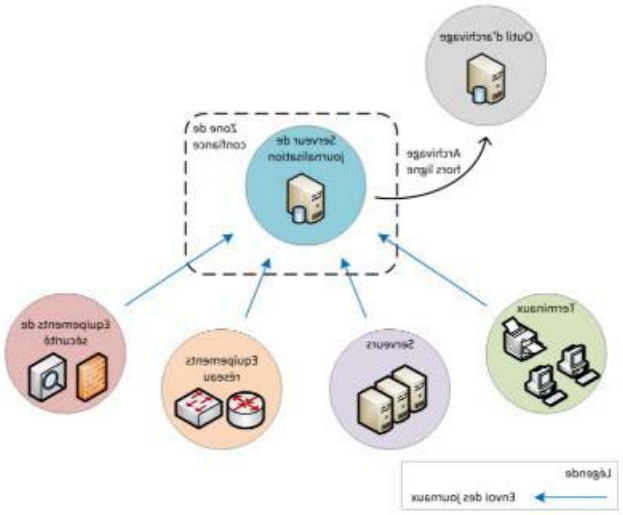
Rsyslog / Loganalyzer

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 renvoie leurs donnée (ex : de connexion utilisateur) le message et envoyer sur le serveur qui les reçoit et il les stocks 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 ces déconnecter, mais il ne fait pas que ça, nous pouvons recevoir aussi les erreurs système et bien d'autre. Tous ces logs transitent en UDP ou TCP, l'UDP est pas protéger nous pouvons les intercepter et les lire, TCP luis est protéger donc nous ne pouvons pas les lire.

Quel protocole réseau est utilisé par syslog par défaut ?
Le protocole utiliser et 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.

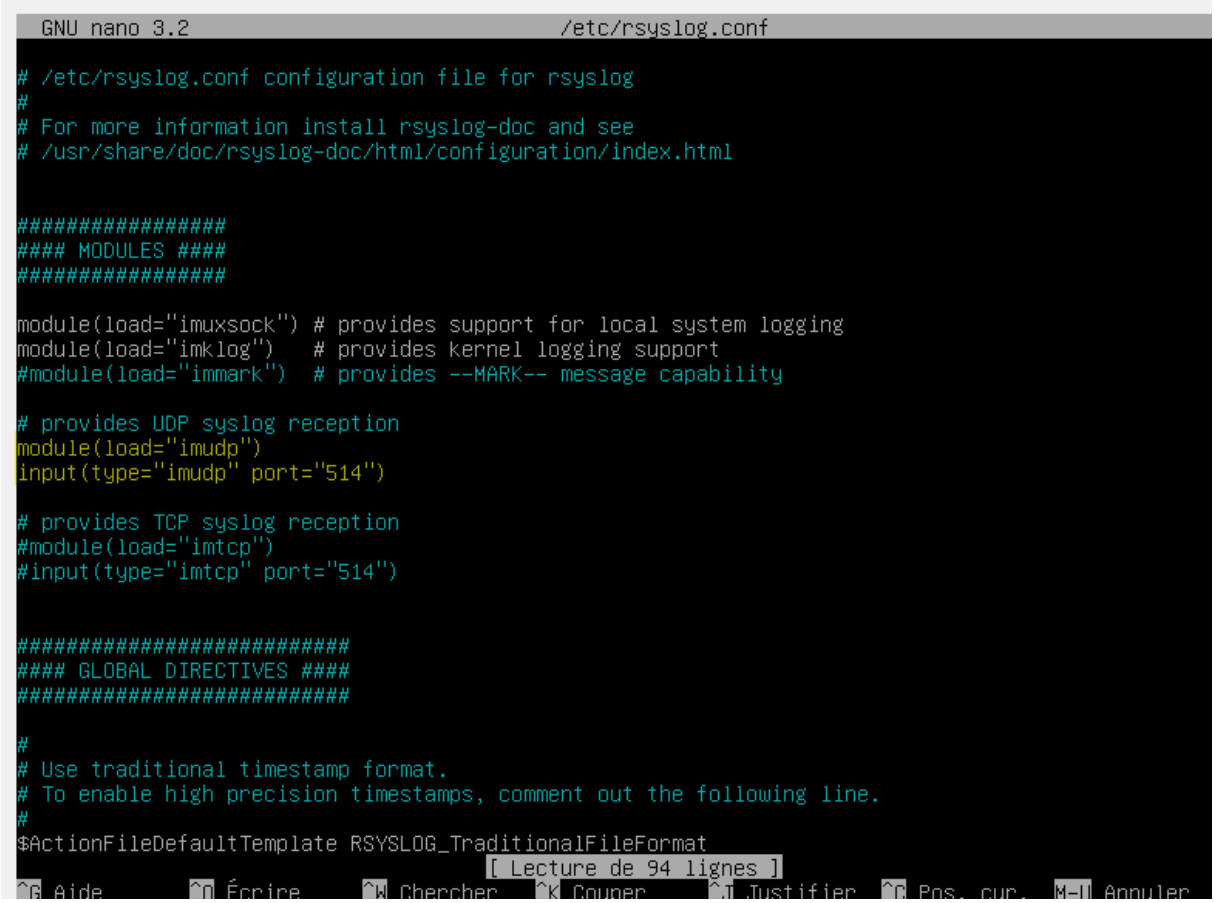
Définir, dans le contexte de syslog les termes : origine, priorité.
- Origine : origine sont des messages, dont des codes qui sont regroupés par des types qui sont appeler des "facilités", soit d'origine de loca10 jusqu'à loca17 bien évidement personnalisable
- Priorité : La priorité d'un message Syslog est définie par sa fonctionnalité et sa sévérité. Cette priorité et du au résultat d'une multiplication de la fonctionnalité et elle est multiplier par 8 sur les quelle 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 utilisateur on une machine configurer 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 envoyer. Se qui permet aussi de superviser les systèmes d'une manière très bref. Faire attention la sécurité avant tout, il faut bien choisir son protocole soit UDP soit TCP sécuriser ou pas sécuriser.

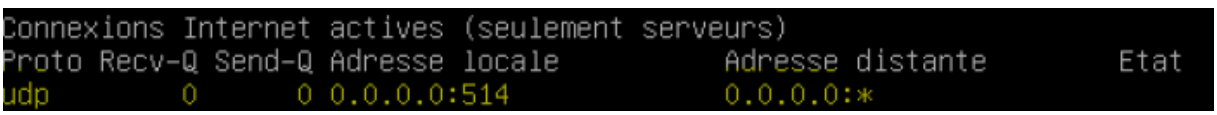
Installation et configuration du service

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



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



Nous retournons dans le fichier rsyslog.con, 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 donné 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.

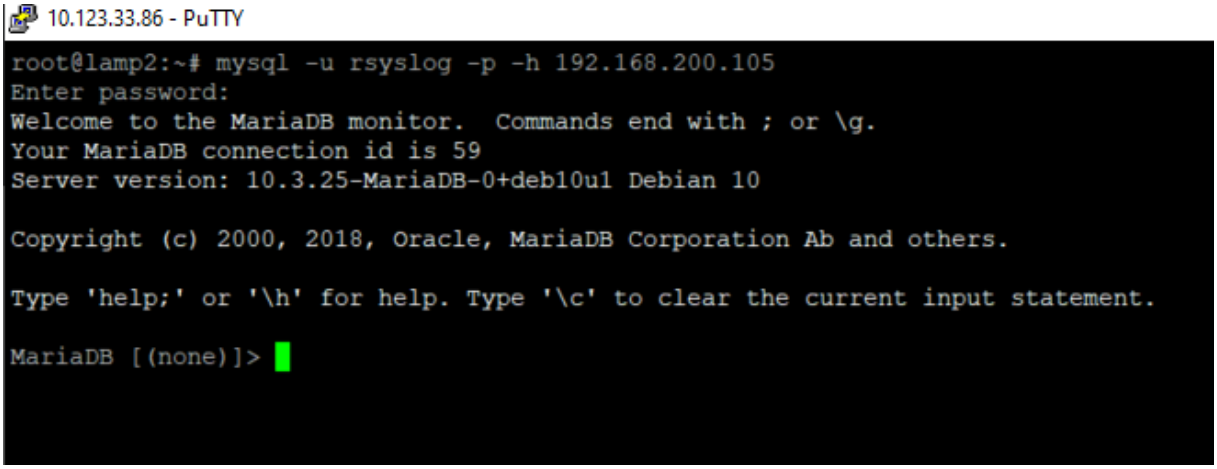
Sur le Serveur de base de données, vous devez créer un utilisateur et une base, l'utilisateur doit s'appeler par convention de nom rsyslog, cet utilisateur doit pouvoir se connecter à distance donc il faut ouvrir le port Mysql 3306 pour que la liaison se face. Editer le fichier /etc/mysql/mariadb.conf.d/50-server.cnf

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.



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

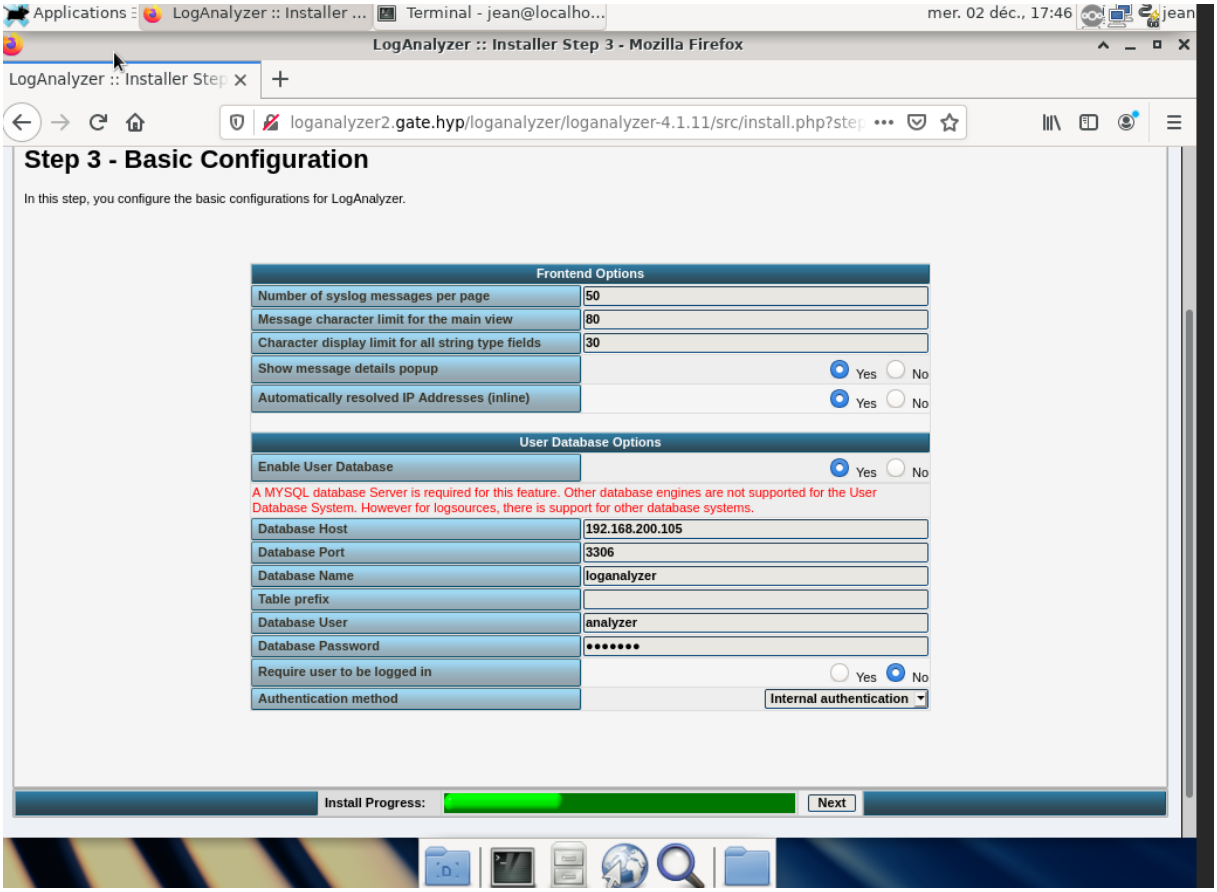
);

Ajouter l'utilisateur rsyslog a la base de données.

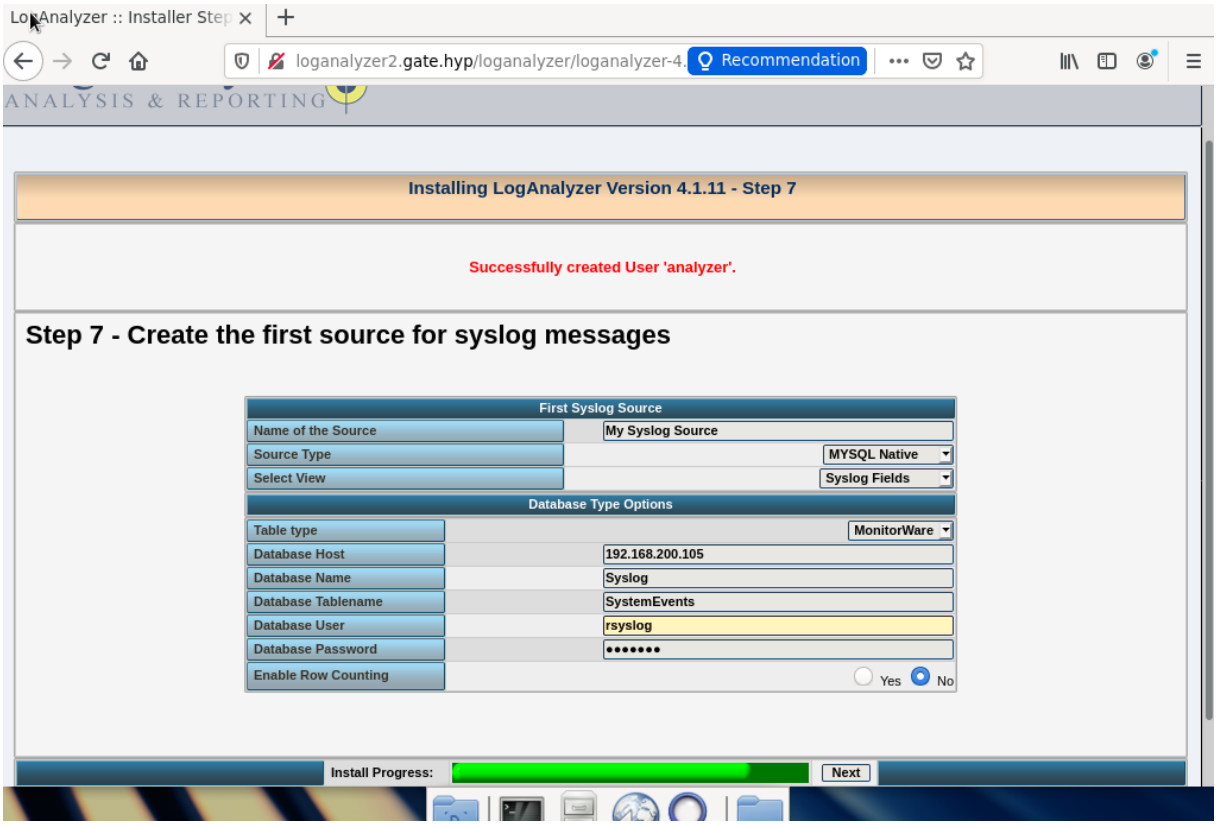
Installer loganalyzer :

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

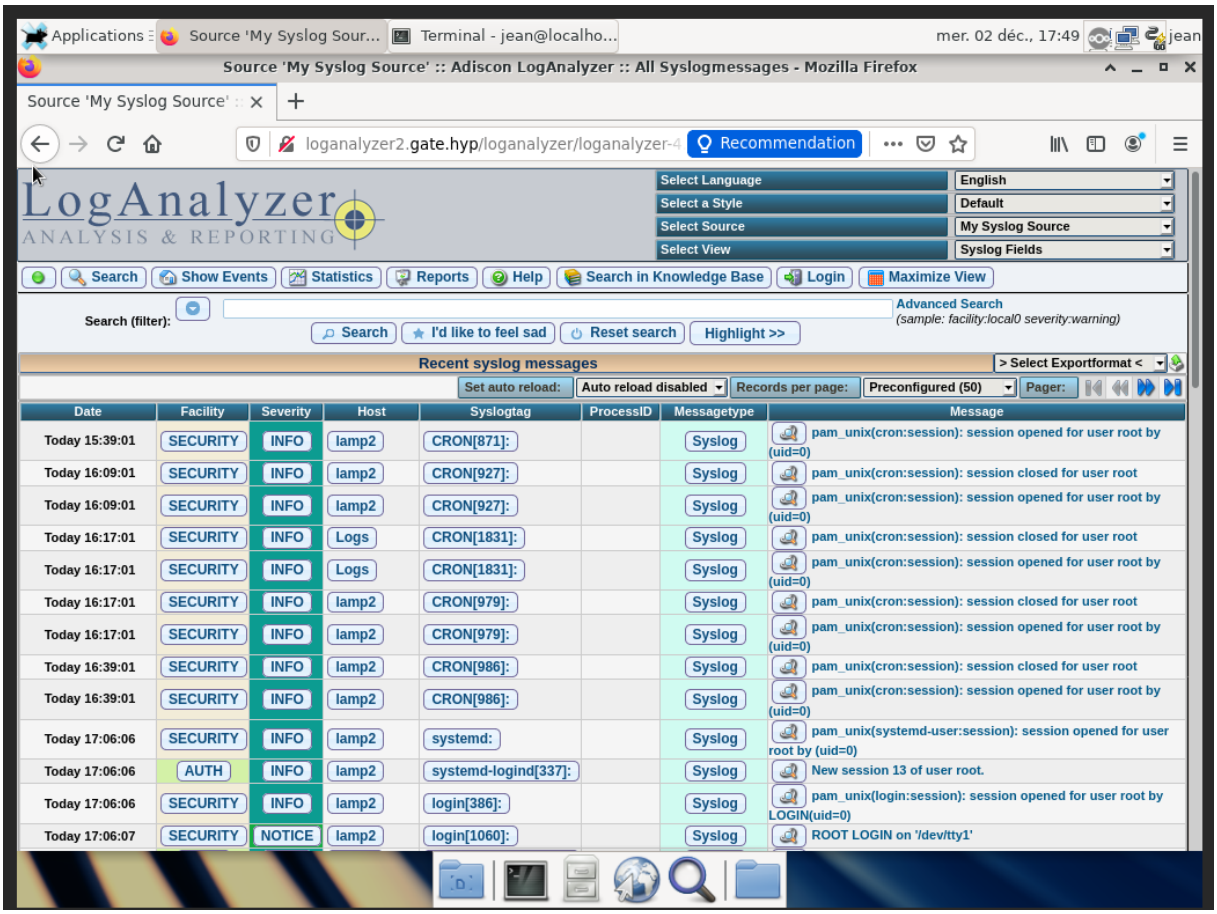


Nous nous retrouvons sur cette page pour renseigner les informations de connections de la base de données Loganalyzer, cette base et l'endroit ou loganalyzer pourra s'installer. Donc nous activons Enable user databases. Il faut renseigner l'IP du serveur de base de données, le port, et le nom de la base, 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 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 loganalyzer et soumis à la cast faite bien attention. Identifier l'utilisateur de la base Syslog et le mdp.



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