Doc journalisation

Question :

Le rôle des fichiers de journaux son de garder une trace de ce qui se passe dans notre système, c'est une liste détaillée d'événement qui ont eu lieu avant un dysfonctionnement.

Les serveurs Syslog permettent de collecter les messages Syslog dans un lieu unique. Un serveur Syslog peut être un serveur physique, une machine virtuelle autonome ou un service logiciel.

Le protocole de base utiliser par syslog est le port 514 en UDP.

Dans le contexte syslog les périphériques son les différents éléments du réseau, le relais est une machine ou application qui reçois des message syslog pour les retransmettre à une autre machine et le collecteur permet de collecter et de lire les message syslog. Ensuite la fonctionnalité d'un message syslog correspond au type d'application générant le message syslog, La sévérité d'un message Syslog correspond au degré d'urgence du message et La priorité d'un message Syslog est définie par sa fonctionnalité et sa sévérité définit dans ce paragraphe.

Installation :

Pour commencer nous installons les paquets syslog **apt install rsyslog.**

Sur notre machine syslog est déjà installer donc va s'assurer qu'il démarrera automatiquement en même temps que le machine **systemctl enable rsyslog**, puis nous regardons le statut du service **systemctl status rsyslog**.

```
root@deb:~# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-11-25 11:10:23 CET; 8min ago
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 338 (rsyslogd)
      Tasks: 4 (limit: 1147)
     Memory: 2.6M
     CGroup: /system.slice/rsyslog.service
             └─338 /usr/sbin/rsyslogd -n -iNONE

nov. 25 11:10:23 deb systemd[1]: Starting System Logging Service...
nov. 25 11:10:23 deb rsyslogd[338]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.1901.
nov. 25 11:10:23 deb rsyslogd[338]:  [origin software="rsyslogd" swVersion="8.1901.0" x-pid="338" x-info="https://www.rsyslog.co
nov. 25 11:10:23 deb systemd[1]: Started System Logging Service.
```

Nous allons ensuite modifier le fichier **/etc/rsyslog.conf**

Nous décommentons les lignes « module » et « input » pour que le serveur accepte les logs venant de l'extérieur sur le pour 514 en UDP.

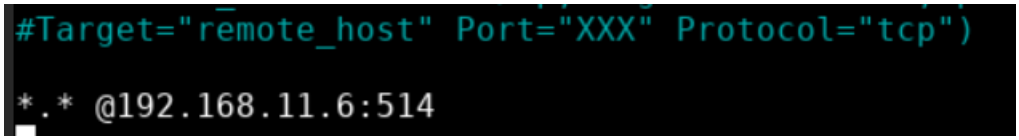
```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
```

On redémarre ensuite notre serveur syslog **systemctl restart rsyslog.service**

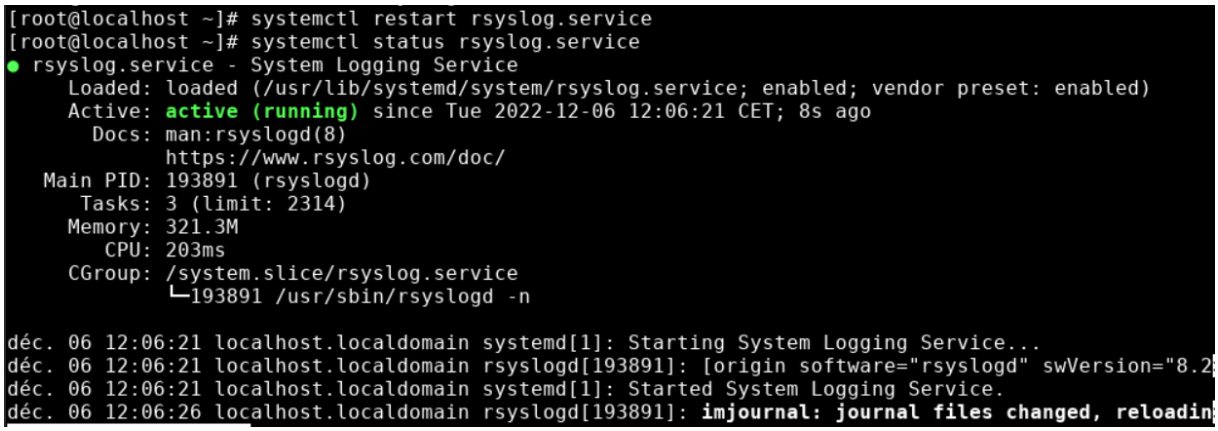
Sur le client :

Je m'assure que syslog démarrera à chaque démarrage de ma machine avec la commande **systemctl enable rsyslog**.

Je vais ensuite dans le fichier **/etc/rsyslog.conf** pour rajouter la ligne qui permettra à mon client de communiquer avec le serveur syslog.



Je redémarre ensuite mon service **systemctl restart rsyslog** et vérifie son statut **systemctl status rsyslog.**



Sur le serveur de journalisation pour voir les logs regarder dans le dossier **/var/log** et faire **cat syslog**.

Installation de loganalyzer :

Ce rendre dans le répertoire **/srv.**

Puis taper la commande : **wget http://download.adiscon.com/loganalyzer/loganalyzer-[dernière version disponible].tar.gz**

Nous devons ensuite décompresser le fichier télécharger **tar -zxvf [emplacement/nom dufichier]**

mkdir /var/www/html/loganalyzer → nous créons un répertoire loganalyzer