SERVEUR DE LOG RSYSLOG

1)

Le rôle d'un fichier de log est de permet de stocker un historique des événements survenus sur un serveur, un ordinateur ou une application.

2)

Le rôle d'un serveur syslog est de gérer et de centraliser les fichier de journalisation de plusieurs application est de service

3)

le protocole réseau par defaut de syslog est UDP sur le port 514

Fonction Transmission de journaux

Port UDP 514

4)

terme à chercher :

un périphérique est le nom donner au équipement constituer dans un réseaux switch , routeur, ordinateur , serveur.

Un relais est une machine ou une application qui reçoit des messages Syslog et les retransmet à une autre machine.

Collecteur :

6)

6. Expliciter le fonctionnement d'un serveur syslog. Quelques éléments à considérer :

- Journal
- Traçabilité
- Sécurité

Configuration de rsyslog et installation de loganalyzer

configuration serveur rsyslog :

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 ####
###########################
```

Vérifiez que rsyslog écoute maintenant sur deux ports
ss -4altunp |grep 514

```
root@debian:~# ss -4altunp |grep 514
udp     UNCONN   0        0               0.0.0.0:514          0.0.0.0:*       users:(("rsyslogd",pid=581,fd=6))
```

configuration client: *etc*/rsyslog.conf

```
*.* @IP_SERVER:514
```

installer de loganalyzer

mise en place du service appache2 + php créer d'un vhost pour la page loganalyzer

```
apt-get install apache2 mariadb-server php7.0 php7.0-mysql php7.0-gd -y
```

installation de mysql secure :

```
mariadb_secure_installation
```

installation du plugin rsyslog pour mariadb :

```
apt-get install rsyslog-mysql -y
```

nano /etc/rsyslog.conf

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

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

service rsyslog restart
```

téléchargement de loganalyzer :

```
cd /srv
wget --no-check-certificate
http://download.adiscon.com/loganalyzer/loganalyzer-4.1.13.tar.gz
```

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

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

création de vhost

ajouter le nom de domaine sur le DNS

filtrage enlever les infos inutiles :

*.*info,*.=debug stop

si syslog not readable read access may be denied :

```
chmod 770 /var/log
```

sources :

https://www.it-connect.fr/centralisez-vos-logs-avec-rsyslog/
https://www.linuxtechi.com/setup-rsyslog-server-on-debian/
https://neptunet.fr/rsyslog-loganalyzer/
https://www.malekal.com/rsyslog-logrotate-gerer-les-logs-et-journaux-linux/

mariadb -u root -p
mdp : caribou

rsyslog_BDD :
user:rsyslog
mdp:caribou

loganalyzer :
user : caribou
mdp : caribou