LES LOGS

LogAnalyzer

ST JO SUP

13 décembre 2017

Créé par : Alexandre Mutel, Kevin Bréant, Djibril Guenni

LES LOGS

LogAnalyzer

Table des matières

I) Les logs qu'est-ce que c'est ?

1) Définition

En informatique, on parle de log (diminutif de logging) pour désigner un fichier, ou tout autre dispositif, permettant de stocker un historique des évènements attachés à un processus. Ces évènements sont horodatés et ordonnés en fonction du temps. En clair, le log est un peu le "journal de bord" d'un système. On parle parfois en français de fichier journal pour désigner les logs. Il sera consulté en cas de besoin, par exemple pour essayer d'identifier l'origine d'une panne ou l'auteur d'une intrusion (réussie ou manquée).

Voici une image montrant à quoi peut ressembler des logs :

2) Les différents logs

a) Log des accès serveur (journal d'accès au serveur)

Pour un serveur web (comme par exemple apache), on désigne généralement par log serveur le dispositif permettant de connaître le détail des différentes requêtes effectuées par des clients (au sens client-serveur). On parle de "journal des accès au serveur". Il s'agit en réalité d'un abus de langage : le serveur possède également d'autres types de logs. Les informations stockées dans ces logs sont typiquement :

- L'adresse IP depuis laquelle est effectuée la requête.

- L'utilisateur si celui-ci est authentifié.
- La date de la requête, placée entre crochets.
- La requête elle-même, placée entre guillemets.
- Le code de réponse de statut du serveur.
- La taille de l'objet envoyé par le serveur au client, en octets.

b) Log de connexion

De nombreux systèmes informatiques stockent l'historique des accès authentifiés à une application. Ce log est particulièrement utile pour savoir qui s'est connecté à un système et à quelle heure. Les applications de ce log sont nombreuses : contrôle des salariés, enquêtes judiciaires, identification des comptes corrompus en cas d'intrusion, etc.

c) Log en webanalytics

On l'oublie souvent, mais les systèmes de mesure du trafic web ne sont en réalité que des logs évolués, qui collectent de nombreuses informations à chaque fois qu'un utilisateur consulte un site web.

d) Log d'erreur

Les logs d'erreur sont surtout utiles aux développeurs. Ils permettent d'enregistrer les différentes informations d'environnement lorsqu'une erreur se produit sur un système, facilitant ainsi le débogage.

II) Installation et configuration de rsyslog et LogAnalyzer

Rsyslog est présent par défaut dans Ubuntu et Debian depuis peu et LogAnalyzer est l'interface graphique web permettant d'interagir avec la base de données dans laquelle rsyslog va stocker les logs qui lui parviennent du réseau.

Pour suivre ce qui suit, il vaut mieux avoir un serveur LAMP fonctionnel et une machine à jour.

1) Installation et configuration de rsyslog

- Rsyslog est installé par défaut mais il faut lui rajouter un module MySQL, grâce à la commande suivante : `aptitude install rsyslog-mysql`

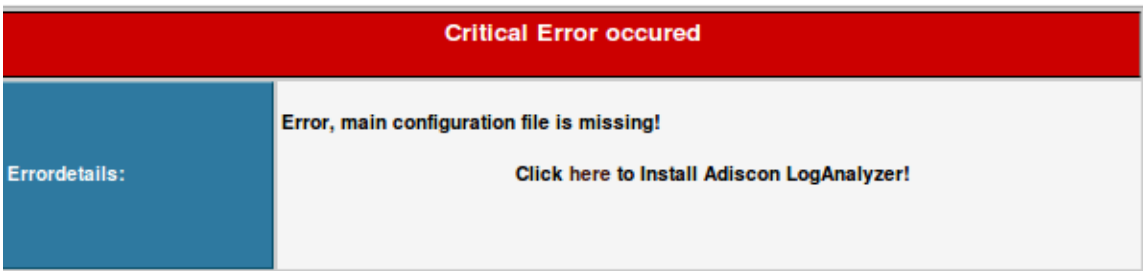
- Pour la configuration tout passe dans un fichier de configuration, pour y accéder on utilise la commande : `nano /etc/rsyslog.conf`
    - Dans ce fichier on décommentera (enlever le # qui est devant) ces six lignes :
        - **provides UDP syslog reception**
        - **$ModLoad imudp**
        - **$UDPServerRun 514**
        - **provides TCP syslog reception**
        - **$ModLoad imtcp**
        - **$InputTCPServerRun 514**
    - Puis on modifiera les lignes :
        - **$UDPServerRun 514** par **$UDPServerRun 1514**
        - **$InputTCPServerRun 514** par **$InputTCPServerRun 1514**
    - Normalement on dispose d'un serveur MySQL donc il faut là encore activer le module MySQL de rsyslog en décommentant ou ajoutant une ligne (si vous devez en ajouter faites-le tout en bas) :
        - **$ModLoad MySQL**
    - Ensuite pour que rsyslog rentre automatiquement les logs dans la base de données il faut lui donner les informations de connexion à cette base :
        - ***.* >serveurSQL,nomdelabase,utilisateur,motdepasse**
    - Vous enregistrez en faisant CTRL+O et vous quittez en faisant CTRL+X
    - Pour être sur des modifications effectuées vous pouvez redémarrer le service grâce à la commande : `/etc/init.d/rsyslog restart`

- On créera ensuite la base de données via le terminal en mode superutilisateur avec la commande : `mysql -u root --password=votremotdepasse` puis `CREATE DATABASE Syslog;`

2) Installation et configuration de LogAnalyzer

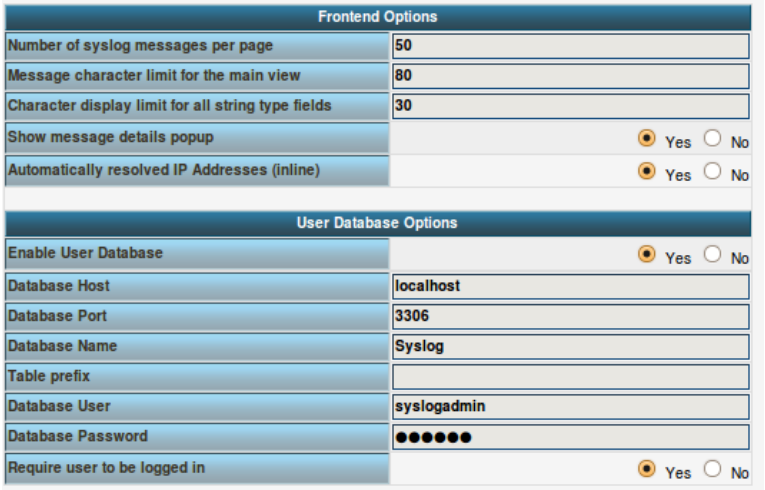
- On va tout d'abord le télécharger puis placer l'archive sur le bureau
- Ensuite on extrait l'archive grâce à la commande : `tar -zxvf /home/ « nom d'utilisateur »/Bureau/loganalyzer-4.1.5.tar.gz`

- On déplace le dossier que l'on vient d'extraire grâce à la commande : `cp -R loganalyzer-4.1.5/src/ /var/www/`
- Afin que l'installation se déroule sans encombre il faut mettre les droits d'écriture sur le contenu du dossier /src ; pour plus de simplicité on va appliquer ces droits à tout le répertoire ainsi qu'aux sous-dossiers grâce à la commande : `chmod 777 /var/www/src`
- Ensuite à l'aide d'un navigateur type Firefox ou autre on se rend à l'adresse : `http://127.0.0.1/src` plus tard une fois que notre serveur sera opérationnel nous pourrons nous connecter à distance grâce à `http://« adresse IP du serveur »/src`
- Cet écran s'affiche alors :



Mais c'est tout à fait normal vu que l'on n'a pas encore créé le fichier de configuration. Ce fichier va se créer et se remplir au fur et à mesure que l'on avance dans l'installation.

- Suivent plusieurs écrans de vérification de la configuration. Le plus important est le 3e qui doit nous permettre de configurer l'interaction avec notre base de données notamment ici pour stocker les utilisateurs.
- On y renseigne les informations de connexion à la base ainsi que le nombre de log qui vont apparaître simultanément sur la page de LogAnalyzer.
- Puis l'assistant d'installation va créer les tables.



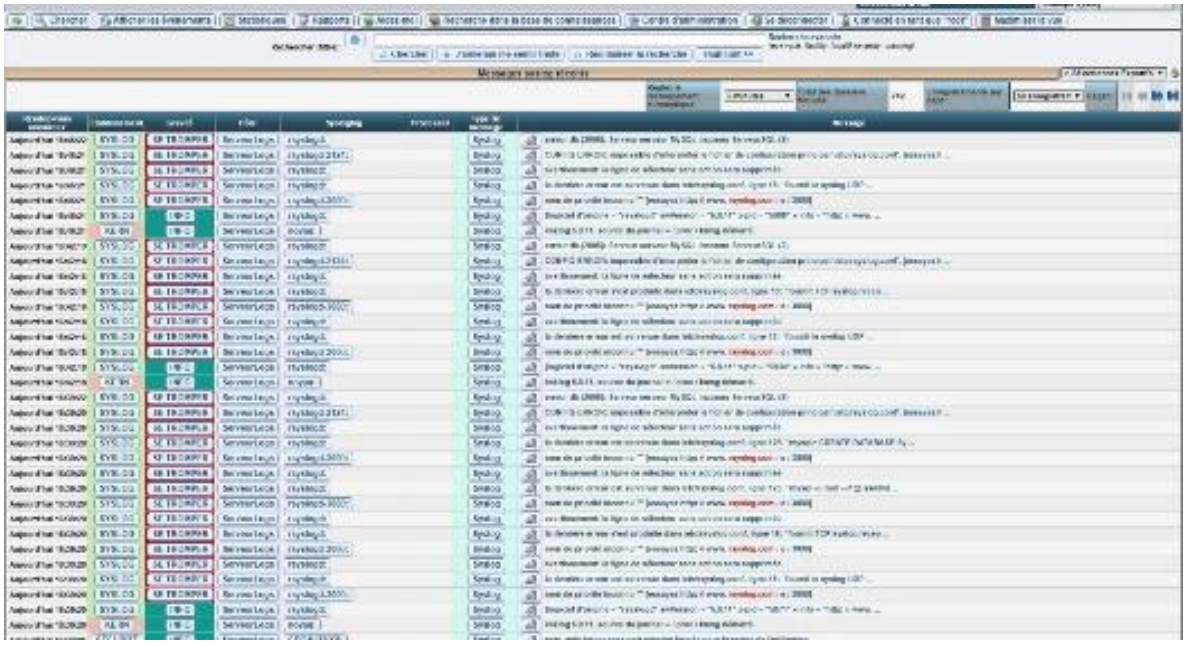
- L'étape 6 est très importante car elle permet de déterminer le login et le mot de passe pour l'accès à l'interface de LogAnalyzer

Create User Account	
Username	admin
Password	●●●●●●
Repeat Password	

- Ensuite on paramètre notre première source de log soit notre base de données (faire attention en remplissant sinon ça ne fonctionnera pas, s'il y a des majuscules il faut les rentrées) :

First Syslog Source	
Name of the Source	Source1
Source Type	MYSQL Native
Select View	Syslog Fields
Database Type Options	
Table type	SyslogNG
Database Host	localhost
Database Name	Syslog
Database Tablename	SystemEvents
Database User	syslogadmin
Database Password	●●●●●●
Enable Row Counting	(•) Yes ( ) No

- La configuration est maintenant terminée nous allons pouvoir nous connecter à l'interface d'administration et visualiser les logs de notre réseau
- Une fois, votre nom d'utilisateur et votre mot de passe rentrés, vous devrez normalement arriver sur cette page :

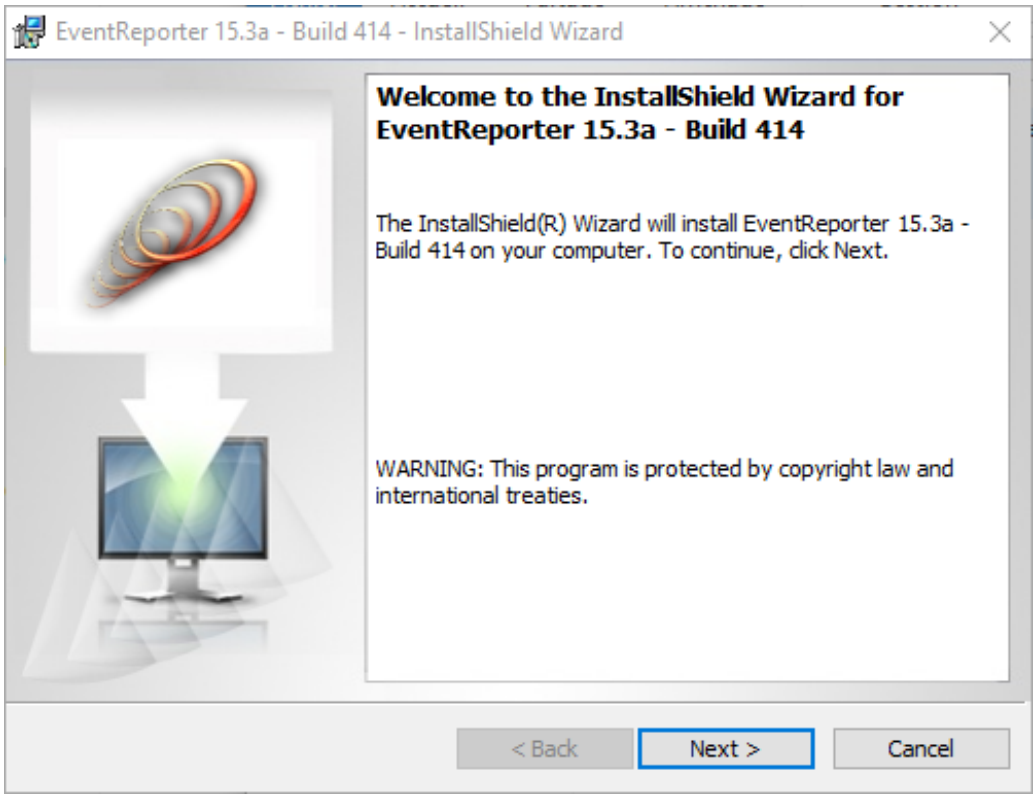


III) Envoyer des logs d'un système Windows sur notre serveur de logs

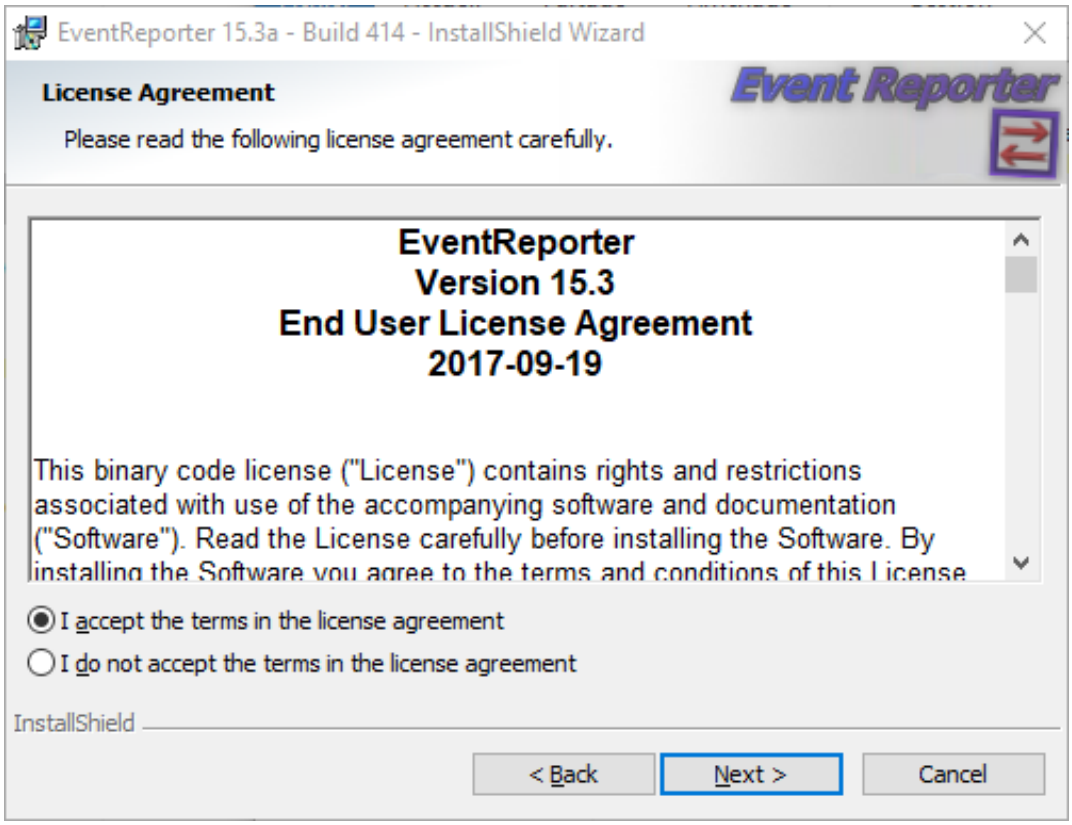
Pour pouvoir envoyer des logs Windows sur un serveur de logs sous Linux on devra télécharger un logiciel car Windows ne peut pas par défaut envoyer ses logs vers un système Linux. Dans mon cas j'ai utilisé le logiciel EventReporter.

1) Installation d'EventReporter

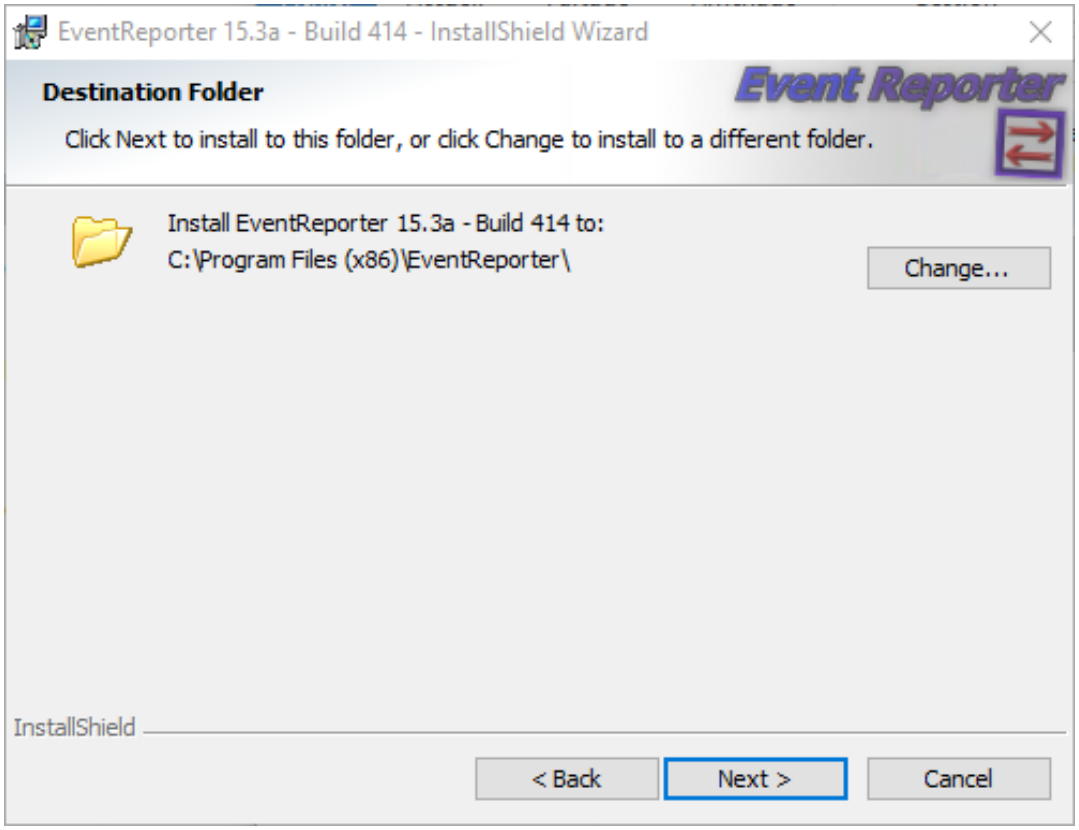
- Une fois que vous avez téléchargé le logiciel, faites un double clic, ceci devrait apparaître, cliquer sur next



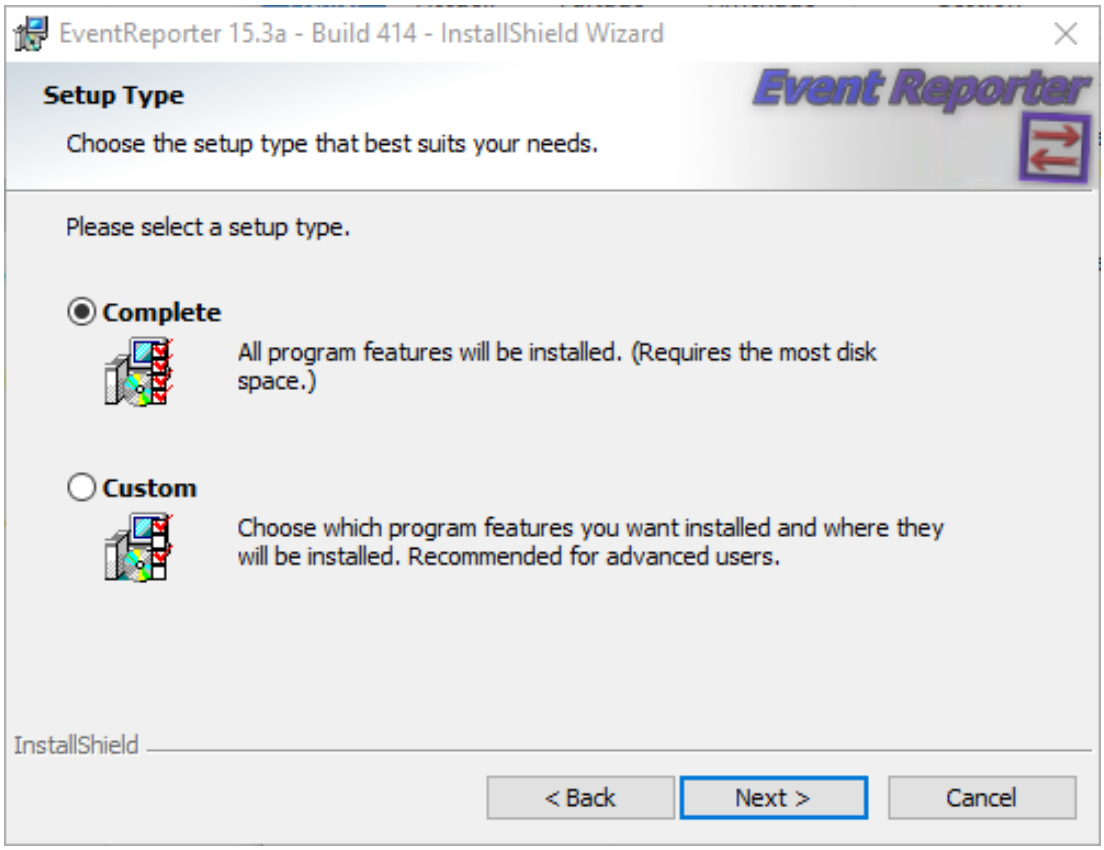
- Accepter les termes du contrat et cliquer sur next



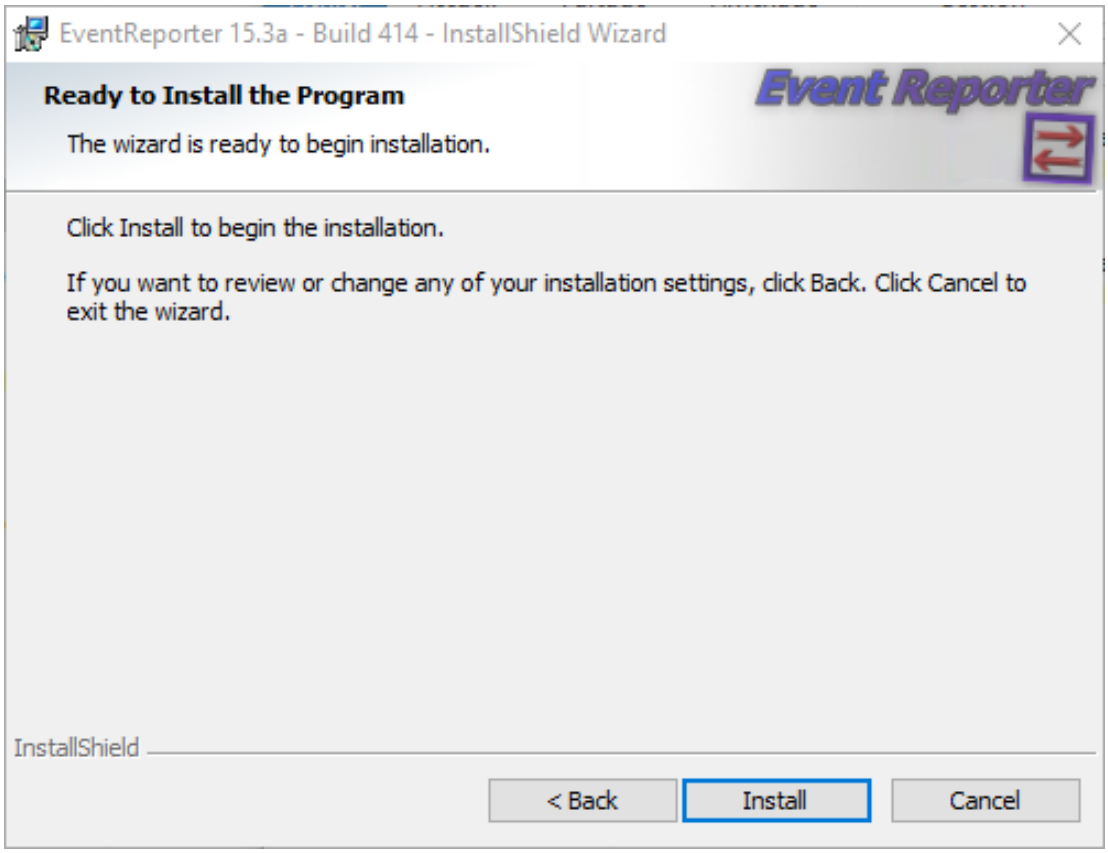
- Choisissez le dossier d'installations du logiciel et cliquer sur next



- Choisissez ensuite le type d'installation et cliquer sur next

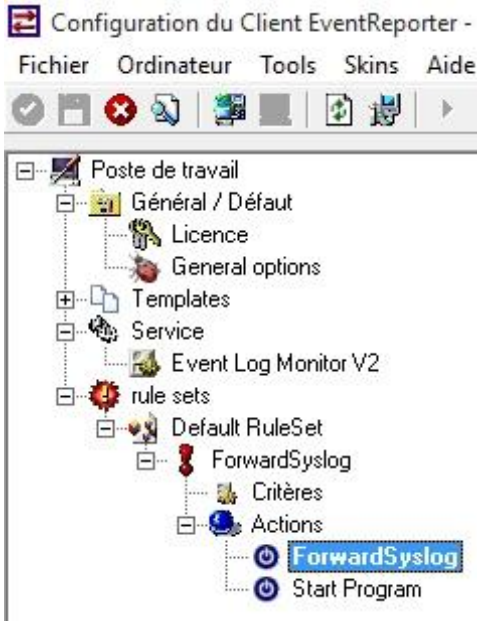


- Enfin cliquer sur install

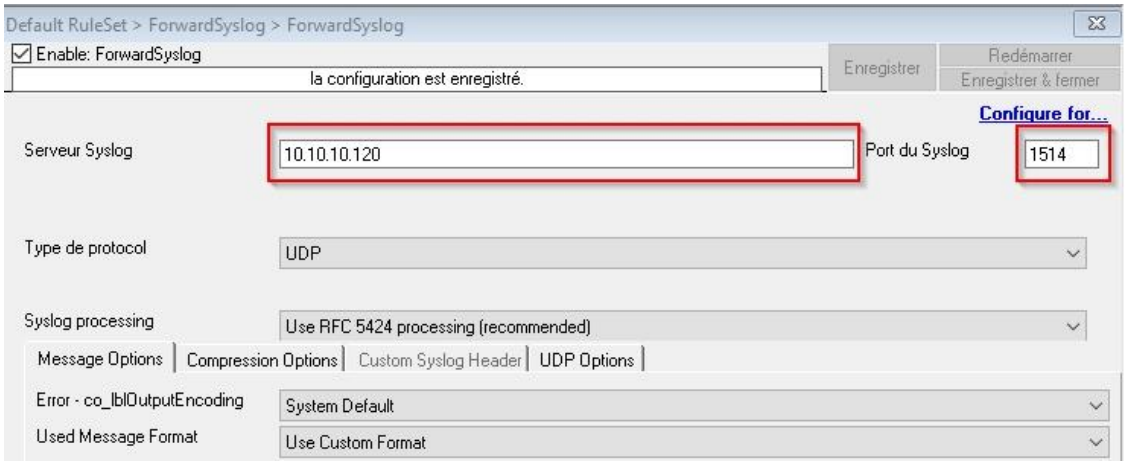


2) Configuration d'EventReporter

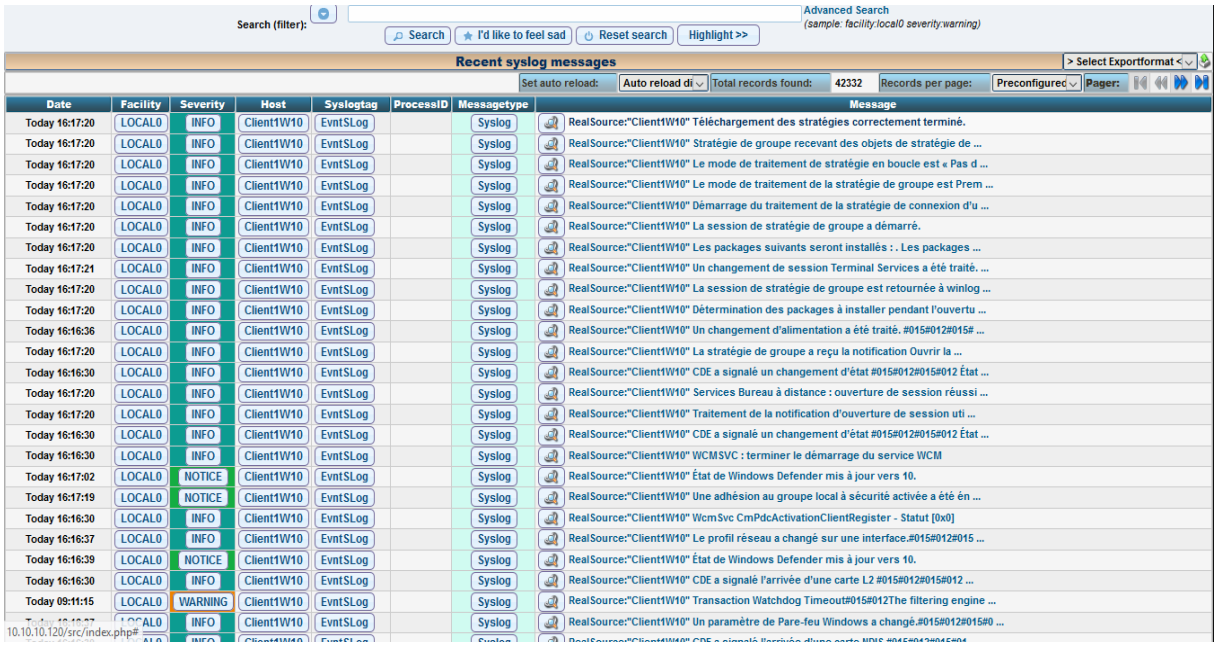
- Pour configurer le logiciel, dérouler les menus :
  - Poste de travail
  - Rule sets
  - Default RuleSet
  - ForwardSyslog
  - Actions
- Et cliquer sur ForwardSyslog



- Une fois que vous êtes dans le bon menus nous allons rentrer l'adresse IP ainsi que le port de notre serveur en faisant attention que notre protocole est bien sur UDP et cliquer sur enregistrer.



- Voici une image montrant les logs Windows remontés sur notre serveur de logs :



IV) Conclusion

Pour conclure on peut dire que LogAnalyser est un bon outil pour visualiser les logs de différents systèmes d'exploitation et ainsi voir et réparer les différentes erreurs sur les différentes machines. De plus le logiciel est administrable via une interface web, ce qui fait que l'on peut aller regarder les logs depuis n'importe quel appareil.