réseau

rsyslog
installation / configuration

Introduction

rsyslog est un système de journalisation open source pour les systèmes basés sur Unix. Son rôle principal est de recueillir, traiter et acheminer des journaux système (logs) à partir de diverses sources sur un système. Voici quelques-unes de ses principales fonctions :

1. Collecte des journaux : `rsyslog` peut recevoir des journaux à partir de diverses sources telles que le noyau du système, les applications, les services et d'autres composants du système d'exploitation. Il est capable de traiter une grande variété de formats de journalisation.

2. Traitement des journaux : `rsyslog` peut filtrer, formater et traiter les journaux en fonction de règles configurées. Cela permet aux administrateurs système de spécifier

comment les journaux doivent être manipulés en fonction de critères tels que le niveau de gravité, l'origine, etc.

3. Stockage des journaux : `rsyslog` peut stocker les journaux localement ou les transmettre à des serveurs de journalisation distants. Cela est utile pour la centralisation des journaux, ce qui facilite la gestion et l'analyse des journaux sur un réseau.

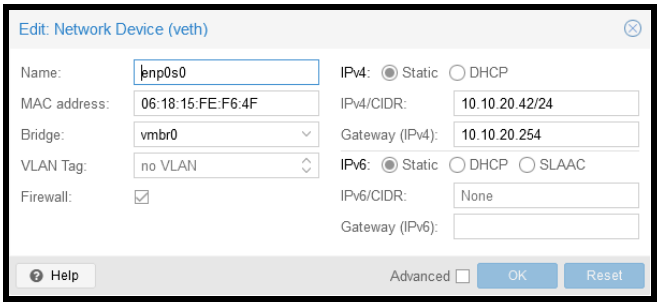
4. Protocoles de communication : `rsyslog` prend en charge plusieurs protocoles de communication, notamment UDP, TCP, et TLS, ce qui lui permet de transférer des journaux de manière sécurisée sur le réseau.

5. Sécurité : `rsyslog` offre des fonctionnalités de sécurité telles que la journalisation chiffrée et la possibilité de restreindre l'accès aux journaux.

En résumé, `rsyslog` est un outil puissant et flexible pour la gestion des journaux système sur les systèmes basés sur Unix, facilitant la collecte, le traitement, le stockage et la transmission des journaux pour l'analyse et la détection des problèmes.

Installation

On crée un conteneur avec un Debian 11, et on lui ajoute une nouvelle carte réseau avec l'adressage suivant ::



Commencez par mettre à jour le serveur avec :

```
apt update
apt upgrade
```

Ensuite, installez les extensions nécessaires pour le rsyslog :

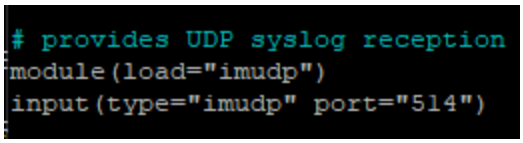
```
apt install rsyslog apache2 mariadb-server libapache2-mod-php7.4 php7.4
php7.4-mysql php7.4-gd
```

```
apt install rsyslog-mysql
```

Fournissez un mot de passe lorsqu'il est demandé : "centrallog".

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

Modifiez-le comme suit, en laissant le port par défaut :




```
*.* :ommysql:localhost,Syslog,rsyslog,rsyslog05
```

Une fois terminé, redémarrez le service rsyslog :

```
systemctl restart rsyslog.service
```

Ensuite, installez LogAnalyzer. Accédez au dossier srv et installez LogAnalyzer avec wget :

```
cd /srv
```

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

Décompressez le fichier :

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

Créez un nouveau dossier pour LogAnalyzer :

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

Copiez le contenu décompressé dans le nouveau dossier :

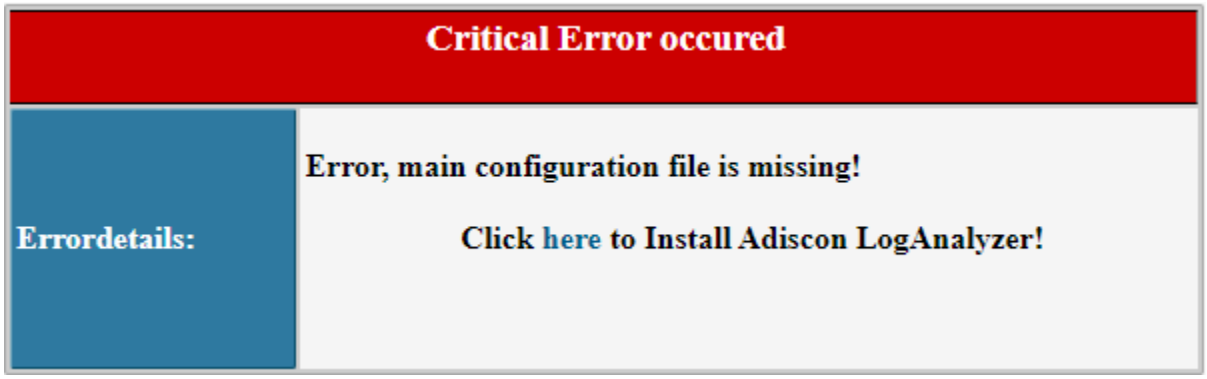
```
cp -a /srv/loganalyzer-4.1.13/src/* /var/www/html/loganalyzer
```

Donnez les droits au groupe et à l'utilisateur www-data utilisés par Apache :

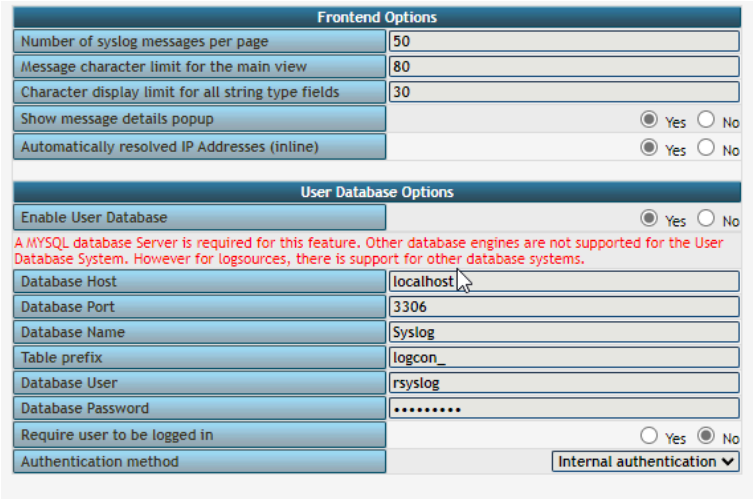
```
chown -R www-data:www-data /var/www/html/loganalyzer
```

Configuration

maintenants on rentre dans le navigateurs : http://10.10.20.42/loganalyzer

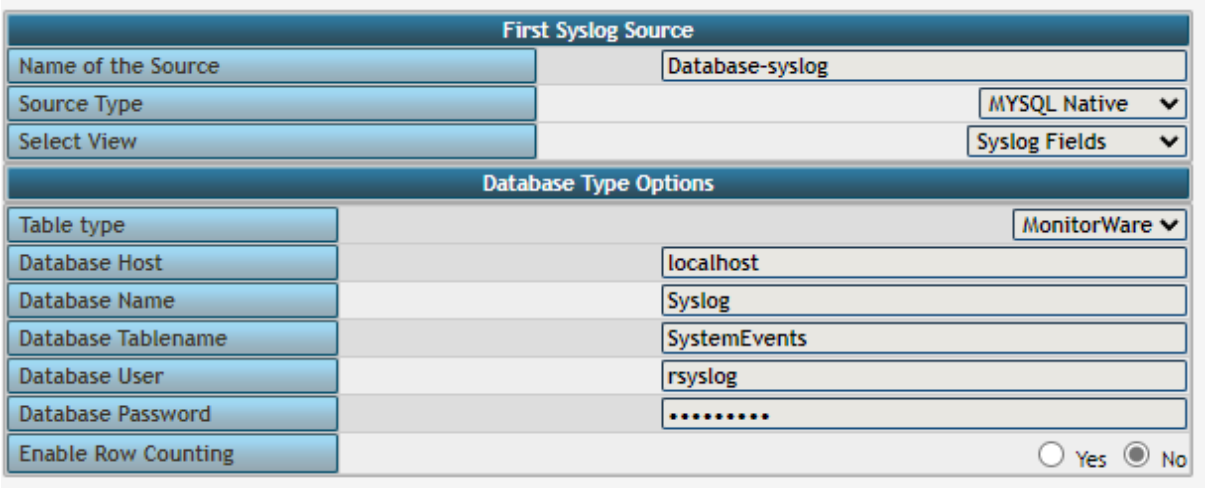


Cliquez sur "Here".



Acceptez l'activation des bases de données utilisateur (enable user databases) et ajoutez les identifiants utilisateur et mot de passe. Ensuite, cliquez sur "Next". Si vous arrivez à la page suivante, la connexion est opérationnelle. Cliquez sur "Next" à nouveau et attendez. Continuez à cliquer sur "Next", créez un utilisateur admin avec les informations suivantes :

- Nom d'utilisateur : admin
- Mot de passe : password



Et voilà, nous sommes sur Rsyslog. Maintenant, il faut faire remonter les logs de toutes nos machines.

remonter les logs

Éditez le fichier de configuration rsyslog :

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

Ajoutez la ligne suivante à la fin du fichier pour spécifier l'endroit où remonter les logs :

```
*.* @10.10.20.42
```

Enregistrez les modifications.

Ces étapes devraient vous permettre de configurer et d'utiliser Rsyslog avec succès.

Enfin, on installe Fail2Ban ainsi que l'agent GLPI et l'agent Zabbix. Voir le compte rendu correspondant.