Rsyslog et Loganalyzer

Mise en Place de LOGANALYZER

apt update && apt upgrade

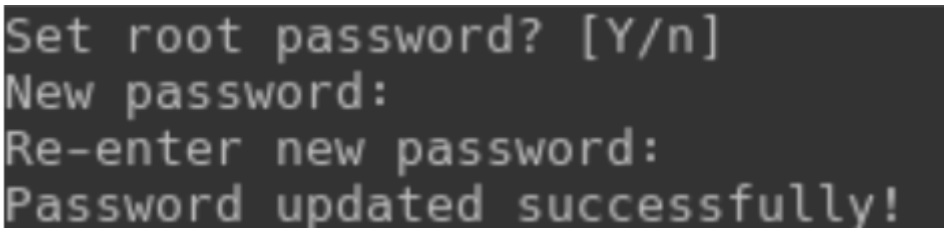
Ensuite, installez les services de base d'une pile « LAMP » (Linux Apache Mysql ou MariaDB PHP) et les modules de PHP nécessaires au bon fonctionnement de l'interface web Loganalyzer :

apt install apache2 mariadb-server php php-mysql php-gd

Sécurisez l'installation de mysql (mariadb) en définissant au compte root un mot de passe.

mysql_secure_installation

Ensuite on vous demande « Set root password ? [Y/n] ». Appuyez de nouveau sur la touche Entrée pour répondre « Oui » (Y = Yes) et définir un mot de passe pour l'utilisateur root (2 fois).

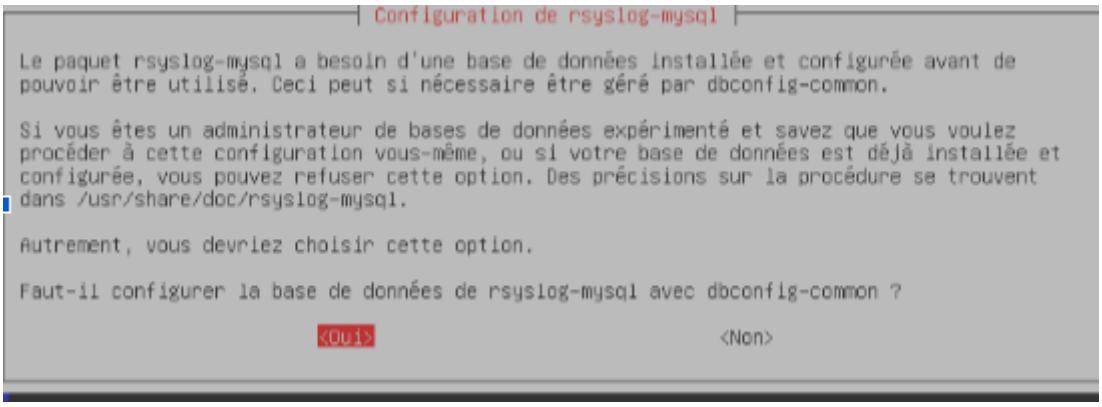


Password : Caribou

Pour toutes les questions qui suivront, appuyez sur Entrée pour valider.

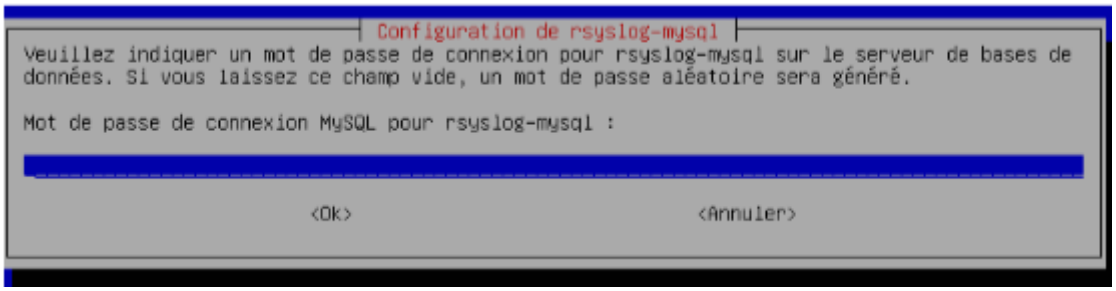
On termine la phase d'installation des services par le module mysql de rsyslog car nous allons héberger les journaux d'événements en base de données :

apt install rsyslog-mysql



Le dbconfig-common va alors s'occuper de créer une base de données appelée « Syslog » dont l'utilisateur « rsyslog » recevra les permissions adéquates pour interagir avec cette base.

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



Password : rsyslog

Poursuivons en activant la réception des logs sur le serveur dédié. Modifiez le fichier de configuration de rsyslog :

```
nano /etc/rsyslog.conf
```

A la fin de ce même fichier, ajoutez la ligne suivante pour envoyer les logs directement à la base de données en renseignant le password que vous avez défini à l'utilisateur rsyslog à la place de « mdp user rsyslog » :

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

Redémarrez le service rsyslog.

systemctl restart rsyslog

C'est tout pour la configuration de Rsyslog ! Passons maintenant à LogAnalyzer.

Placez vous dans le répertoire de votre choix, pour moi ça sera /tmp, et téléchargez la dernière version stable de LogAnalyzer.

```
cd /tmp
wget
http://download.adiscon.com/loganalyzer/loganalyzer-
4.1.13.tar.gz
```

Une fois le téléchargement terminé, **décompressez les fichiers** :

```
tar -zxvf /tmp/loganalyzer-4.1.13.tar.gz
```

D'abord sortez du répertoire : cd .., **puis créez un répertoire loganalyzer »** à la racine du serveur web.

```
mkdir /var/www/html/loganalyzer
```

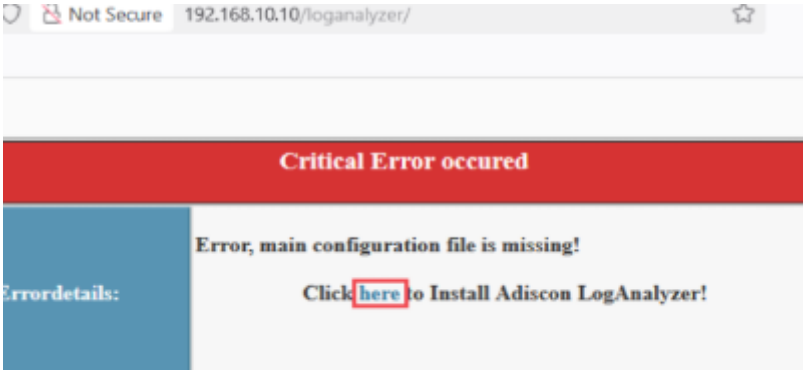
Copiez les fichiers requis dans ce nouveau répertoire :

```
cp -a /tmp/loganalyzer-4.1.13/src/*
/var/www/html/loganalyzer
```

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

Teste :

http://IP-serveur-syslog/loganayzer

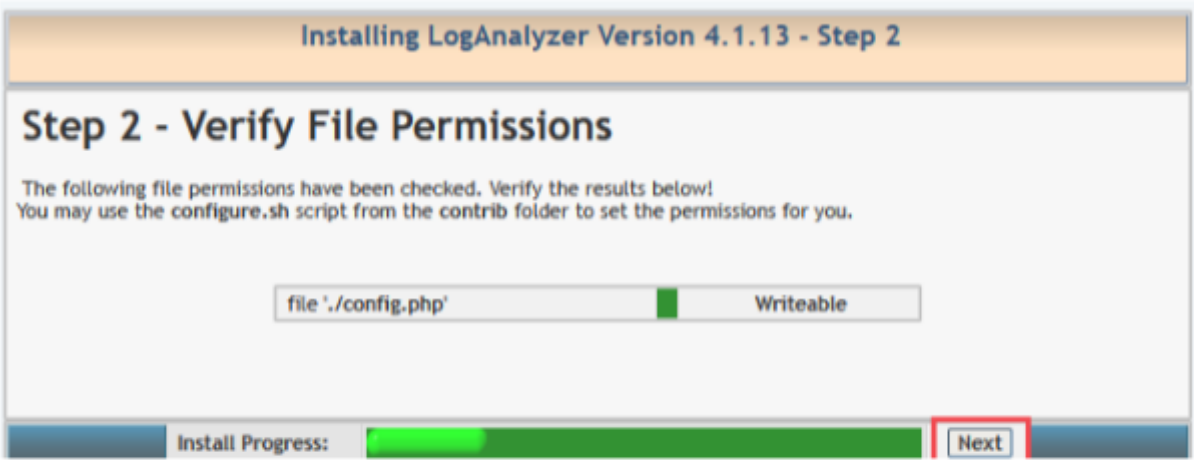


C’est NORMAL ! En effet nous n’avons pas encore initier l’installation de LogAnalyzer, il n’existe donc pas encore de fichier de configuration. Cliquez sur « here » pour lancer le setup.

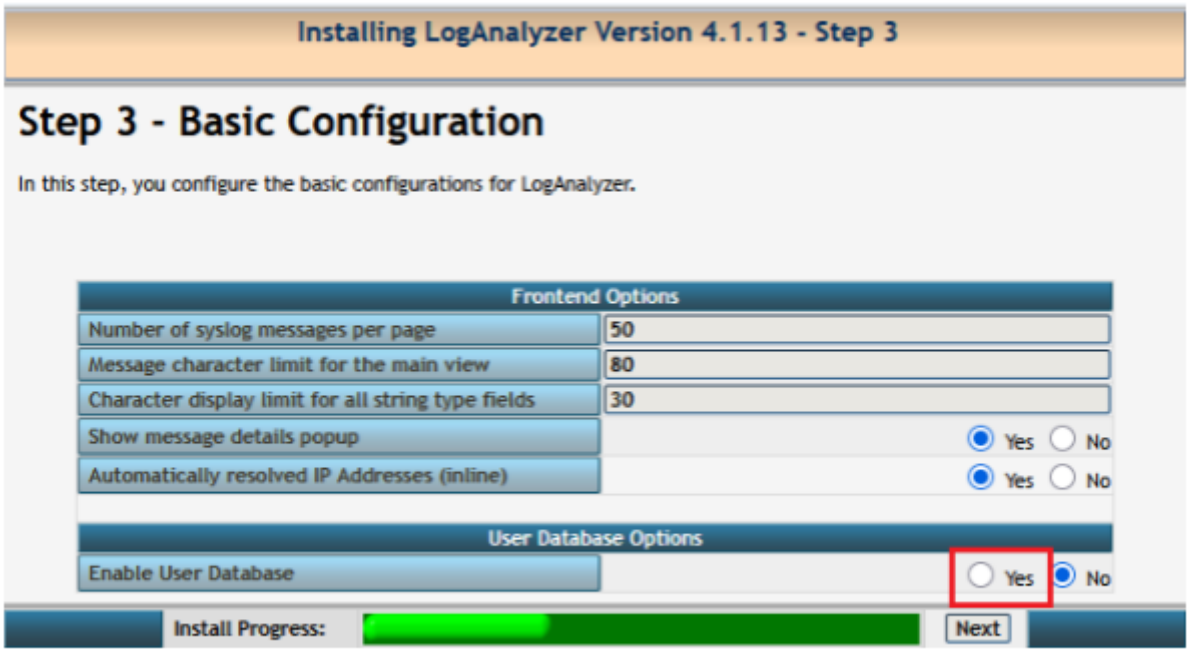
A l’étape 1, on vous explique que le setup va vérifier si les pré-requis sont respectés. Cliquez sur « Next » .



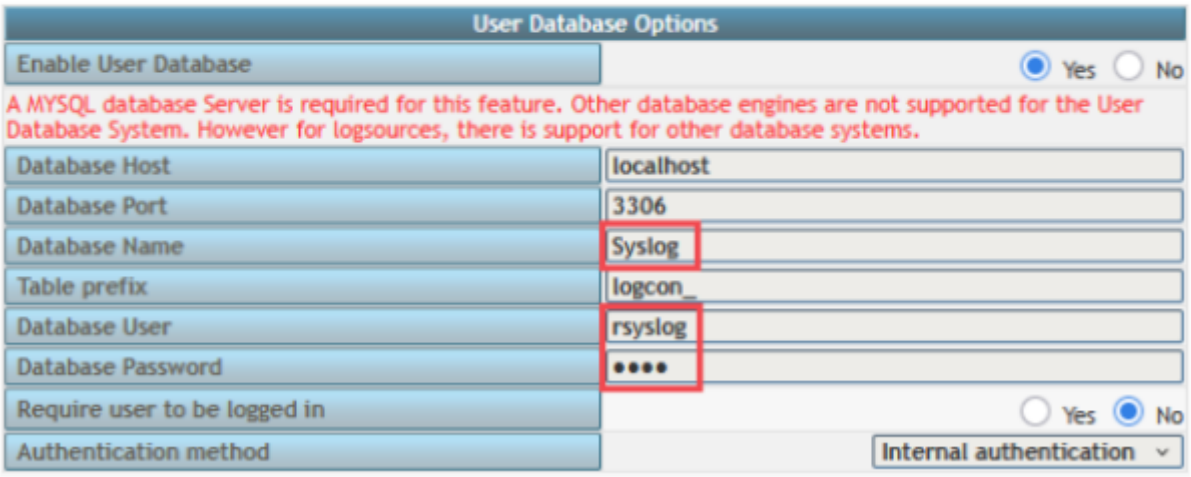
L’étape 2 contrôle les permissions sur les fichiers placés dans /var/www/html/loganalyzer. S’il n’y a pas d’erreur, cliquez sur « NEXT » sinon, relancez la commande « chown » précédemment décrite.



L’étape 3 est la configuration basique du logiciel. **Cochez la case « Yes »** de la question « Enable User Database » **pour renseigner les options de base de données.**



Dans la partie inférieure, **remplir les champs avec les informations de notre propre base de données Syslog** comme sur la capture ci-dessous. **Attention, pour le nom de la base de données il faut bien mettre un S majuscule.**
L'utilisateur sera **« rsyslog »** et le mot de passe que vous avez vous même défini au début.



Ces paramètres vont en réalité créer des tables supplémentaires dédiées à LogAnalyzer dans notre base de données Syslog. La partie « Table prefix » peut être laissée par défaut. Cliquez sur « Next ».

L'étape 4 indique que la connexion à la base de données définie à l'étape 3 a bien réussi et que les tables pour LogAnalyzer seront créées à l'étape suivante. Cliquez sur « Next ».

L'étape 5 valide la création des tables. Cliquez sur «Next ».

Prochaine étape, Créez un utilisateur pour se connecter à l'interface web de loganalyzer et définissez lui un mot de passe. Cliquez sur «Next ».

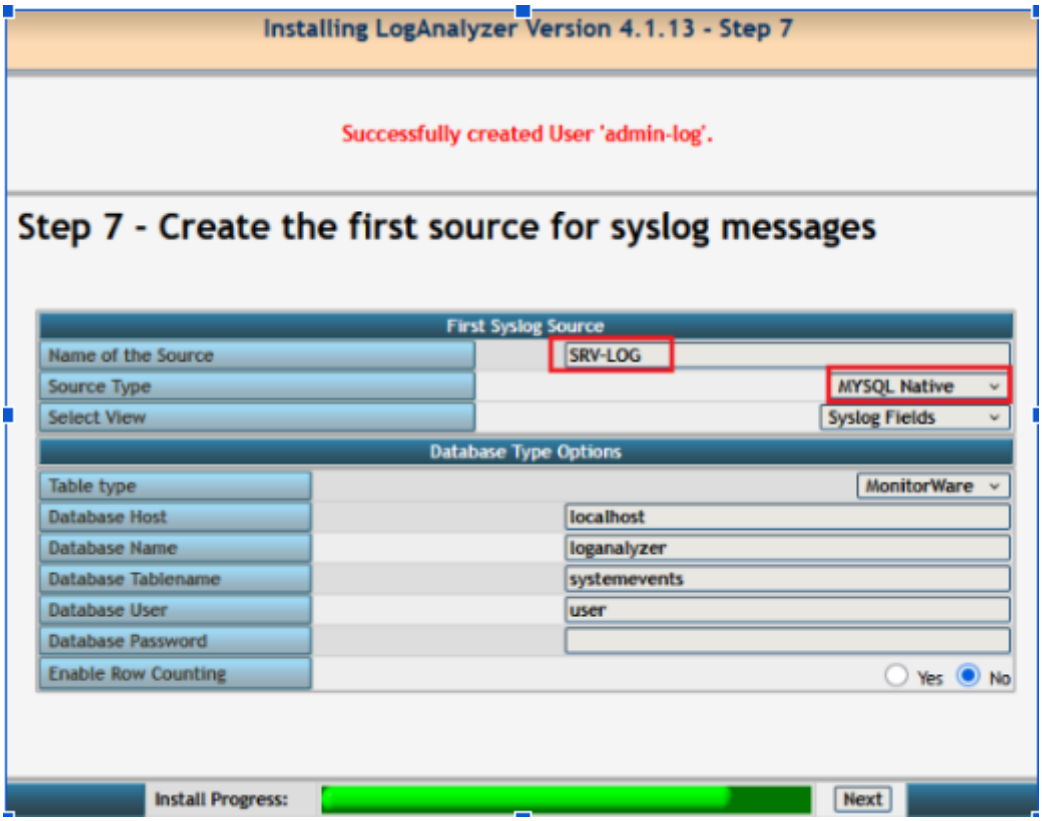


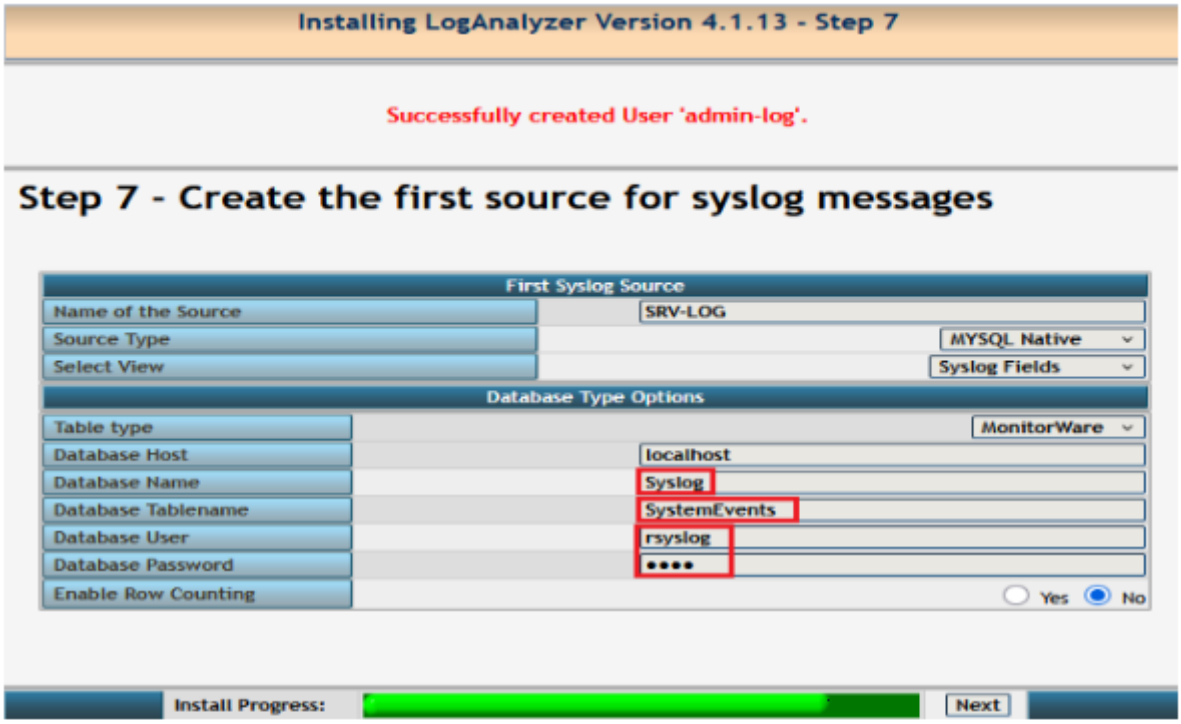
Créez un utilisateur pour se connecter à l'interface web de loganalyzer ell faut maintenant paramétrer la source des logs comme étant notre base de données. Renseignez le champ « Name of the Source » en indiquant ce que vous voulez, ici j'ai mis un nom de serveur par exemple.

Modifiez le champ « Source Type » en sélectionnant « MYSQL Native » ce qui déroule le menu inférieur des options de base de données.

Créez un utilisateur pour se connecter à l'interface web de loganalyzer ell faut maintenant paramétrer la source des logs comme étant notre base de données. Renseignez le champ « Name of the Source » en indiquant ce que vous voulez, ici j'ai mis un nom de serveur par exemple.

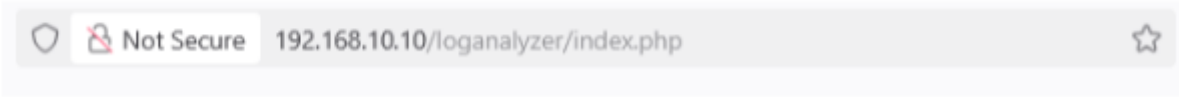
Modifiez le champ « Source Type » en sélectionnant « MYSQL Native » ce qui déroule le menu inférieur des options de base de données.


Installing LogAnalyzer Version 4.1.13 - Step 7
Successfully created User 'admin-log'.
Step 7 - Create the first source for syslog messages
First Syslog Source
Name of the Source
SRV-LOG
Source Type
MYSQL Native
Select View
Syslog Fields
Database Type Options
Table type
MonitorWare
Database Host
localhost
Database Name
loganalyzer
Database Tablename
systemevents
Database User
user
Database Password
Enable Row Counting
Yes
No
Install Progress:
Next



Terminez l'installation en cliquant sur « Finish! ».

Et là, **c'est le drame** ! Une page blanche WTF!



On ne panique pas ! C'est un bug connu de colonnes manquantes dans certaines tables de la base de données de syslog. Retournez sur votre serveur Debian, dans un terminal.

Connectez vous au service de base de données (juste écrire « mysql » si vous n'avez pas fait la sécurisation) :

```
mysql -u root -p
```

```
root@debian:/# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 73
Server version: 10.11.11-MariaDB-0+deb12u1 Debian 12

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)]>
```

Saisissez les commandes suivantes (vous pouvez copier/coller tout le bloc d'un seul coup) qui vont ajouter les colonnes manquantes à la **table SystemEvents** :

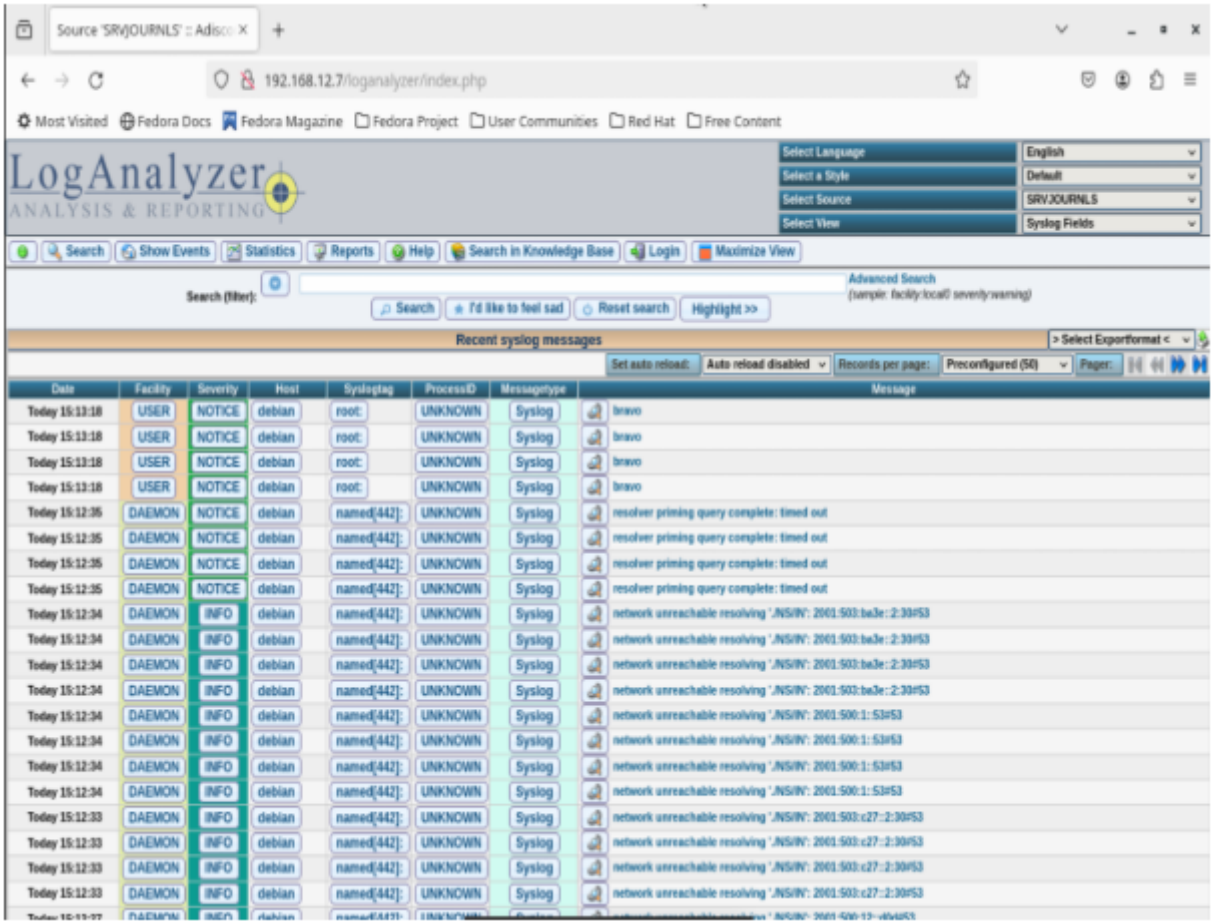
```
USE Syslog;
ALTER TABLE SystemEvents
ADD COLUMN checksum INT NOT NULL
DEFAULT 0,
ADD COLUMN processid VARCHAR(60) NOT
NULL DEFAULT 'UNKNOWN';
EXIT;
```

```
MariaDB [(none)]> USE Syslog;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [Syslog]> ALTER TABLE SystemEvents
    -> ADD COLUMN checksum INT NOT NULL DEFAULT 0,
    -> ADD COLUMN processid VARCHAR(60) NOT NULL DEFAULT 'UNKNOWN';
Query OK, 0 rows affected (0,017 sec)
Records: 0  Duplicates: 0  Warnings: 0

MariaDB [Syslog]> EXIT;
Bye
```

Retournez sur l'interface web de LogAnalyzer. Actualisez la page qui était blanche.



Pour installer RSYSLOG sur Fedora :

sudo dnf install rsyslog

sudo systemctl enable rsyslog

sudo systemctl start rsyslog

sudo systemctl status rsyslog

sudo nano /etc/rsyslog.d/50-remote.conf

#Envoi via UDP

. @adresse_ip_serveur:514

#Envoi via TCP

. @@adresse_ip_serveur:514

Remplacez adresse_ip_serveur par l’IP ou le nom du serveur de logs.

sudo systemctl restart rsyslog

sudo systemctl status rsyslog

Revision #2
Created 2026-03-23 13:20:24 UTC by SISR
Updated 2026-05-16 16:53:11 UTC by Admin