'en étendre les fonctionnalités comme l'utilisation du protocole TCP de la couche transport.

**Pré requis :**

* 1 ordinateur sous Debian 8 ;
* Le logiciel Loganalyzer disponible [ici](http://loganalyzer.adiscon.com/downloads/) ;
* 1 ordinateur client sous Debian 8.

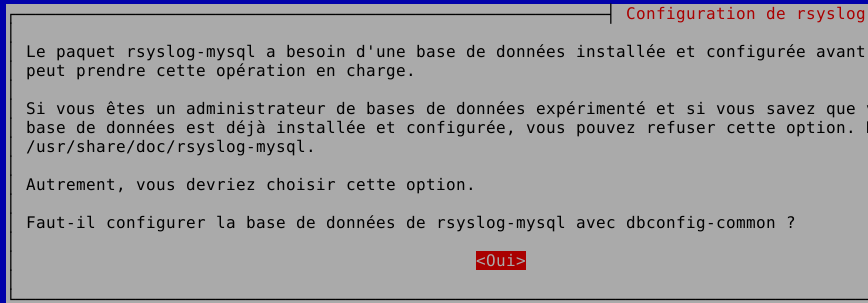
**Installation et configuration de Loganalyzer :**

Les commandes se feront toutes en mode super-utilisateur. Avant de commencer l’installation de **Rsyslog** et **Loganalyzer**, nous devons mettre à jour notre machine puis ensuite nous installerons les paquets qui assureront le bon fonctionnement de notre serveur (il y en a beaucoup). Nous allons donc ouvrir un terminal sur le serveur, nous connecter en mode ***Super-Utilisateur* (su)** et écrire les commandes suivantes :

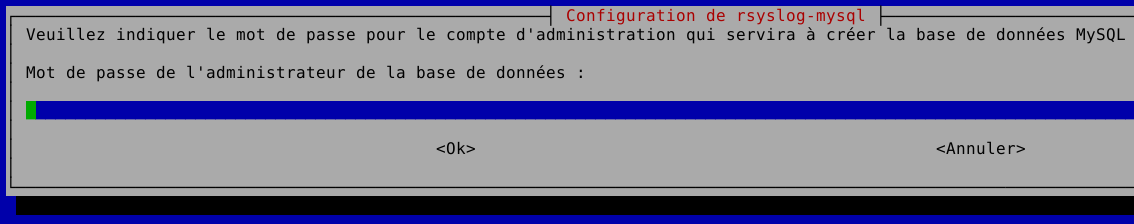
**apt-get update && apt-get upgrade**

***apt-get install python-software-properties rsyslog rsyslog-mysql unzip zip binutils cpp fetchmail flex gcc libc6-dev libpcre3 libpopt-dev lynx m4 make ncftp nmap openssl perl perl-modules zlib1g-dev autoconf libtool bison autotools-dev g++ mysql-server mysql-client libmysqlclient-dev apache2 apache2-doc apache2-mpm-prefork apache2-utils libexpat1 ssl-cert libapache2-mod-php5 php5 php5-common php5-curl php5-dev php5-gd php5-intl php-pear php5-imagick php5-imap php5-json php5-mcrypt php5-memcache php5-common php5-mysql php5-pspell php5-recode php5-snmp php5-sqlite php5-tidy php5-xmlrpc php5-xsl***

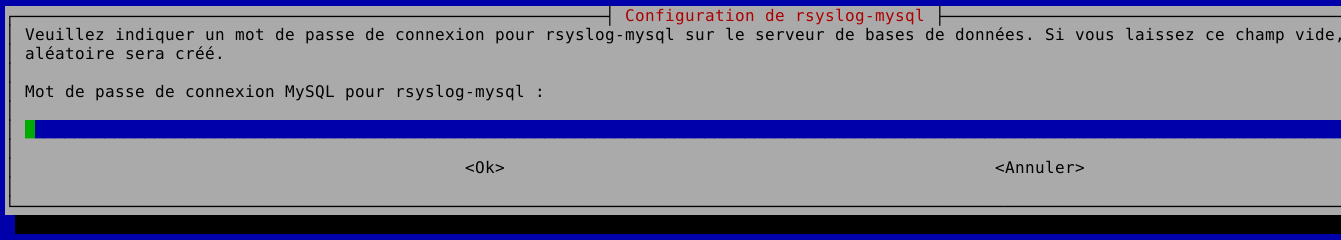
Nous devrions avoir une nouvelle fenêtre nous demandant si nous souhaitons configurer la base de données. Nous allons répondre ***oui***.



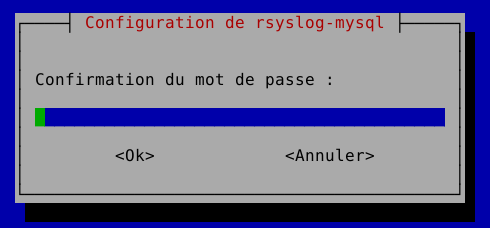
L’installateur nous demande maintenant le mot de passe du compte ***root***. Indiquons-le (ici c’est ***hhhhh***).



Il nous faut maintenant créer un mot de passe pour la connexion à la base de données. Nous pouvons en rentrer un ou bien laisser l’outil en générer un. Ici, nous allons utiliser le même mot de passe qu’avant : ***hhhhh***.



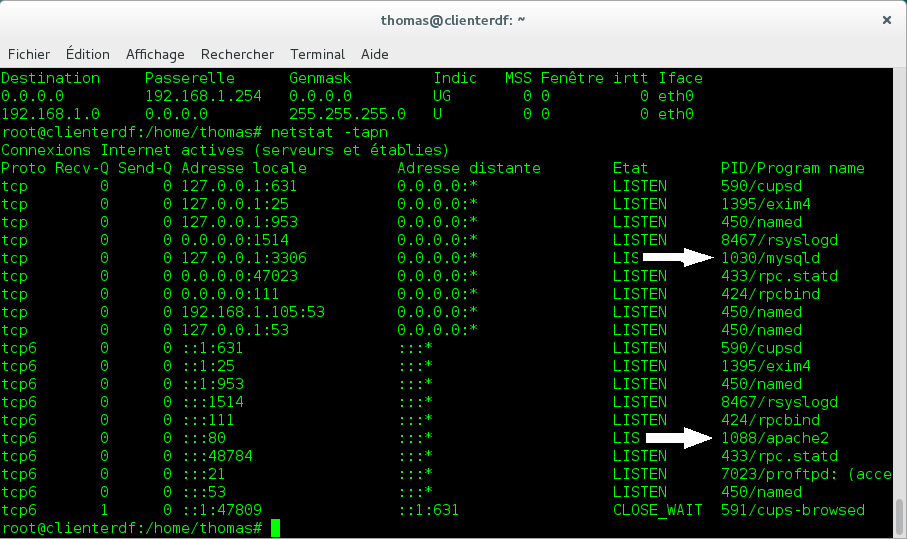
Nous devons confirmer ce mot de passe en le retapant.



Afin de vérifier que les services ***Apache2*** et ***MySQL*** sont sur écoute, nous pouvons utiliser la commande ***netstap –tapn***. Nous devrions voir ces lignes :

***tcp 0 0 127.0.0.1 :3306 0.0.0.0 :\* LISTEN \*\*\*\*\*/mysqld***

***tcp 0 0 0.0.0.0 ::80 0.0.0.0 :\* LISTEN \*\*\*\*\*/apache2***

****

Maintenant que l'outil Rsyslog est bien installé, nous passons à la configuration du fichier de configuration :

***nano /etc/rsyslog.conf***

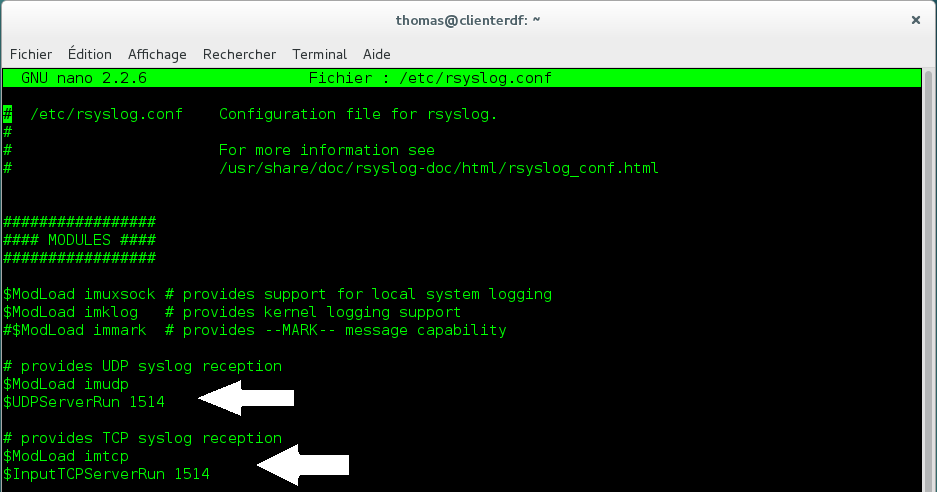
Dans la première page de configuration, il faut dé commenter (enlever le ***#*** en début de ligne) quelques paramètres qui sont :

***$ModLoad imtcp***

***$InputTCPServerRun 1514*** (il faut remplacer 514 par 1514)

***$ModLoad imudp***

***$UDPServerRun 1514*** (même chose ici)

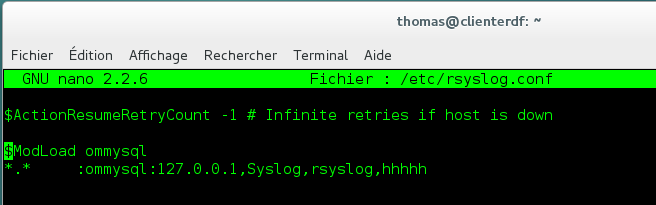


Une fois ces paramètres dé commentés, nous nous rendons tout en bas du fichier pour ajouter ces paramètres :

***$ModLoad ommysql***

***\*.\* :ommysql:127.0.0.1,<SyslogDatabase>,<rsyslogUserName>,<rsyslogUserPassword>***

Nous avons à remplacer ***rsyslogUserName*** par ***rsyslog*** qui est le nom d'utilisateur par défaut, ***SyslogDatabase*** par le nom de la base qui est Syslog puis ***rsyslogUserPassword*** par le mot de passe qui a été choisi durant l'installation de Rsyslog.

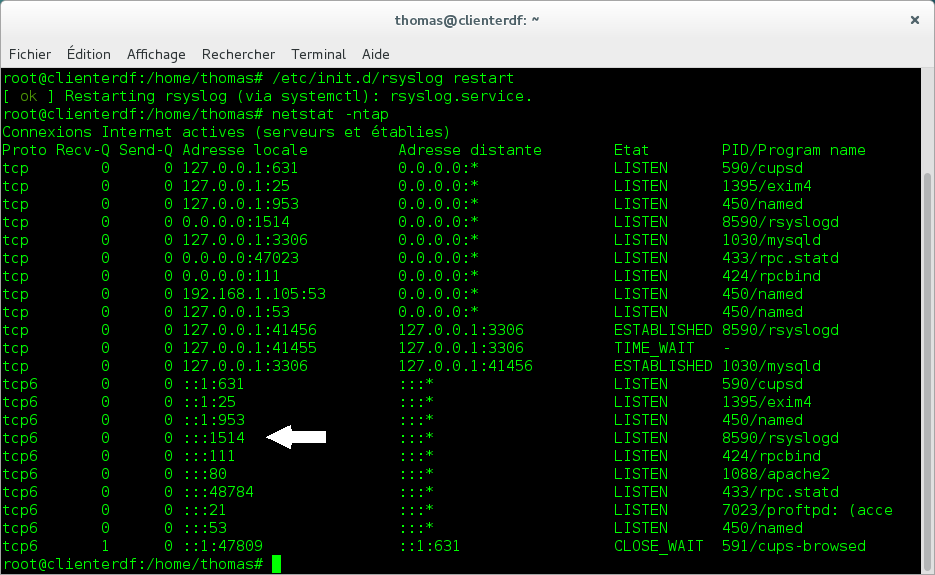


Nous allons maintenant redémarrer notre service Rsyslog afin que le serveur ait bien pris en compte les nouveaux paramètres : ***/etc/init.d/rsyslog restart***

Pour vérifier que notre outil Rsyslog est bien sur écoute, nous revérifions avec la commande :

***netstat -ntap***

Nous devrions voir une nouvelle ligne : ***tcp 0 0 0.0.0.0:1514 0.0.0.0:\* LISTEN \*\*\*\*\*/rsyslogd***

******

Pour faciliter la vision des logs, nous allons télécharger le logiciel LogAnalyzer qui nous permet d'avoir une vision des logs via un navigateur internet. Pour l'installer nous allons utiliser ces commandes :

***cd /usr/local/src***

***wget http://download.adiscon.com/loganalyzer/loganalyzer-3.6.6.tar.*gz** (cette version est la dernière version stable en Juin 2016)

***tar -zxvf loganalyzer-3.6.6.tar.gz***

***mv loganalyzer-3.6.6/src/\* /var/www/html***

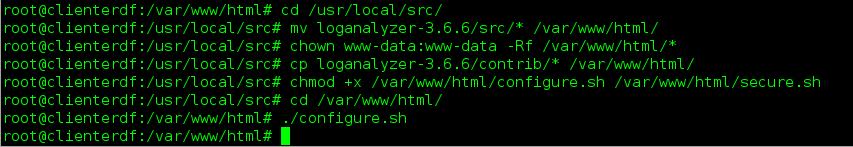
***chown www-data:www-data -Rf /var/www/html/\****

***cp loganalyzer-3.6.6/contrib/\* /var/www/html***

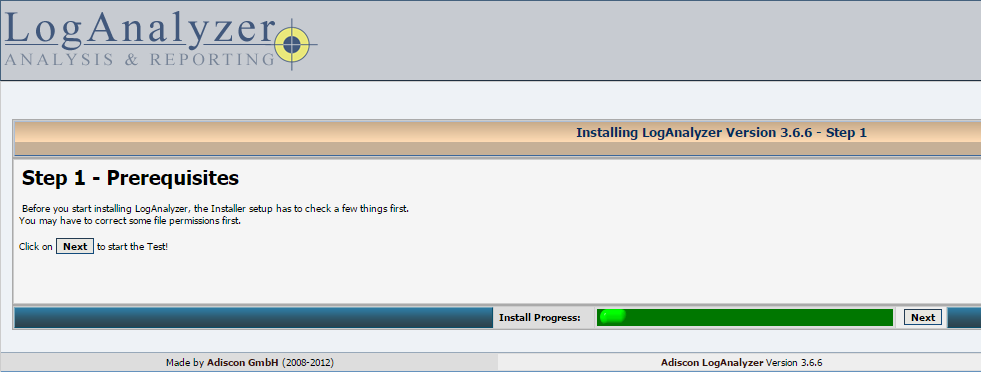
***chmod +x /var/www/html/configure.sh /var/www/html/secure.sh***

***cd /var/www/html***

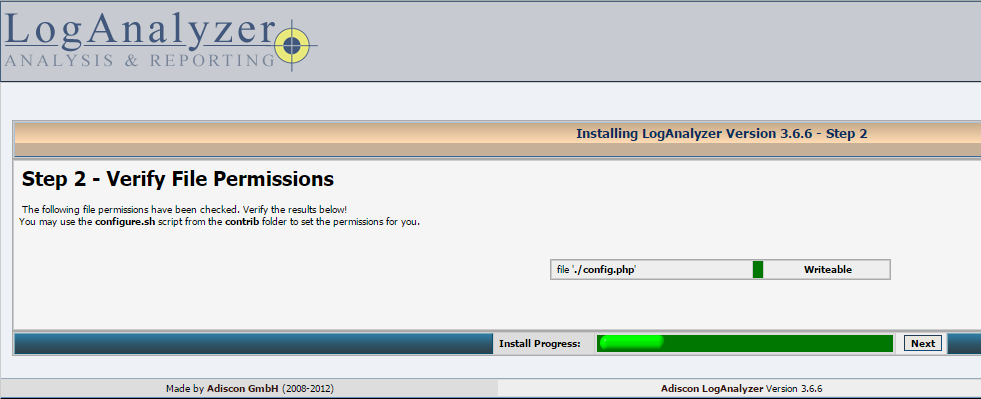
***./configure***

******

Maintenant que LogAnalyzer est installé, nous allons accéder à l'interface web en se rendant sur l’adresse [***http://localhost/install.php***](http://localhost/install.php) (ou [***http://adresseduserveur/installphp***](http://adresseduserveur/installphp)). Mais avant toutes choses, nous redémarrons le service ***apache2*** (***/etc/init.d/apache2 restart***).Nous devrions avoir la première étape de l’installation de LogAnalyzer. Nous cliquons sur ***Next***. L’installation nécessite d’être minutieux car certaines étapes sont très importantes au bon fonctionnement de notre serveur de logs.

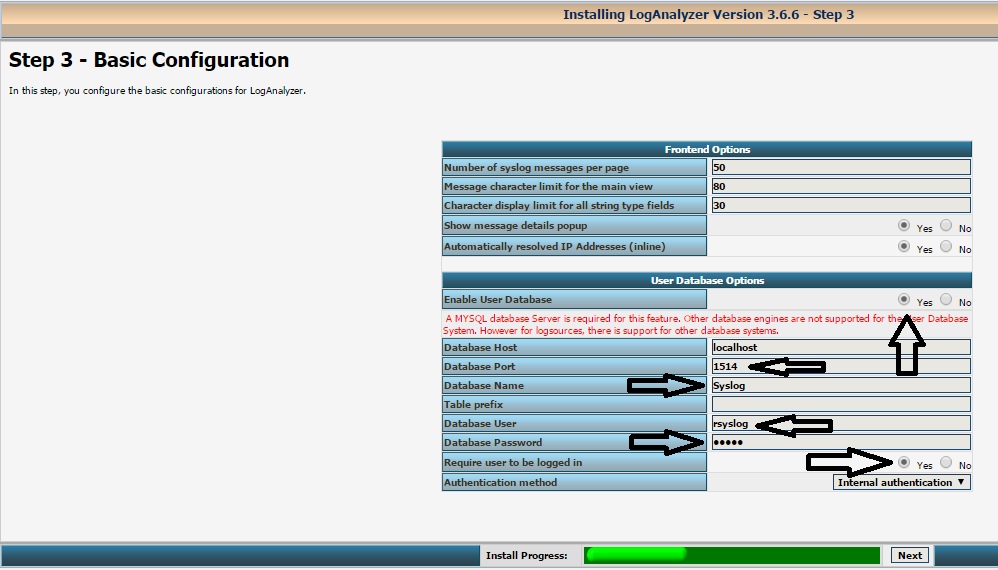


Nous avons ensuite la deuxième étape qui vérifie si le fichier ***config.php*** est modifiable. Faisons ***Next***.

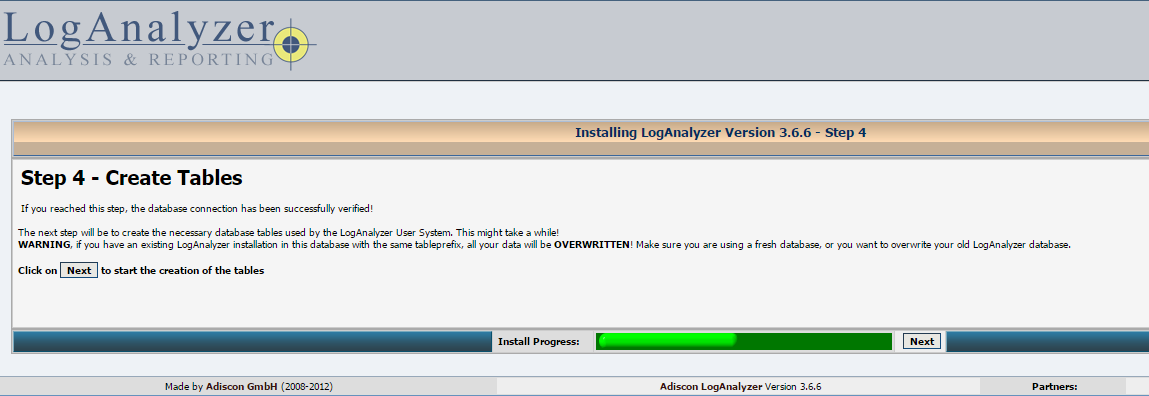


Nous voilà arrivé à l’étape numéro 3. Il faut correctement compléter les informations de cette étape. Au niveau de la ligne ***Enable User Database*** nous allons cocher la case ***yes***. Nous allons changer les informations pas défaut par les données que nous allons utiliser. Au niveau de ***Database Port*** nous allons mettre le numéro de port que nous avons mis dans le fichier ***rsyslog.conf*** donc ce sera ***1514***.

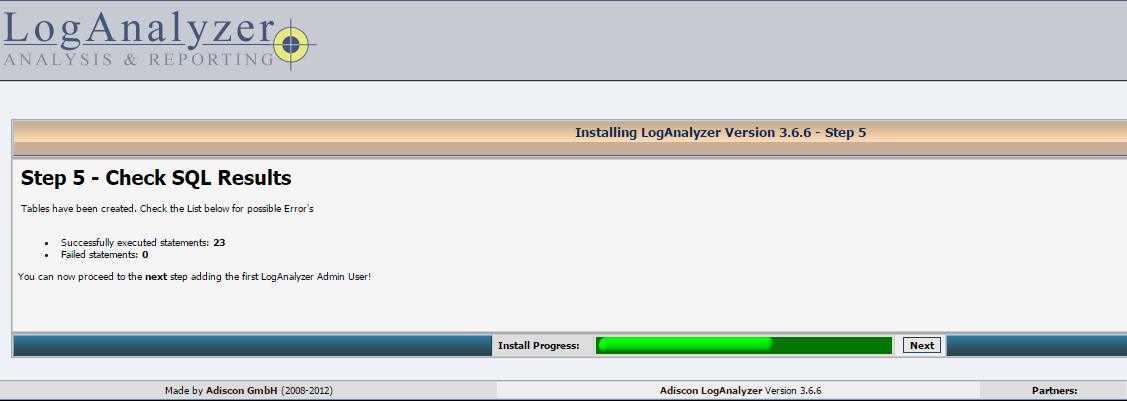
Au niveau de ***Database Name*** nous allons mettre le nom de notre base de données qui est ***Syslog***. Ensuite, ce sera au tour de ***Table prefix*** que nous supprimons. Nous choisissons maintenant l’utilisateur au niveau de ***Database User*** que nous avons choisis dans le fichier ***rsyslog.conf*** donc ***rsyslog***. Et enfin, nous rentrons le mot de passe dans ***Database Password*** qui est celui que nous avons choisis au moment de l’installation de ***rsyslog*** et nous cochons la case ***Require user to be logged in***. Nous pouvons ensuite faire ***Next***.



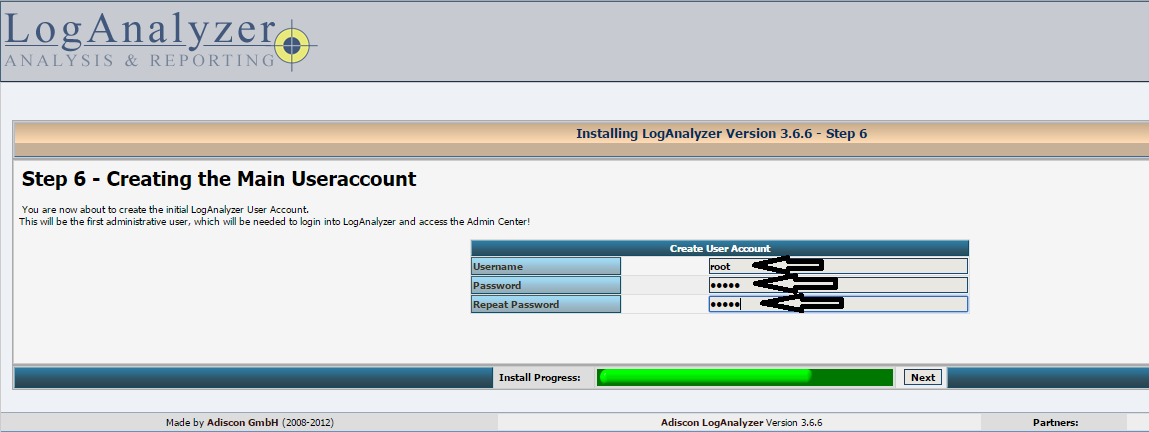
Nous arrivons à l’étape numéro 4 qui nous stipule que notre base de données a été vérifiée. Cliquons sur ***Next***.



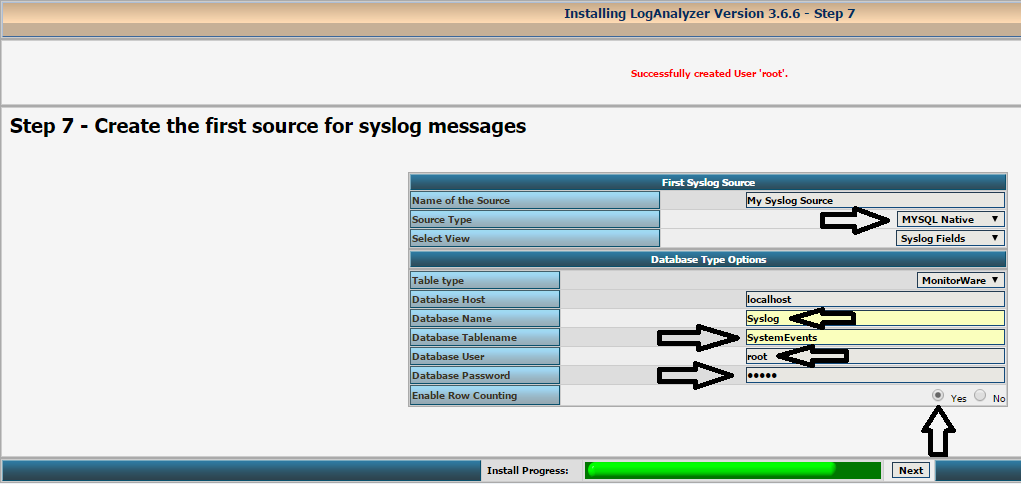
L’étape numéro 5 nous indique que nos tables sont correctes. Cliquons une fois de plus sur ***Next***.



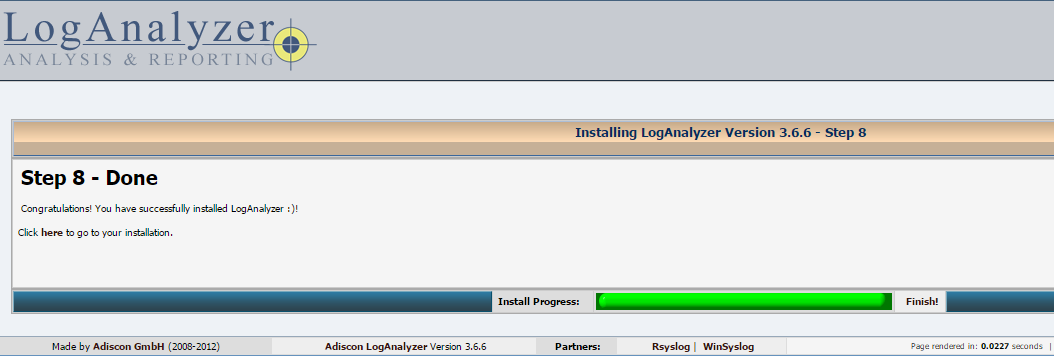
L'étape 6 nous demande de créer un utilisateur. Dans notre situation je choisis l’utilisateur ***root*** et comme mot de passe ***hhhhh***. ***Next***.



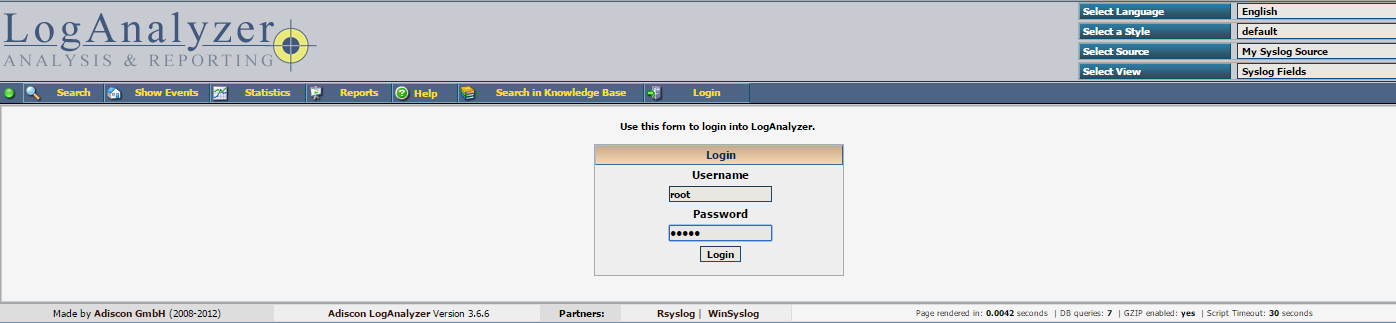
Nous arrivons à l'étape 7 qui est elle aussi très importante. Il nous est demandé de renseigner les informations de notre base de données qui récupèrera les informations des clients et qui les affichera sur ***LogAnalyzer***. Il faut choisir l’option ***MYSQL Native*** au niveau de ***Source Type.*** Les informations à rentrer sont donc ***Syslog*** pour ***Database Name***, ***SystemEvents*** (les majuscules sont à respecter) pour ***Database Tablename***, ***root*** pour ***Database User*** et ***hhhhh*** pour ***Database Password***.



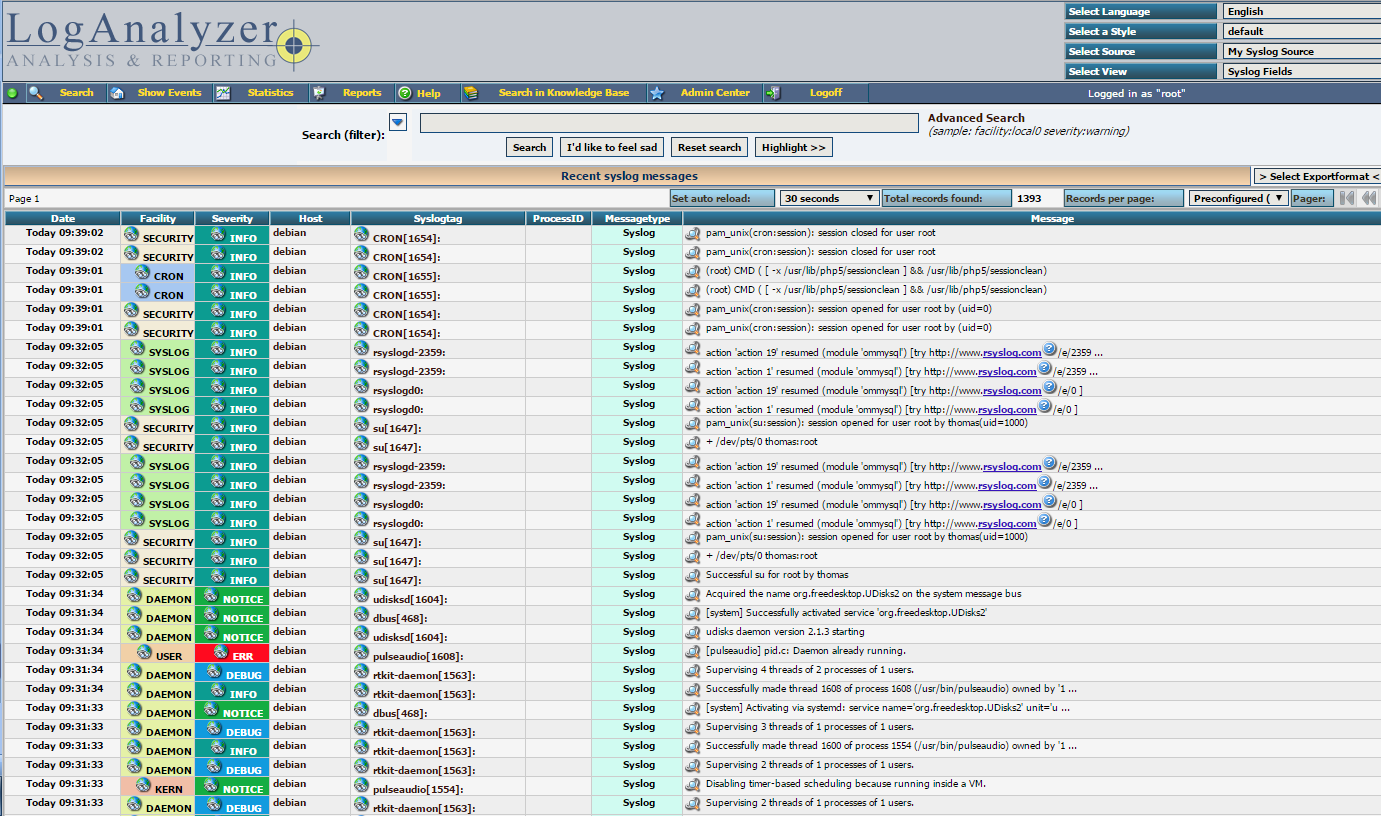
L’étape numéro 8 nous indique que toutes les informations rentrées sont correctes et que nous pouvons passer à nos logs. ***Next***.



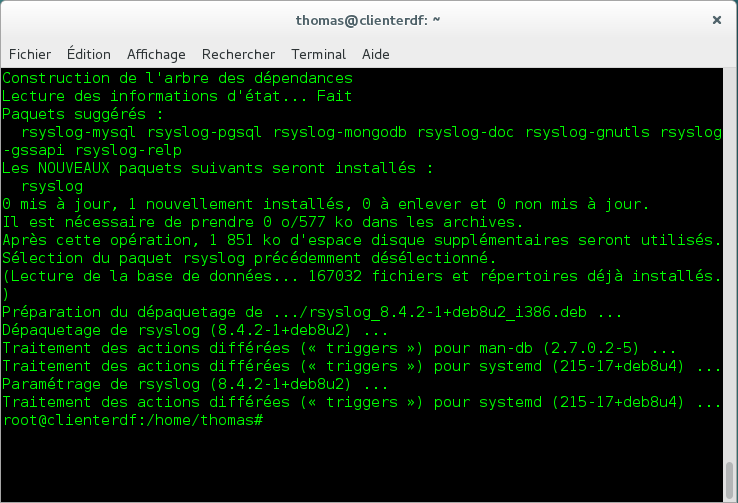
Pour entrer dans notre base de logs, il faut nous connecter avec l’utilisateur créé précédemment qui est donc ***root*** et ***hhhhh***.



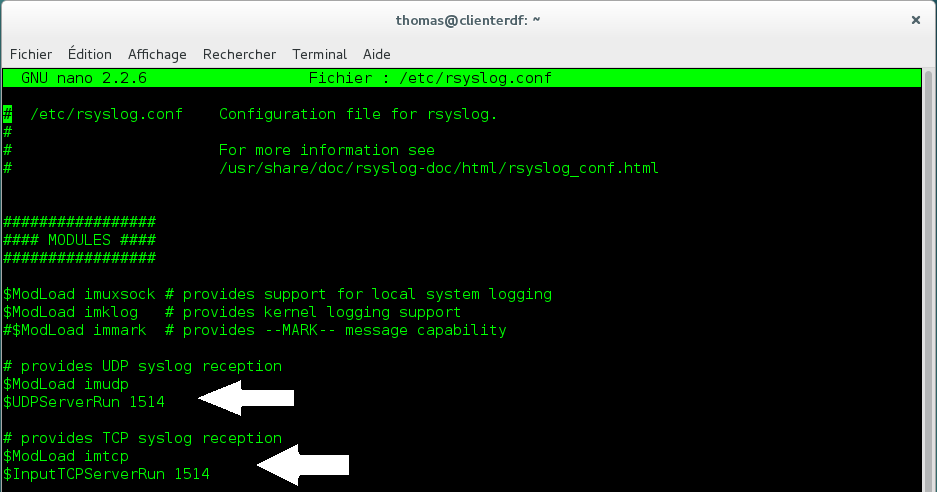
Voici ce que l’affichage de LogAnalyzer devrait donner :



Bon, maintenant que notre serveur de centralisation des logs est installé et fonctionnel, nous allons configurer les clients pour qu’ils envoient leurs informations à notre serveur. Nous allons commencer par les clients type Unix (ici ce sera Debian 8). La manipulation des clients est relativement simple. Il faut commencer par installer le paquet ***rsyslog*** avec la commande ***apt-get install rsyslog***.

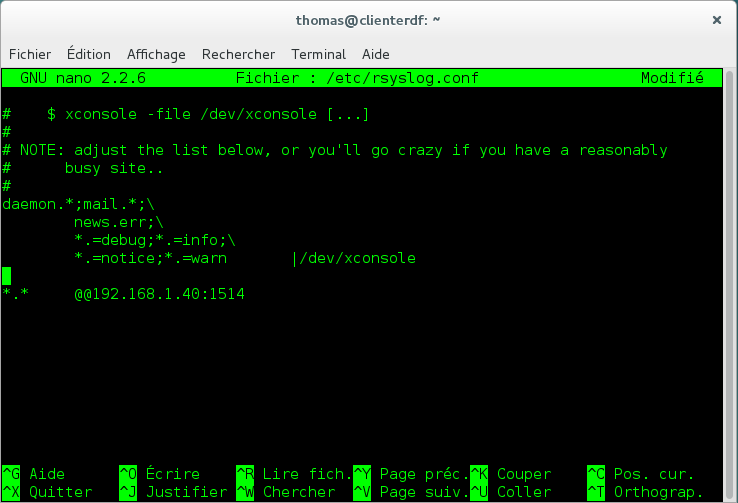
******

Comme pour l’installation de ***rsyslog***, il faut que l’on dé commente les paramètres dans le fichier ***rsyslog.conf*** avec la commande ***nano /etc/rsyslog.conf.***

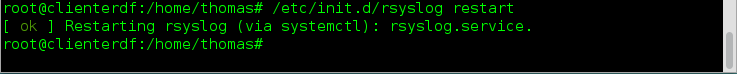


Maintenant, pour que le client envoie ses informations au serveur il faut se rendre tout en bas du fichier ***rsyslog.conf*** et ajouter la ligne suivante : ***\*.\* @@adresseduserveur :1514***

Cette ligne signifie que le client envoie toutes ses informations avec le protocole de niveau 3 dans le modèle OSI ***TCP*** via le port 1514.

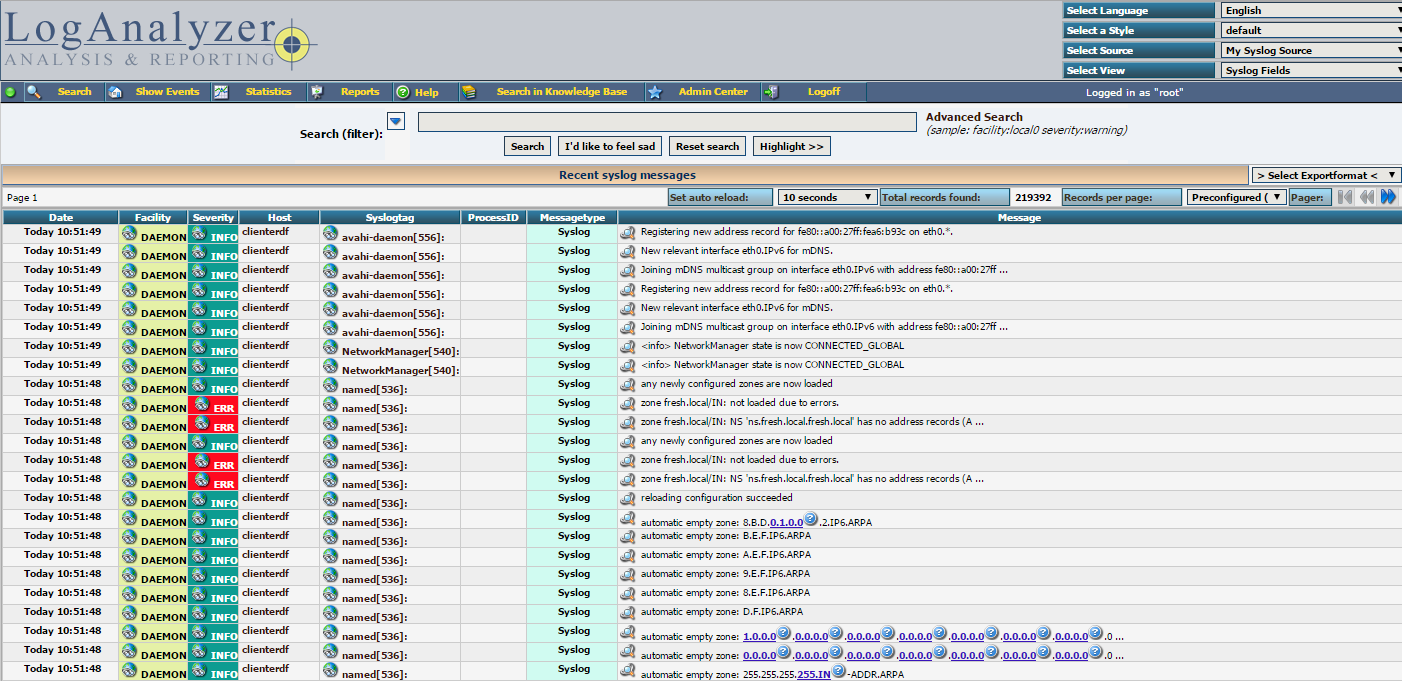


Il ne nous reste plus qu’à redémarrer le service ***rsyslog*** avec la commande ***/etc/init.d/rsyslog restart***

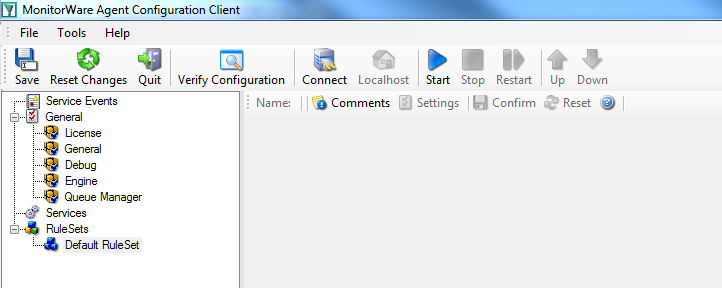


Cette manipulation concernant les machines clients sous Debian sont à reproduire autant de fois qu’il y a de machines Debian sur le réseau. Sur la page web de LogAnalyzer nous verrons dorénavant les informations envoyées par les clients.

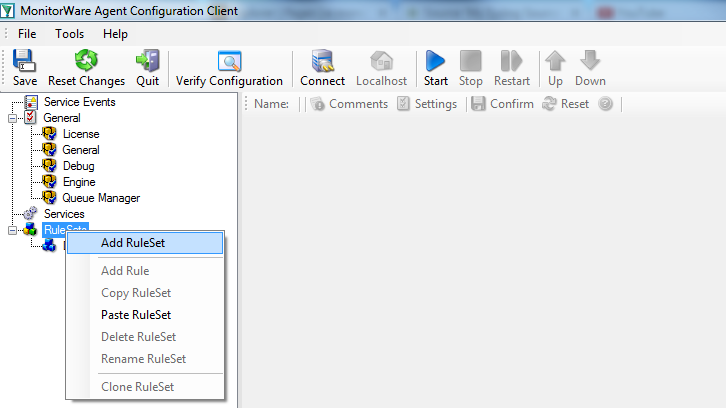
Dans le cas ci-dessous, nous voyons le client nommé ***clienterdf*** qui a utilisé le service de ***NetworkManager*** pour un renouvellement d’adressage. Nous pouvons constater qu’il y a 4 messages d’erreur car il y a un problème de DNS en local (dû à une configuration non terminée).



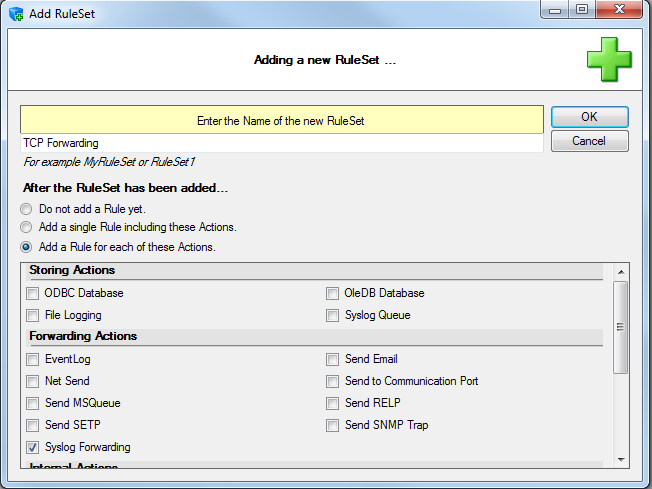
Nous allons maintenant voir comment faire envoyer les logs d’une machine sous Windows sur un serveur Debian. Pour ce faire nous pouvons utiliser un logiciel payant mais qui a une période d’essaie nommé ***MonitorWare***. Ce logiciel est téléchargeable [ici](http://www.mwagent.com/download/). L’interface se présente ainsi :



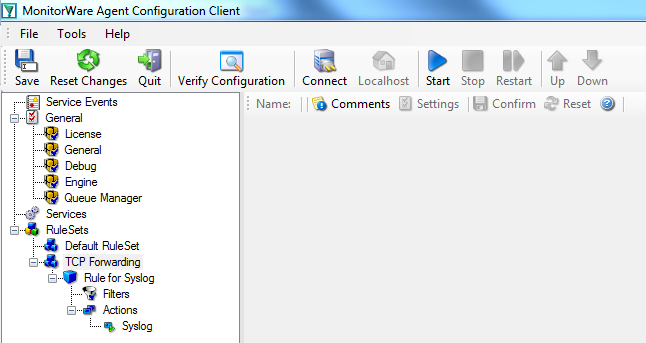
Pour commencer, il faut ajouter une règle. Donc pour ajouter une règle il faut cliquer droit sur ***Rule Sets*** et aller sur ***Add RuleSet***.



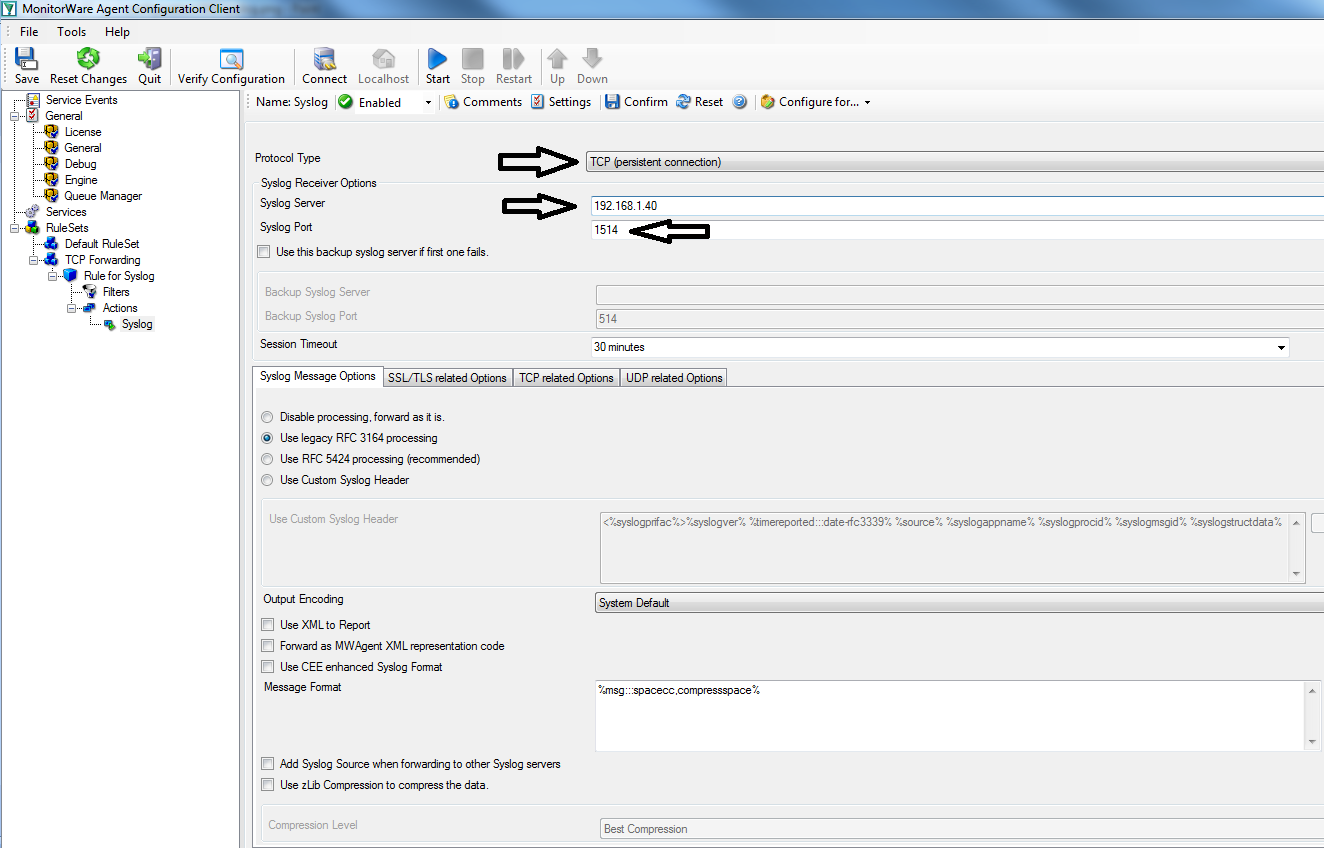
Une nouvelle fenêtre fait son apparition nous demandant d’attribuer un nom à notre nouvelle règle. Je l’ai appelée ici ***TCP Forwarding***. Nous cochons la case ***Add a Rule for each of these Actions*** puis nous sélectionnons ***Syslog Forwarding***.



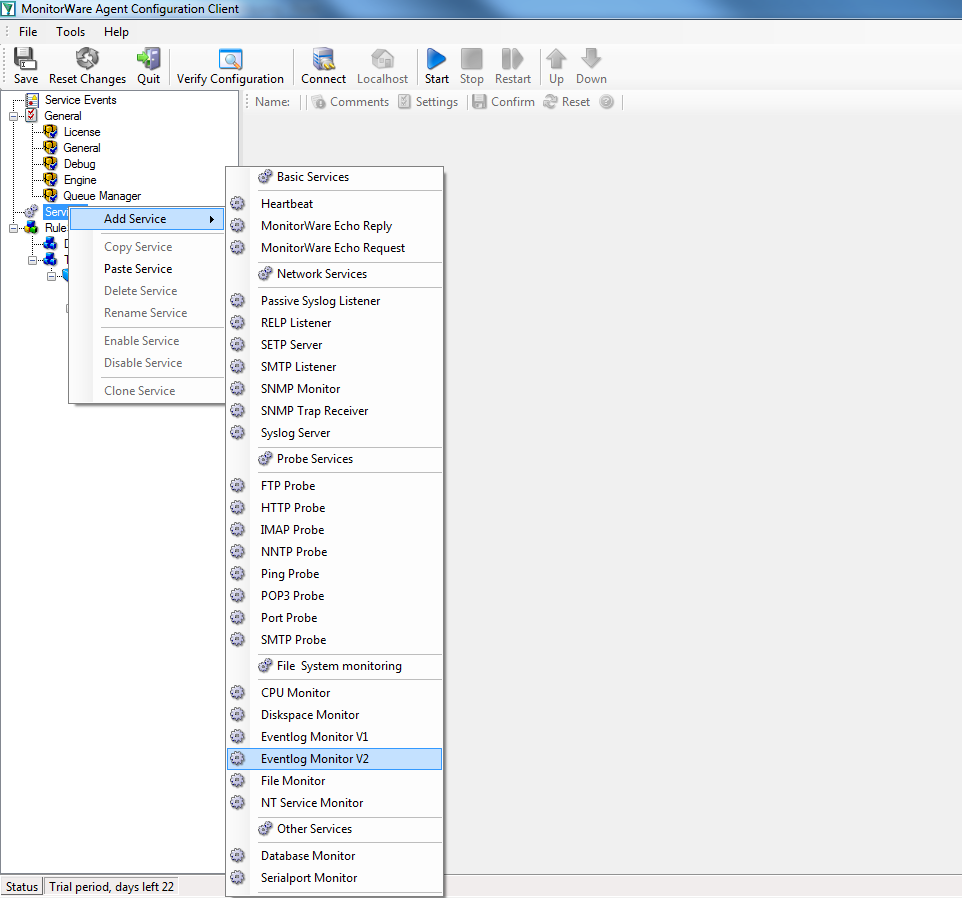
Nous devons obtenir une arborescence de ce type : ***TCP Forwarding*** – ***Rule for Syslog – Actions – Syslog***.



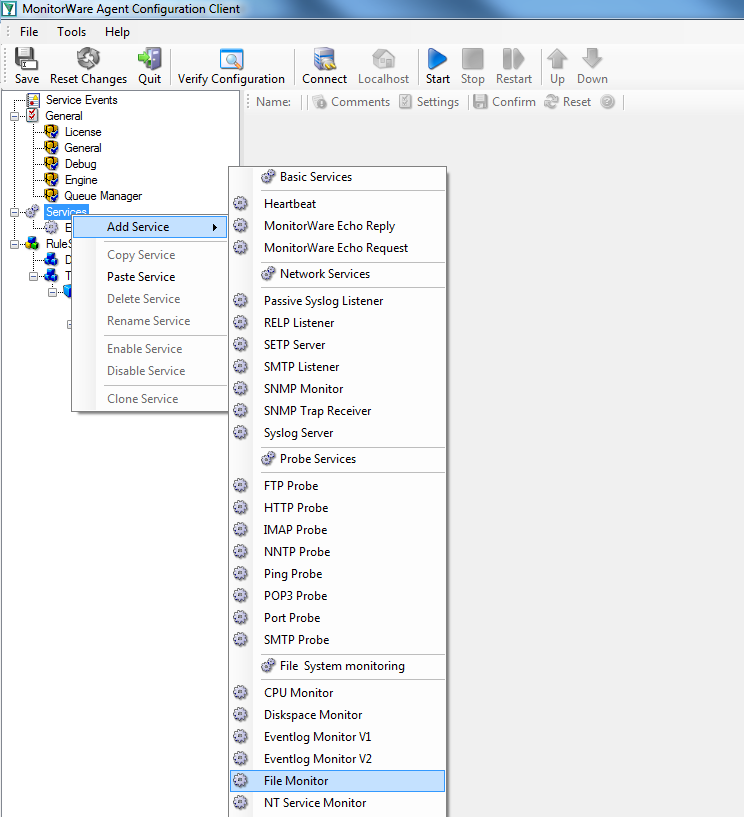
Nous allons commencer la configuration de notre client Windows. Pour ce faire nous allons nous rendre dans ***Syslog*** situé à la fin de l’arborescence dans ***Actions***. Certaines informations sont à rentrer comme l’adresse du serveur de logs, le port utilisé, le type de protocole qui sera ***TCP (persistent connection)*** et d’autres options qui ne nous sont pas nécessaires dans le cadre de cette documentation. Puis cliquons sur ***Save*** en haut à gauche.



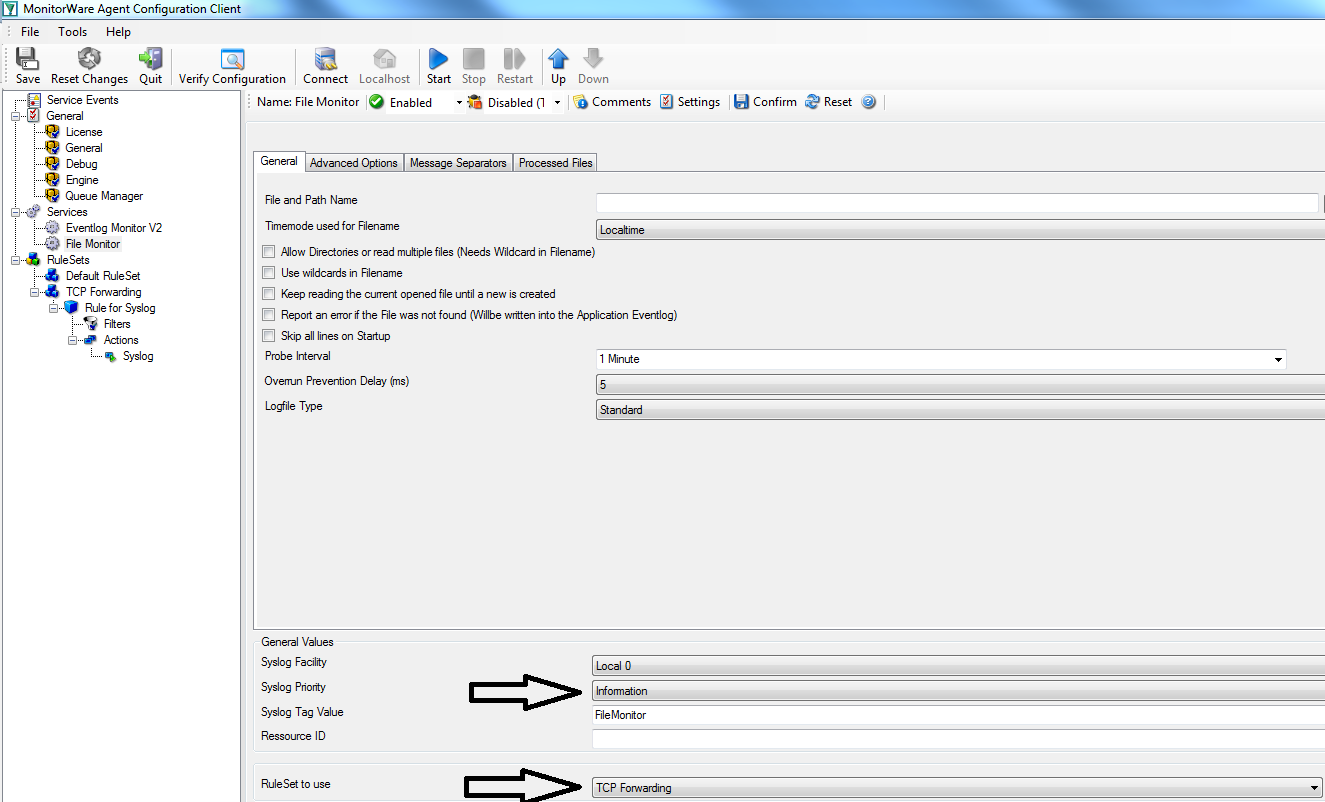
Prochaine étape, nous allons ajouter deux services. Donc nous cliquons droit sur ***Services***, nous allons sur ***Add Service*** puis nous sélectionnons ***Eventlog Monitor V2***.



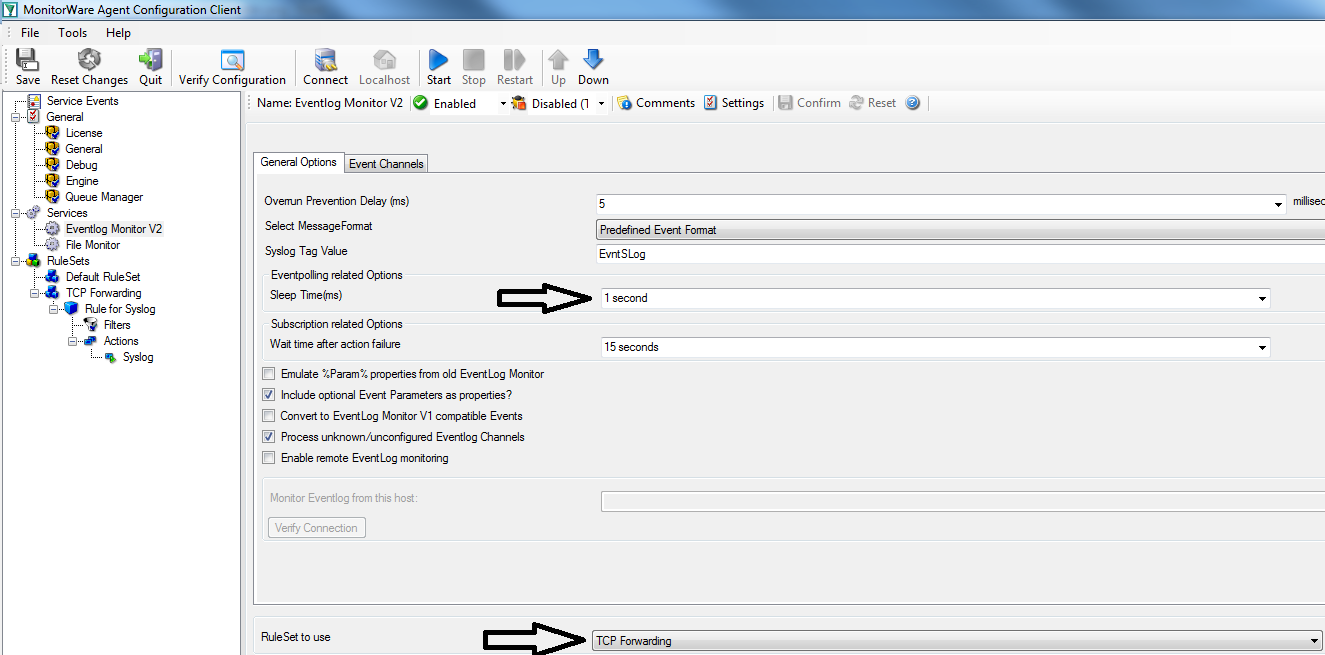
Nous allons ajouter un second service donc nous procédons à la même manipulation sauf que nous sélectionnons ***File Monitor***.



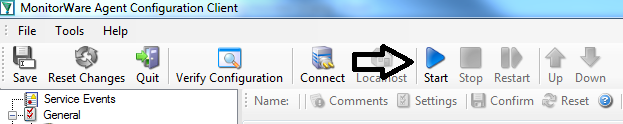
Maintenant que nos deux services sont créés, nous allons configurer (c’est très rapide) le service ***File Monitor***. Une fois dans ***File Monitor***, nous nous rendons en bas et sélectionnons dans ***RuleSet to use*** l’option ***TCP Forwarding*** qui est notre règle. Puis dans ***Syslog Priority*** nous choisissons ***Information***.



Configurons maintenant le service ***Eventlog Monitor V2*** en choisissant ***1 second***  dans ***Sleed time(ms)***, puis nous sélectionnons notre règle ***TCP Forwarding*** dans ***RuleSet to use***.



Et voilà ! Notre client ***MonitorWare*** sous Windows est maintenant fonctionnel. Il ne nous plus qu’à cliquer sur le bouton ***Start*** en haut.



Si nous retournons sur notre interface web avec LogAnalyzer nous pourrons voir notre nouveau client ici nommé ***Internet-PC***.

