

loganalyzer

Objectif

Nous allons ici procéder à l'installation de l'application **Loganalyzer** nous permettant d'avoir une interface graphique de gestion des logs.

Pre-requis

Avoir installé les programmes :

- [rsyslog](#)
- l'environnement [LAMP](#)

Installation

On télécharge depuis le site officiel de l'application la dernière version stable et décompressons l'archive obtenue. Nous créons ensuite un dossier dans **/var/www**.

```
# mkdir /var/www/loganalyzer
```

Puis nous copions/collons les fichiers nécessaire et changeons le propriétaire.

```
# cp -a loganalyzer-3.6.6/src/* /var/www/loganalyzer/  
# chown -R www-data:www-data /var/www/loganalyzer/
```

Configuration

On ouvre l'application dans notre navigateur internet, ici <http://172.16.4.103/loganalyzer/>

Lors de la première étape, nous n'avons qu'à cliquer sur le bouton **next**. Le système vérifie alors qu'il possède le droit d'écrire sur fichier *config.php*.

La troisième étape consiste à effectuer une configuration de base du logiciel. Dans cette étape, nous activons l'utilisation d'une base de donnée en définissant les paramètres de connexion et la base de donnée nécessaire à son bon fonctionnement.

Step 3 - Basic Configuration

In this step, you configure the basic configurations for LogAnalyzer.

Frontend Options	
Number of syslog messages per page	50
Message character limit for the main view	80
Character display limit for all string type fields	30
Show message details popup	<input checked="" type="radio"/> Yes <input type="radio"/> No
Automatically resolved IP Addresses (inline)	<input checked="" type="radio"/> Yes <input type="radio"/> No

User Database Options	
Enable User Database	<input checked="" type="radio"/> Yes <input type="radio"/> No
<small>A MYSQL database Server is required for this feature. Other database engines are not supported for the User Database System. However for logsources, there is support for other database systems.</small>	
Database Host	localhost
Database Port	3306
Database Name	Syslog
Table prefix	logcon_
Database User	rsyslog
Database Password	*****
Require user to be logged in	<input checked="" type="radio"/> Yes <input type="radio"/> No
Authentication method	Internal authentication ▼

Les étapes 4 et 5 ne requièrent aucune action, on peut cliquer sur le bouton **next** sur ces deux étapes.

Nous arrivons à l'étape 6, consistant à créer le premier utilisateur de notre installation LogAnalyzer. Nous choisissons de mettre **admin** en *Username* et **roger** en *Password*

Lors de l'étape 7, nous ajouter une source de donnée. On définit le type (*Source Type*) en **MYSQL Native** et remplissons les informations de connexion comme précédemment.

Step 7 - Create the first source for syslog messages

First Syslog Source	
Name of the Source	Rsyslog
Source Type	MYSQL Native ▼
Select View	Syslog Fields ▼

Database Type Options	
Table type	MonitorWare ▼
Database Host	localhost
Database Name	Syslog
Database Tablename	systemevents
Database User	rsyslog
Database Password	*****
Enable Row Counting	<input checked="" type="radio"/> Yes <input type="radio"/> No

Il faut bien préciser les majuscules sur le champ *Database Tablename* ⇒ **SystemEvents**

La huitième et dernière étape est une confirmation annonçant la bonne configuration du logiciel. On clique sur *Finish* pour arriver sur l'écran de login de l'application. Une fois logué avec nos identifiants créer dans les étapes plus haut, nous avons accès au logs.

The screenshot shows the LogAnalyzer web interface. At the top, there's a navigation bar with options like 'Search', 'Show Events', 'Statistics', 'Reports', 'Help', 'Search in Knowledge Base', 'Admin Center', and 'Logout'. Below this is a search filter and an advanced search box. The main content area is titled 'Recent syslog messages' and contains a table with columns: Date, Facility, Severity, Host, Syslogtag, ProcessID, Message type, and Message. The table lists various system events such as authentication failures, account expirations, and session management.

Date	Facility	Severity	Host	Syslogtag	ProcessID	Message type	Message
Today 11:09:01	CRON	ERR	roger	CRON[3209]:	Syslog	Authentic d authentication	
Today 11:09:01	SECURITY	NOTICE	roger	CRON[3209]:	Syslog	pam_unix(cron:account): account root has expired (account expired)	
Today 11:02:14	USER	NOTICE	roger	mpt-statusd:	Syslog	detected non-optimal RAID status	
Today 10:52:14	USER	NOTICE	roger	mpt-statusd:	Syslog	detected non-optimal RAID status	
Today 10:42:14	USER	NOTICE	roger	mpt-statusd:	Syslog	detected non-optimal RAID status	
Today 10:39:01	CRON	ERR	roger	CRON[3159]:	Syslog	Authentic d authentication	
Today 10:39:01	SECURITY	NOTICE	roger	CRON[3159]:	Syslog	pam_unix(cron:account): account root has expired (account expired)	
Today 10:35:35	DAEMON	ERR	roger	mysqld:	Syslog	150505 10:35:35 [Warning] Access denied for user 'root@localhost' (using pass ...	
Today 10:35:30	DAEMON	ERR	roger	mysqld:	Syslog	150505 10:35:30 [Warning] Access denied for user 'root@localhost' (using pass ...	
Today 10:35:26	DAEMON	ERR	roger	mysqld:	Syslog	150505 10:35:26 [Warning] Access denied for user 'root@localhost' (using pass ...	
Today 10:35:14	DAEMON	ERR	roger	mysqld:	Syslog	150505 10:35:14 [Warning] Access denied for user 'logalyzer@localhost' (usi ...	
Today 10:35:07	DAEMON	ERR	roger	mysqld:	Syslog	150505 10:35:07 [Warning] Access denied for user 'logalyzer@localhost' (usi ...	
Today 10:32:14	USER	NOTICE	roger	mpt-statusd:	Syslog	detected non-optimal RAID status	
Today 10:28:50	SECURITY	INFO	roger	login[2956]:	Syslog	pam_unix(login:session): session closed for user laurent	
Today 10:28:45	SECURITY	INFO	roger	sshd[3044]:	Syslog	pam_unix(sshd:session): session opened for user laurent by (uid=0)	
Today 10:28:45	AUTH	INFO	roger	sshd[3044]:	Syslog	Accepted password for laurent from 172.16.4.47 port 29950 ssh2	
Today 10:24:17	SECURITY	INFO	roger	sudo:	Syslog	pam_unix(sudo:session): session closed for user root	
Today 10:24:17	SECURITY	INFO	roger	sudo:	Syslog	pam_unix(sudo:session): session opened for user root by laurent(uid=0)	
Today 10:24:17	SECURITY	NOTICE	roger	sudo:	Syslog	laurent : TTY=tty1 : PWD=/home/laurent : USER=root : COMMAND=/sbin/ifconfig	
Today 10:24:02	SECURITY	INFO	roger	login[2956]:	Syslog	pam_unix(login:session): session opened for user laurent by LOGIN(uid=0)	
Today 10:23:53	SECURITY	NOTICE	roger	login[2956]:	Syslog	FAILED LOGIN (1) on '/dev/tty1' FOR 'laurent'. Authentication failure	
Today 10:23:50	SECURITY	NOTICE	roger	login[2956]:	Syslog	pam_unix(login:auth): authentication failure: logname=LOGIN uid=0 euid=0 tty=/dev/...	
Today 10:22:56	SECURITY	NOTICE	roger	login[2920]:	Syslog	FAILED LOGIN (2) on '/dev/tty1' FOR 'laurent'. Authentication failure	
Today 10:22:45	SECURITY	NOTICE	roger	login[2920]:	Syslog	FAILED LOGIN (1) on '/dev/tty1' FOR 'laurent'. Authentication failure	
Today 10:22:41	SYSLOG	INFO	roger	rsyslogd-2359:	Syslog	action 'action 1' resumed (module 'ommysql') [v8.8.0:ad1 by http://www.rsyslog...	
Today 10:22:41	SYSLOG	INFO	roger	rsyslogd-2359:	Syslog	action 'action 1' resumed (module 'ommysql') [v8.8.0:ad1 by http://www.rsyslog...	
Today 10:22:41	SECURITY	NOTICE	roger	login[2920]:	Syslog	pam_unix(login:auth): authentication failure: logname=LOGIN uid=0 euid=0 tty=/dev/...	
2015-04-10 12:54:21	DAEMON	ERR	roger	mysqld:	Syslog		
2015-04-10 12:54:21	DAEMON	ERR	roger	mysqld:	Syslog	150410 12:54:21 [Note] /usr/sbin/mysqld: Normal shutdown	
2015-04-10 12:54:20	SECURITY	INFO	roger	sudo:	Syslog	pam_unix(sudo:session): session closed for user root	
2015-04-10 12:54:20	DAEMON	INFO	roger	init:	Syslog	Switching to runlevel 0	
2015-04-10 12:54:20	USER	NOTICE	roger	shutdown[3189]:	Syslog	shutting down for system halt	
2015-04-10 12:54:20	SECURITY	INFO	roger	sudo:	Syslog	pam_unix(sudo:session): session opened for user root by laurent(uid=0)	
2015-04-10 12:54:20	SECURITY	INFO	roger	sudo:	Syslog	laurent : TTY=tty1 : PWD=/home/laurent : USER=root :	

From: <https://wiki.viper61.fr/> - Viper61's Wiki
Permanent link: https://wiki.viper61.fr/sio/ppe2_2/logalyzer
Last update: 18/09/2016 02:54