

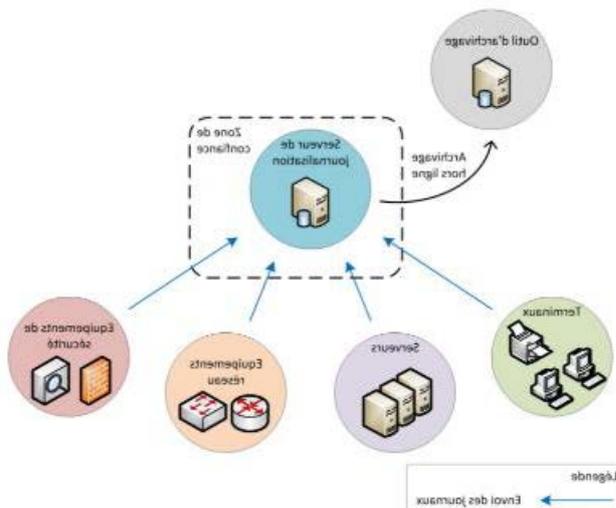
## Rsyslog / Logalyzer

Définir le rôle des fichiers de journaux.

En informatique, le concept de sauvegarder les événements de journalisation c'est chaque jour tout est enregistré, on appelle ça l'enregistrement séquentiel dans un fichier ou dans une base de données, mais ça enregistre plus particulièrement les actions, l'activité dans un réseau informatique.

Définir le rôle d'un serveur syslog

Un serveur de log nous permet de récupérer des informations coté client :



Comme le montre cette image, les clients renvoient leurs données (ex : de connexion utilisateur) le message et envoient sur le serveur qui les reçoit et il les stocke dans son système ou dans une base de données (à configurer) c'est log vas nous permet de savoir par exemple qui c'est connecter sur le pare-feu, à quelle heure, et quand il se déconnecte, mais il ne fait pas que ça, nous pouvons recevoir aussi les erreurs système et bien d'autres. Tous ces logs transitent en UDP ou TCP, l'UDP n'est pas protégé nous pouvons les intercepter et les lire, TCP lui est protégé donc nous ne pouvons pas les lire.

Quel protocole réseau est utilisé par syslog par défaut ?

Le protocole utilisé est le TCP ou l'UDP et il écoute sur le port 514.

Définir, dans le contexte de syslog les termes : périphérique, relais, collecteur.

- Périphérique : est une machine ou une application qui génère des messages Syslog.
- Relais : est une machine ou une application qui reçoit des messages Syslog et les retransmet à une autre machine.
- Collecteur : est une machine ou une application qui reçoit des messages Syslog, mais qui ne les retransmet pas.

Définir, dans le contexte de syslog les termes : origine, priorité.

- Origine : origine sont des messages, dont des codes qui sont regroupés par des types qui sont appelés des "facilités", soit d'origine de local0 jusqu'à local17 bien évidemment personnalisable

- Priorité : La priorité d'un message Syslog est définie par sa fonctionnalité et sa sévérité. Cette priorité est le résultat d'une multiplication de la fonctionnalité et elle est multipliée par 8 sur laquelle s'ajoute la sévérité.

Numéro de fonctionnalité	Usage
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0
17	local use 1
18	local use 2
19	local use 3
20	local use 4
21	local use 5
22	local use 6
23	local use 7

Expliciter le fonctionnement d'un serveur syslog.

Un serveur de logs reçoit des journaux des utilisateurs dans un réseau, c'est à dire qu'un utilisateur ou une machine configure de manière à envoyer des rapports en TCP ou UDP sur des points précis (Erreur Critique system) par exemple, si l'utilisateur nous informe que son ordinateur ne fonctionne plus, nous pouvons vérifier dans les logs si une erreur a été envoyée. Ce qui permet aussi de superviser les systèmes d'une manière très brève. Faire attention la sécurité avant tout, il faut bien choisir son protocole soit UDP soit TCP sécuriser ou pas sécuriser.

## Installation et configuration du service

Utilisation de Rsyslog : Dans le cadre de ce TP j'utilise une machine nommer Lamp2 / BBD / logs.

Rsyslog est déjà installer sur la machine.

Configuration du serveur syslog :

Editer le fichier rsyslog.conf

**Nano /etc/rsyslog.conf**

```
GNU nano 3.2 /etc/rsyslog.conf
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

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

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

#####
#### GLOBAL DIRECTIVES ####
#####

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
[ Lecture de 94 lignes ]
␣ Aide ␣ Écrire ␣ Chercher ␣ Couper ␣ Justifier ␣ Pos. cur. ␣ Annuler
```

Décommenter les # sur les lignes en jaune (c'est pour que le serveur de log puisse écouter sur le port UDP 514). Save la conf.

Faire un test pour savoir si le port UDP et ouvert :

**Netstat -nul**

```
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat
udp 0 0 0.0.0.0:514 0.0.0.0:*
```

Nous retournons dans le fichier rsyslog.conf, se rendre dans la partie RULES, ajouter cette ligne,

**Auth,authpriv.\* @192.168.200.240**

Cette ligne là nous informe que nous envoyons dur le serveur de logs les messages Auth en UDP car nous avons utilisé qu'un @suivie de l'IP, si nous voulons utiliser le TCP il faut utiliser 2 @@suivie de le l'IP

Quelques notions à savoir :

Les **facilites** sont des catégories dans lesquelles les logs vont se "ranger" afin de mieux les archiver et les trier

- **auth** : Utilisé pour des évènements concernant la sécurité ou l'authentification à travers des applications d'accès (type SSH)
- **authpriv** : Utilisé pour les messages relatifs au contrôle d'accès
- **daemon** : Utilisé par les différents processus systèmes et d'application
- **kern** : Utilisé pour les messages concernant le kernel
- **mail** : Utilisé pour les évènements des services mail
- **user** : Facilitie par défaut quand aucune n'est spécifiée
- **local7** : Utilisé pour les messages du boot
- **none** : Ne désigne aucune facilites

En plus de ces facilites, nous retrouvons pour chaque facilities un niveau de gravité (appelé **Priorité**) qui va du plus grave à la simple information :

- **Emerg** : Urgence, système inutilisable
- **Alert** : Alerte. Intervention immédiate nécessaire
- **Crit** : Erreur système critique
- **Err** : Erreur de fonctionnement
- **Warning** : Avertissement
- **Notice** : Évènements normaux devant être signalé
- **Info** : Pour information
- **Debug** : Message de debogage

Test :

**Tail -f /var/log/auth.log**

Effectué plusieurs authentifications avec un faux utilisateur et on peut voir qu'il y a plusieurs FAILED LOGIN, donc on peut voir que les logs fonctionnent bien.

Installation de LogAnalyzer.

Installer Rsyslog-mysql, ce paquet nous permettra de nous connecter à la base de données MySQL.

Pour le configurer il faudra aller dans ce fichier :

`/etc/rsyslog.d/mysql.conf`

```
module (load="ommysql")
*. * action(type="ommysql" server="localhost" db="Syslog" uid="rsyslog" pwd="Password_BDD")
```

Il doit ressembler à ceci.

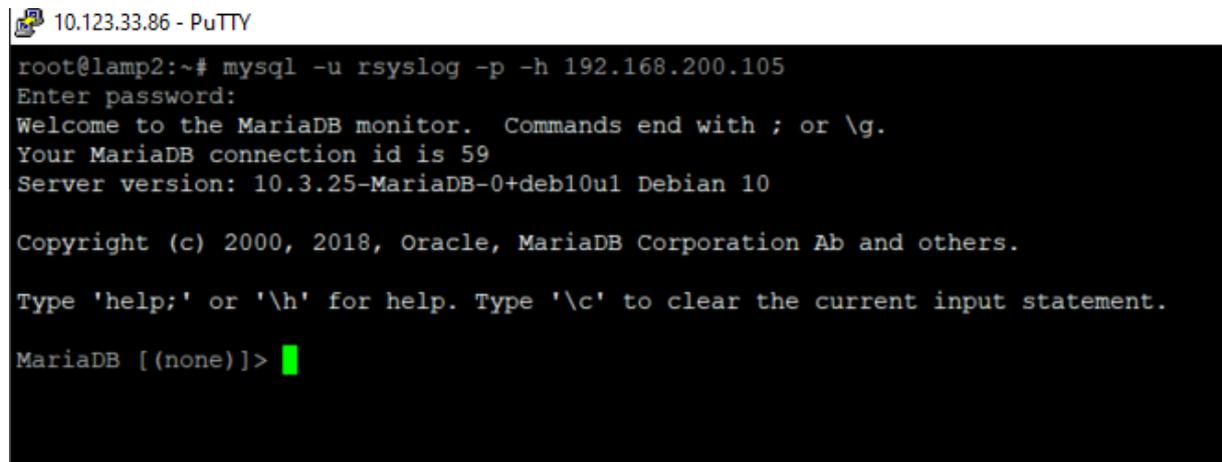
Sur le Serveur de base de données, vous devez créer un utilisateur et une base, l'utilisateur doit s'appeler par convention de nom rsyslog, cet utilisateur doit pouvoir se connecter à distance donc il faut ouvrir le port Mysql 3306 pour que la liaison se face. Editer le fichier /etc/mysql/mariadb.conf.d/50-server.cnf

Dans le fichier vous devrez trouver le Bind-address, là ou-il faut indiquer l'IP de notre server de BDD.

```
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 192.168.1.17
```

Redémarrer votre service Mysql, pour que les modifications soit prise en compte.

Test de connexion sur le serveur LAP pour se connecter au serveur de BDD. -h pour haute distant donc le serveur BDD.



```
10.123.33.86 - PuTTY
root@lamp2:~# mysql -u rsyslog -p -h 192.168.200.105
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 59
Server version: 10.3.25-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Créer une base de données Syslog, pour ce faire, voici la base de données en ligne de commande :

```
CREATE DATABASE Syslog;

USE Syslog;

CREATE TABLE SystemEvents
(
  ID int unsigned not null auto_increment primary key,
  CustomerID bigint,
  ReceivedAt datetime NULL,
  DeviceReportedTime datetime NULL,
  Facility smallint NULL,
  Priority smallint NULL,
  FromHost varchar(60) NULL,
  Message text,
  NTSeverity int NULL,
```

Importance int NULL,  
EventSource varchar(60),  
EventUser varchar(60) NULL,  
EventCategory int NULL,  
EventID int NULL,  
EventBinaryData text NULL,  
MaxAvailable int NULL,  
CurrUsage int NULL,  
MinUsage int NULL,  
MaxUsage int NULL,  
InfoUnitID int NULL ,  
SysLogTag varchar(60),  
EventLogType varchar(60),  
GenericFileName VarChar(60),  
SystemID int NULL

);

CREATE TABLE SystemEventsProperties

(

ID int unsigned not null auto\_increment primary key,

SystemEventID int NULL ,

ParamName varchar(255) NULL ,

ParamValue text NULL

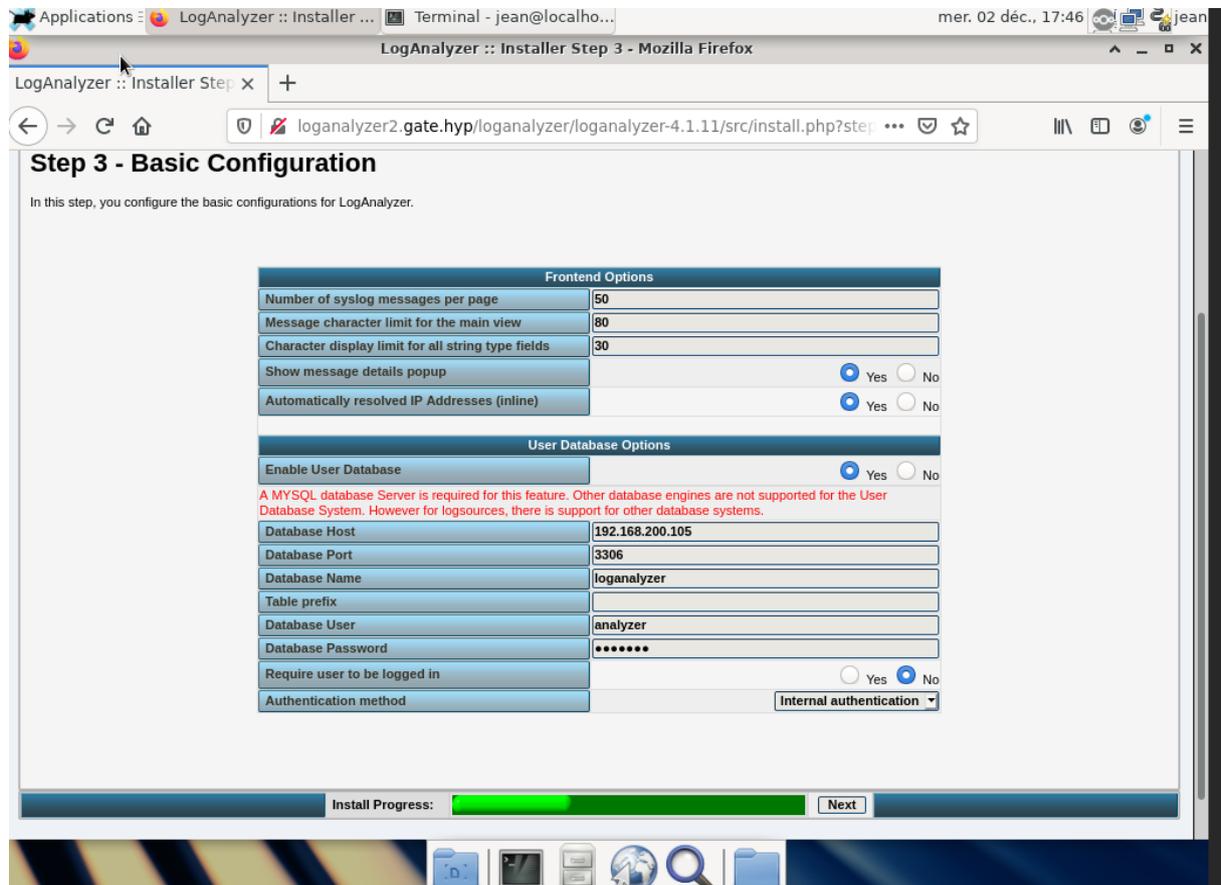
);

Ajouter l'utilisateur rsyslog a la base de données.

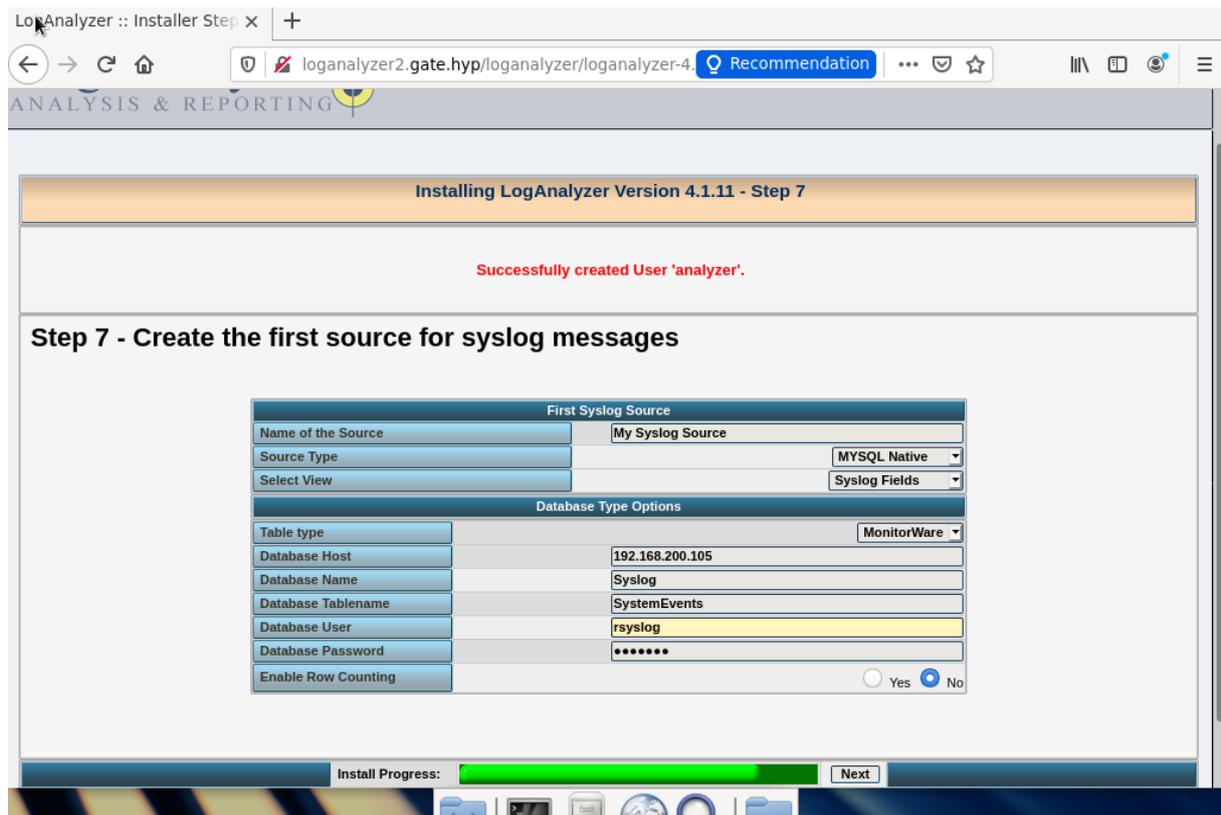
Installer loganalyzer :

Pour ce faire nous avons au préalable créer un vhost.

Lien de téléchargement de loganalyzer : <http://download.adiscon.com/loganalyzer/loganalyzer-4.1.11.tar.gz>



Nous nous retrouvons sur cette page pour renseigner les informations de connexions de la base de données Loganalyzer, cette base et l'endroit où loganalyzer pourra s'installer. Donc nous activons 'Enable user databases'. Il faut renseigner l'IP du serveur de base de données, le port, et le nom de la base, ATTENTION, il faut créer la base loganalyzer sur le serveur de BDD avant de continuer. Une fois fait, il faut créer un utilisateur analyzer qui a les droits sur la base loganalyzer. Renseigner c'est l'information pour se connecter.



Dans source Type, sélectionner MYSQL Native, pour pouvoir connecter la base Syslog.

Sur cette page il nous demande de connecter la base Syslog, il faut renseigner l'IP, le nom de la BDD, le nom de la tables SystemEvents ATTENTION logalyzer et soumis à la cast faite bien attention. Identifier l'utilisateur de la base Syslog et le mdp.

The screenshot shows the LogAnalyzer web interface. At the top, there's a navigation bar with tabs for Search, Show Events, Statistics, Reports, Help, Search in Knowledge Base, Login, and Maximize View. Below this is a search filter and an advanced search section. The main content area displays a table titled "Recent syslog messages".

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 15:39:01	SECURITY	INFO	lamp2	CRON[871]:		Syslog	pam_unix(cron:session): session opened for user root by (uid=0)
Today 16:09:01	SECURITY	INFO	lamp2	CRON[927]:		Syslog	pam_unix(cron:session): session closed for user root
Today 16:09:01	SECURITY	INFO	lamp2	CRON[927]:		Syslog	pam_unix(cron:session): session opened for user root by (uid=0)
Today 16:17:01	SECURITY	INFO	Logs	CRON[1831]:		Syslog	pam_unix(cron:session): session closed for user root
Today 16:17:01	SECURITY	INFO	Logs	CRON[1831]:		Syslog	pam_unix(cron:session): session opened for user root by (uid=0)
Today 16:17:01	SECURITY	INFO	lamp2	CRON[979]:		Syslog	pam_unix(cron:session): session closed for user root
Today 16:17:01	SECURITY	INFO	lamp2	CRON[979]:		Syslog	pam_unix(cron:session): session opened for user root by (uid=0)
Today 16:39:01	SECURITY	INFO	lamp2	CRON[986]:		Syslog	pam_unix(cron:session): session closed for user root
Today 16:39:01	SECURITY	INFO	lamp2	CRON[986]:		Syslog	pam_unix(cron:session): session opened for user root by (uid=0)
Today 17:06:06	SECURITY	INFO	lamp2	systemd:		Syslog	pam_unix(systemd-user:session): session opened for user root by (uid=0)
Today 17:06:06	AUTH	INFO	lamp2	systemd-logind[337]:		Syslog	New session 13 of user root.
Today 17:06:06	SECURITY	INFO	lamp2	login[386]:		Syslog	pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Today 17:06:07	SECURITY	NOTICE	lamp2	login[1060]:		Syslog	ROOT LOGIN on 'dev/tty1'

Voici la page de configuration des logs et nous retrouvons les logs auth que nous avons configuré sur le serveur lamp.