TP : Rsyslog : Collecte et analyse

Préparation de l'environnement

Pour ce TP, il vous sera nécessaire d'avoir deux machines GNU/Linux Debian en mode **réseau NAT**.
Elle seront nommé dans ce TP :

- rsyslog01 : Correspondra à la machine qui fera office de serveur / collecteur syslog
- rsyslog02 : Correspondra à la machine qui exportera des syslogs

Vous installerez sur chacunes le paquet « rsyslog ».

Facilities & Severities

Syslog intègre nativement plusieurs types d'informations.
Parmis elles, vous retrouverez deux indicateurs importants :

- Les facilitées [1]
- Les sévéritées [2]

Les facilitées permettent de « trier » les messages syslog qui sont envoyés au daemon.
Celà vous permet de générer des fichiers propre pour chaque facilité et de faciliter l'analyse des logs, que celà soit de façon manuelle ou par des outils d'analyses.

Les sévéritées sont des information spécifiant l'importance du message.
Le niveau de la sévérité indique par exemple si c'est un message d'erreur, d'information ou autre.
Les sévéritées peuvent également servir à trier les messages syslog, ou à les transmettres à des collecteurs afin de générer des alertes, dans le cadre d'une supervision par exemple.

1. https://en.wikipedia.org/wiki/Syslog#Facility
2. https://en.wikipedia.org/wiki/Syslog#Severity_level

Rsyslog l'ancêtre

1. **Configurez le collecteur rsyslog**

   Sur la machine « rsyslog01 », il vous faudra en tout premier lieu configurer les ports et protocoles d'écoute réseau afin de permettre la récupération des messages syslog.
   Dans sa configuration standard sous Debian, rsyslog lit les fichiers de configurations présents dans le répertoire « /etc/rsyslog.d/ » ayant une extension en « .conf ».
   Vous utiliserez ce mécanisme pour clarifier les écritures des configurations. (Attention, les chiffres qui seront explicité devant le nom de fichier tout le long du TP permettent de faire de l'ordonnancement dans les configurations. Ils sont donc très importants)

   Pour activer ces ports d'écoutes, dans le répertroire « /etc/rsyslog.d/ » créez un fichier nommé « 00-udp_listener.conf ».
   Vous y ajouterez la configuration nécessaire (2 lignes seulement) pour importer le module « imudp », et pour spécifier le port d'écoute UDP sur le 514.

   Il sera nécessaire de redémarrer rsyslog pour prendre en compte la configuration :

```
systemctl restart rsyslog.service
```

2. **Configurez l'exporter rsyslog**

   Maintenant que votre collecteur rsyslog est actif, vous allez pouvoir commencer à lui envoyer des données.

   Sur la machine « rsyslog02 », créez un nouveau fichier « /etc/rsyslog.d/00-forwarder-auth.conf »
   Vous y placerez dedans les configurations nécessaires pour exporter les logs d'authentification (identification rsyslog : auth,authpriv.*).

   Pour prendre en compte la configuration, vous devrez redémarrer le service rsyslog sur l'exporter :

```
systemctl restart rsyslog.service
```

3. **Consultation des logs**

   Sur le collecteur (rsyslog01), affichez en continu à l'aide de la commande tail le fichier « /var/log/auth.log ».
   Connectez vous à la machine rsyslog02 (login, élévation de privilège, connexion SSH, ...), vous devriez voir passer des lignes de logs dans le fichier étant identifié comme venant de la machine « rsyslog02 ».
   Faites la même action sur la machine rsyslog01 (toujours en laissant affiché le fichier).

   Vous devriez voir dans le même fichier des logs provenant des deux machines.

4. **Analyse des logs**

Analysez le format des lignes de log ci dessous, quels indicateurs pertinents y voyez vous ?

```
May 20 08:24:02 rsyslog01 sshd[697]: pam_unix(sshd:session): session opened for user vfricou(uid=1000) by (uid=0)
May 20 08:24:02 rsyslog01 systemd-logind[425]: New session 5 of user vfricou.
May 20 08:24:02 rsyslog01 systemd[1]: Started Session 5 of user vfricou.
May 20 08:24:03 rsyslog02 sshd[752]: pam_unix(sshd:session): session opened for user vfricou(uid=1000) by (uid=0)
May 20 08:24:03 rsyslog02 systemd-logind[393]: New session 10 of user vfricou.
May 20 08:24:10 rsyslog01 sudo:  vfricou : TTY=pts/1 ; PWD=/home/vfricou ; USER=root ; COMMAND=/usr/bin/su -
May 20 08:24:10 rsyslog01 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by vfricou(uid=1000)
May 20 08:24:10 rsyslog01 systemd[1]: Starting Cleanup of Temporary Directories...
May 20 08:24:10 rsyslog02 sudo: vfricou : TTY=pts/0 ; PWD=/home/vfricou ; USER= root ; COMMAND=/usr/bin/su -
May 20 08:24:10 rsyslog02 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by vfricou(uid=1000)
May 20 08:24:10 rsyslog01 su: (to root) vfricou on pts/1
May 20 08:24:10 rsyslog02 su: (to root) vfricou on pts/0
May 20 08:24:10 rsyslog01 su: pam_unix(su-l:session): session opened for user root(uid=0) by vfricou(uid=0)
May 20 08:24:10 rsyslog01 systemd[1]: systemd-tmpfiles-clean.service: Succeeded.
May 20 08:24:10 rsyslog01 systemd[1]: Finished Cleanup of Temporary Directories.
May 20 08:24:13 rsyslog01 su: pam_unix(su-l:session): session closed for user root
May 20 08:24:13 rsyslog01 sudo: pam_unix(sudo:session): session closed for user root
May 20 08:24:30 rsyslog01 sshd[703]: Received disconnect from 192.168.205.1 port 54717:11: disconnected by user
May 20 08:24:30 rsyslog01 sshd[703]: Disconnected from user vfricou 192.168.205.1 port 54717
May 20 08:24:30 rsyslog01 sshd[697]: pam_unix(sshd:session): session closed for user vfricou
May 20 08:24:32 rsyslog02 su: pam_unix(su-l:session): session opened for user root(uid=0) by vfricou(uid=0)
```

D'après ce log, déduisez ce qu'a fait l'utilisateur vfricou sur la machine « rsyslog02 ».

5. **Trier les logs**

Rsyslog possède un mécanisme de template permettant de faire ce tri de façon automatique.
Créez un fichier « /etc/rsyslog.d/10-dynamic_filtering.conf » contenant les deux lignes suivantes :

```
$template DynamicFile,"/var/log/syslog-clients/%HOSTNAME%-syslog.log"
*.* ?DynamicFile
```

Quel va être l'effet de cette configuration ?

6. **Arrêter les traitements de réception**

   En l'état de la configuration, les logs provenant des différentes machines sont stockés dans les mêmes fichiers que les logs de la machine « rsyslog01 ».
   Ce phénomène est entrainé par le fait que rsyslog possède par défaut un jeu de traitement pour plusieurs types de logs.
   Ces traitements sont configurés dans le fichier « /etc/rsyslog.conf ».
   Dans le cas d'une collecte de plusieurs machines, il est souhaitable que les machines distantes qui expédient les logs vers le collecteur ne viennent pas « polluer » les logs de la machine de collecte.

   Trouvez la configuration nécessaire pour arrêter le processing des logs collectés pour toutes les machines qui ne sont pas « rsyslog01 ».
   L'ajouter dans un nouveau fichier « /etc/rsyslog.d/99-stop_processing.conf ».
   (Indice, cherchez l'instruction « stop »)

7. **Dispatcher les logs « clients »**

   Actuellement, les logs reçus de la machine « rsyslog02 » sont stocké uniquement dans le fichier « /var/log/syslog-client/rsyslog02-syslog.log ».
   Pour de l'analyse manuelle, il peut être intéressant de reproduire le traitement prévu à l'origine par rsyslog pour chaques machines qui expédie des logs au collecteur.

   Nous allons tout d'abord modifier la configuration de la machine « rsyslog02 » présente dans le fichier « /etc/rsyslog.d/forward-auth.conf ».
   Ajouter la configuration nécessaire pour expérier également les logs de facilité local3 et user à « rsyslog01 ». (Identifiants local3.* et user.*).

   Pour mettre en place cette configuration il va vous falloir modifier le fichier que vous avez créé précédemment « /etc/rsyslog.d/10-dynamic_filtering.conf » pour ajouter le traitement de ces facilités.
   Vous redirigerez les facilités « local3.* » dans le fichier « /var/log/syslog-client/%HOSTNAME%/local3.log » et la facilité « user.* » dans le fichier « /var/log/syslog-client/%HOSTNAME%/user.log ».

   Pour tester que la segmentation des logs fonctionne bien, vous pouvez sur la machine « rsyslog02 » générer des logs pour les facilités données :

```
logger -p user.info "Message for user facility"
logger -p local3.info "Message for local3 facility"
```

   Si votre configuration est correcte, vous devriez voir sur « rsyslog01 » les logs de la machine « rsyslog02 » apparaitre dans les deux fichiers cités précédemment.