
Mise en place serveur rsyslog

Je sauvegarde mon ancien fichier `/etc/rsyslog.conf` en `/etc/rsyslog.conf.old`

Je fais en sorte que les services que je n'utilise pas comme `lpr` ne soit pas loguer car pas besoin, je met `lpr.none` au lieu de `lpr.*`

Ensuite je fais en sorte que pour le reste des services je n'ai que les messages « warning » et ce qui est supérieur

Pour ne plus voir les logs de « lpr » afficher il faut mettre « .none » dans les logs envoyer à syslog et dans les logs `lpr.log`

```
#
# First some standard log files.  Log by facility.
#
auth,authpriv.warning          /var/log/auth.log
*.warning;auth,authpriv.none;lpr.none_  -/var/log/syslog
#cron.*                        /var/log/cron.log
daemon.warning                 -/var/log/daemon.log
kern.warning                   -/var/log/kern.log
lpr.none                       -/var/log/lpr.log
mail.warning                   -/var/log/mail.log
user.warning                   -/var/log/user.log
```

Capture des logs apache dans un fichier personnalisé

Je dois aller dans le fichier de conf du virtual host

Je vais prendre celui par défaut

`/etc/apache2/sites-enabled/000-default.conf`

#Sa ne fonctionne pas pour enregistrer les logs dans un fichier précis j'ai saisis ceci

```
ErrorLog "|/usr/bin/logger/ -t apache -p local6.warn"
CustomLog "|/usr/bin/logger/ -t apache -p local6.warn" combined
```

Je l'ai enregistré en tant que `local6`

```
ErrorLog /var/log/syslog.log
CustomLog /var/log/syslog.log combined
```

Mise en place serveur de log

Sur le serveur :

Aller dans `/etc/rsyslog.conf`

Et décommenter ces deux lignes pour ouvrir le port 514 en udp pour que les logs des clients soient envoyés sur ce port

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
```

Sur le client :

Dans le fichier `rsyslog.conf`

```
*.* @172.17.1.40
```

Tous les logs sont envoyés vers le serveur log

Je redémarre le service sur le serveur et client

Mon client est mon serveur « `openvpn` »

```
Mar 16 10:21:00 OPENVPN rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2102.0]
Mar 16 10:21:00 OPENVPN rsyslogd: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="1237026" x-info="https://www.rsyslog.com"] start
Mar 16 10:21:38 OPENVPN rsyslogd: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="1237045" x-info="https://www.rsyslog.com"] exiting on
signal 15.
Mar 16 10:21:38 OPENVPN rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2102.0]
Mar 16 10:21:38 OPENVPN rsyslogd: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="1237054" x-info="https://www.rsyslog.com"] start
Mar 16 10:21:59 OPENVPN rsyslogd: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="1237054" x-info="https://www.rsyslog.com"] exiting on
signal 15.
Mar 16 10:22:00 OPENVPN rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2102.0]
Mar 16 10:22:00 OPENVPN rsyslogd: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="1237064" x-info="https://www.rsyslog.com"] start
Mar 16 10:24:48 nagios nagios4: HOST NOTIFICATION: nagiosadmin:winserver:DOWN:notify-host-by-email;CRITICAL - Host Unreachable (192.168.1.2)
Mar 16 10:27:02 nagios nagios4: HOST NOTIFICATION: nagiosadmin:linksys-sru224g:DOWN:notify-host-by-email;CRITICAL - Host Unreachable (192.168.1.253)
```

On voit bien que le serveur « OPENVPN » envoie ses logs à mon serveur de log

Log switch cisco

Il faut d'abord configurer la date

Passer en mode enable

Clock set <heure> :<minute> :<seconde> <mois> <jourDumois> <année>

```
routeurMaster#clock set 10:46:30 march 3 2022
routeurMaster#
```

Sur le routeur cisco les logs sont gérés selon leur gravité si je demande que ce soit le niveau 7 qui soit géré tout ce qui est en dessous du niveau 7 sera géré

Il faut saisir cette commande

Logging trap 7

Ensuite il faut que je définisse les services pour les logs quand ils seront envoyés vers le serveur par exemple

Logging facility <nomService >

```
routeurMaster(config)#logging facility auth
routeurMaster(config)#logging facility kern
routeurMaster(config)#logging facility user
routeurMaster(config)#logging facility on
^
```

Ensuite je définis l'adresse du serveur de log

Logging <Adrlp>

```
routeurMaster(config)#logging 172.17.1.40
routeurMaster(config)#
```

Pour vérifier si tout a été pris en compte je fais la commande : show logging

```
Persistent logging: disabled
Trap logging: level debugging, 40 message lines logged
Logging to 172.17.1.40 (udp port 514, audit disabled,
link up),
2 message lines logged,
0 message lines rate-limited,
```

On voit l'ip de mon serveur de log et on peut voir aussi que 2 logs ont été envoyés

Je vais vérifier sur mon serveur de log si les logs sont correctement reçus

```
Mar 16 10:53:44 172.17.1.50 39: Mar  3 10:54:59.667: %SYS-5-CONFIG_I: Configured from console by adel on vty0 (172.17.1.3)
Mar 16 10:53:45 nagios nagios4: Auto-save of retention data completed successfully.
Mar 16 10:53:45 172.17.1.50 40: Mar  3 10:55:00.667: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 172.17.1.40 port 514 started - CLI initiated
```

172.17.1.50 = IP de mon routeur actif

Client windows

Je vais installer l'agent windows rsyslog sur le site officiel de « rsyslog »

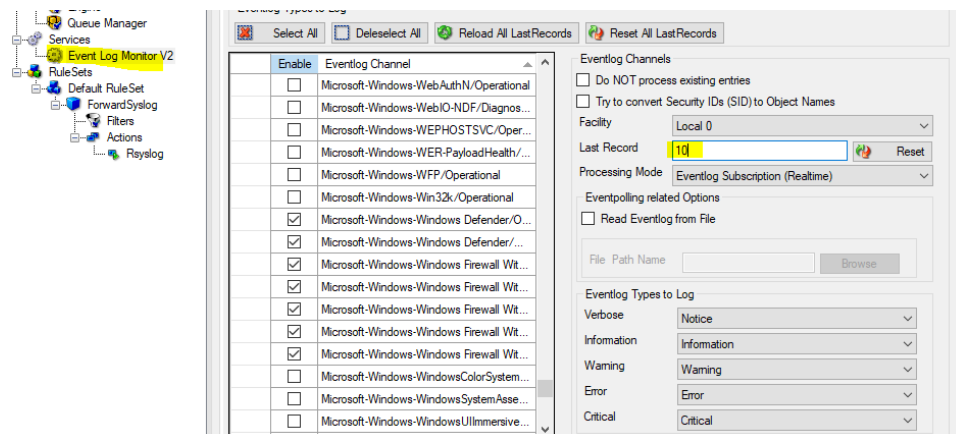
Se rendre dans Rule Set ensuite Rsyslog

Puis préciser qu'on veut comme protocole de transport UDP, IP du serveur

Ne pas oublier d'enregistrer les modifications

Ensuite se rendre dans Event Log Monitor V2

Tout décocher et cocher que ce qu'on veut enregistrer et envoyer comme log à droite on peut choisir combien de log maximum on veut, j'ai configuré pour les 10 derniers logs



Ensuite enregistrer et démarrer

Le résultat :

```
Dec  9 08:46:29 A_SADEK.booktic.info EvntSLog Une interface de transport TCP/IP a été ajoutée. Nom: Connexion au réseau local Index d'interface: 0x29 Aide: Une liaison TCP/IP a été ajoutée à la carte réseau spécifiée pour le client SMB. Le client SMB peut maintenant envoyer et recevoir le trafic SMB sur cette carte réseau via TCP/IP. Attendez-vous à cet événement lors du redémarrage d'un ordinateur ou lorsqu'une carte réseau précédemment désactivée est réactivée. Aucune action de l'utilisateur n'est requise.  
root@nagios:/etc#
```

Les logs sont bien envoyés

Log snort

Envoyer les logs vers un serveur rsyslog

Il faut d'abord envoyer les logs snort vers un « local » ce « local » permet de rajouter des « cases de surveillance » à rsyslog

Cela se fait dans le fichier de configuration « snort.conf »

```
output alert_syslog: LOG_LOCAL5 LOG_ALERT
```

Ceci c'est pour que toutes les alertes soient envoyées

Ensuite dans le fichier rsyslog.conf sur le client

```
local5.* @192.168.1.137  
*.* @192.168.1.137
```

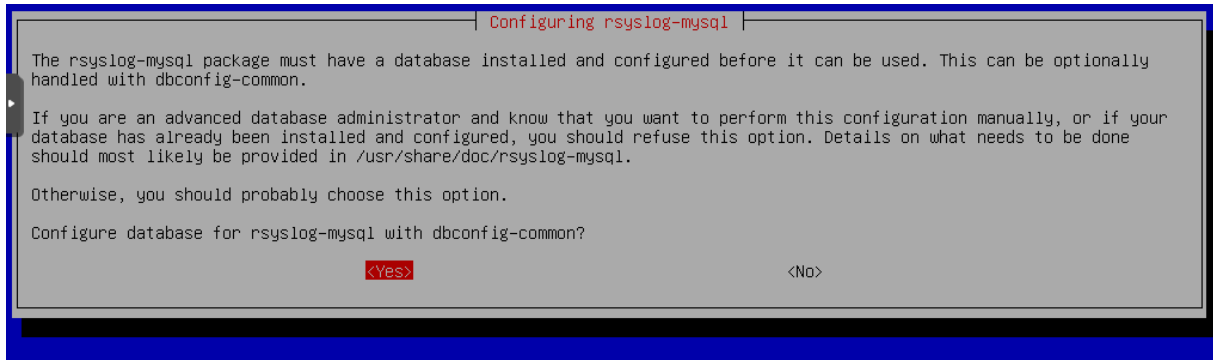
Le résultat sur le serveur :

```
Jun 12 22:29:32 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 51.222.153.159 -> 15.235.39.200  
Jun 12 22:29:32 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 167.114.37.1 -> 15.235.39.200  
Jun 12 22:29:32 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 51.222.153.159 -> 15.235.39.200  
Jun 12 22:29:33 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 92.222.186.1 -> 51.222.153.159  
Jun 12 22:29:33 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 167.114.37.1 -> 51.222.153.159  
Jun 12 22:29:33 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 92.222.186.1 -> 51.222.153.159  
Jun 12 22:29:33 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 167.114.37.1 -> 51.222.153.159  
Jun 12 22:29:34 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 139.99.1.148 -> 15.235.39.200  
Jun 12 22:29:34 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 51.222.153.159 -> 15.235.39.200  
Jun 12 22:29:34 snort snort[11359]: [1:1:1] ALERTE ICMP {ICMP} 139.99.1.148 -> 51.222.153.159
```

Interface web pour rsyslog et envoie de log dans une base de données

D'abord je vais installer un paquet pour envoyer les logs « rsyslog » vers une base de données mysql

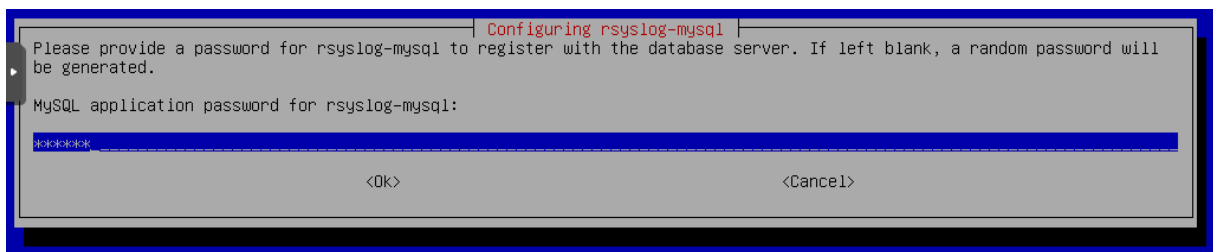
apt-get install rsyslog-mysql -y



Laissez le dbconfig-common configurer automatiquement la base de données en répondant "OUI" :

Le dbconfig-common va alors créer une base de données appelée "Syslog" et les deux tables dont nous aurons besoin : "SystemEvents" et "SystemEventsProperties". Attention à bien respecter la casse de ces noms par la suite !

Définissez un mot de passe pour l'utilisateur nommé "rsyslog" qui aura le contrôle total de la base de données Syslog :



La base de données est prête. Voici les informations importantes à retenir :

Hôte Database : localhost

Port Database : 3306

Nom Database : Syslog

Table Événements : SystemEvents

User Database : rsyslog

Mdp User Database : mdp que vous avez défini

On voit bien que la base a été créée

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| Syslog   |
| information_schema |
| mysql    |
| performance_schema |
+-----+
```

Rajouter ceci dans le fichier /etc/rsyslog

Pour que tout les logs soient envoyées vers notre base de données

```
*.* :ommysql:localhost,Syslog,rsyslog,mdp_user_rsyslog
```

Je redemarre « rsyslog »

Je vais dans ma base de données dans la table SystemEvents je trouve ceci

```
L | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL
]: | NULL | NULL | NULL | NULL | NULL | NULL | 1 | snort[11359
| 1832 | NULL | 2022-06-13 15:07:37 | 2022-06-13 15:07:37 | 21 |
1 | snort | [1:1:1] ALERTE ICMP {ICMP} 139.99.1.148 -> 51.222.153.159

L | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL
]: | NULL | NULL | NULL | NULL | NULL | NULL | 1 | snort[11359
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
1832 rows in set (0.002 sec)
MariaDB [Syslog]> █
```

Maintenant passons à l'installation de log analyzer

Je me rends dans le dossier /var/www/html

Et télécharge l'archive puis la décompresse

```
wget http://download.adiscon.com/loganalyzer/loganalyzer-4.1.8.tar.gz
```

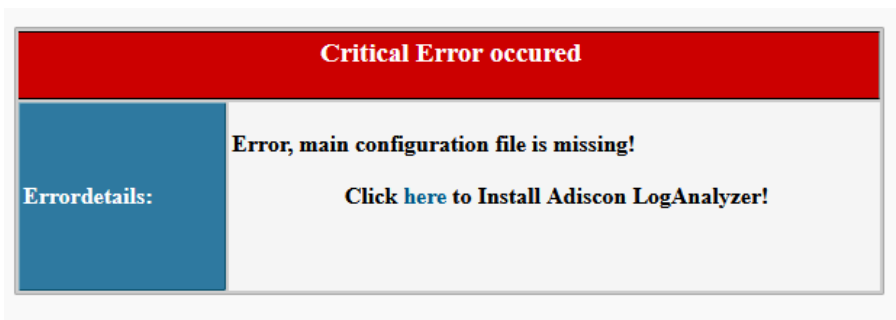
Il y'a un repertoire « src » qui a été décompresser il faut que je prenne son contenu et que le mette dans « /var/www/html »

```
cp -r /var/www/html/loganalyzer/src/* /var/www/html/
```

Ensuite j'attribue la propriété des fichier et répertoires décompresser à l'user « www-data »

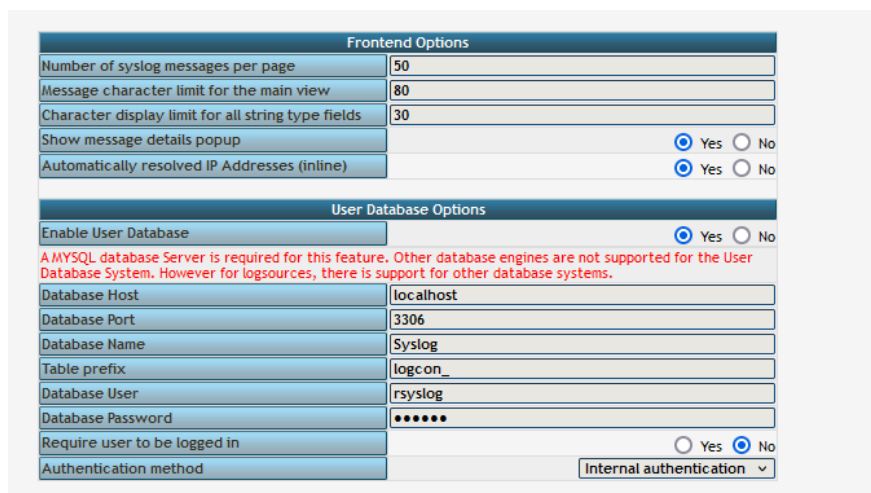
```
chown -R www-data:www-data /var/www/html/loganalyzer
```

Ensuite ce message d'erreur apparait il faut que je clique sur « here » pour lancer l'install



Ensuite il y'a plusieurs vérifications ou je dois appuyer sur « next » c'est pour vérifier que tel et tel fichier sont accessible en écriture et d'autres choses similaires

Ensuite je renseigne les infos de connexion à la base de données



The image shows two configuration screens. The first is titled "Frontend Options" and includes fields for "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" (radio buttons for Yes/No), and "Automatically resolved IP Addresses (inline)" (radio buttons for Yes/No). The second screen is titled "User Database Options" and includes a red warning: "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." Below this are fields for "Database Host" (localhost), "Database Port" (3306), "Database Name" (Syslog), "Table prefix" (logcon_), "Database User" (rsyslog), "Database Password" (masked with dots), "Require user to be logged in" (radio buttons for Yes/No), and "Authentication method" (Internal authentication dropdown).

Ne pas oublier de modifier le nom de la base de données

Et installer le paquet « php-mysql »

Ensuite il faut que je définisse une source je définis son nom et je précise que sa vient d'une base de données MYSQL

Je définis le nom de la base de données

First Syslog Source	
Name of the Source	My Syslog Source
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 type="radio"/> Yes <input checked="" type="radio"/> No

Erreur rencontrer



Si cette erreur apparait c'est juste la syntax du nom de la base de données qui pose problème

Il faut modifier le fichier « config.php » comme ceci et remettre les majuscules correctement

```
$CFG['Sources']['Source1']['DBTableName'] = 'SystemEvents';  
$CFG['Sources']['Source1']['DBEnableRowCounting'] = false;
```

Le résultat

Date	Facility	Severity	Host	Syslogtag	ProcessID	Message type	Message
Today 16:57:08	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 51.222.153.159 (ns576493.ip-51-222-153.net) -> 15.235.39.200 (ip200.ip-15-235-39.net)
Today 16:57:08	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 167.114.37.1 (netmon-icmp-bhs-1.monitoring.ovh.net) -> 15.235.39.200 (ip200.ip-15-235-39.net)
Today 16:57:08	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 51.222.153.159 (ns576493.ip-51-222-153.net) -> 15.235.39.200 (ip200.ip-15-235-39.net)
Today 16:57:08	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 139.99.1.148 (netmon-icmp-sgp-1.monitoring.ovh.net) -> 15.235.39.200 (ip200.ip-15-235-39.net)
Today 16:57:08	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 51.222.153.159 (ns576493.ip-51-222-153.net) -> 15.235.39.200 (ip200.ip-15-235-39.net)
Today 16:57:08	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 167.114.37.1 (netmon-icmp-bhs-1.monitoring.ovh.net) -> 15.235.39.200 (ip200.ip-15-235-39.net)
Today 16:57:08	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 51.222.153.159 (ns576493.ip-51-222-153.net) -> 15.235.39.200 (ip200.ip-15-235-39.net)
Today 16:57:08	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 139.99.1.148 (netmon-icmp-sgp-1.monitoring.ovh.net) -> 15.235.39.200 (ip200.ip-15-235-39.net)
Today 16:57:07	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 167.114.37.1 (netmon-icmp-bhs-1.monitoring.ovh.net) -> 51.222.153.159 (ns576493.ip-51-222-153.net)
Today 16:57:07	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 51.255.169.177 (bijonat.com) -> 51.222.153.159 (ns576493.ip-51-222-153.net)
Today 16:57:07	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 167.114.37.1 (netmon-icmp-bhs-1.monitoring.ovh.net) -> 51.222.153.159 (ns576493.ip-51-222-153.net)
Today 16:57:07	LOCAL5	ALERT	snort	snort[11359]:		Syslog	[1:1:1] ALERTE ICMP (ICMP) 51.255.169.177 (bijonat.com) -> 51.222.153.159 (ns576493.ip-51-222-153.net)