Configuration de Rsyslog

Introduction

Rsyslog est un système de gestion de logs sous Linux qui permet de collecter, filtrer, et envoyer des messages système (logs) à un serveur centralisé. Il est essentiel pour la gestion des journaux d'événements dans un environnement de production. Ce TP consiste à installer et configurer Rsyslog pour collecter et envoyer des logs à un serveur centralisé, ainsi que pour configurer des filtres pour organiser les logs.

Objectifs

1. Installer Rsyslog sur un serveur et un client.
2. Configurer Rsyslog pour envoyer les logs du client vers le serveur.
3. Configurer des filtres pour organiser les logs sur le serveur.
4. Vérifier que les logs sont bien envoyés et collectés sur le serveur centralisé.

Étapes réalisées

1. Installation de Rsyslog :

- **Sur le serveur central (serveur de collecte des logs)** :
    - Installez Rsyslog :

        sudo apt update

        sudo apt install rsyslog
    - Assurez-vous que Rsyslog est activé et fonctionne correctement :

        sudo systemctl enable rsyslog

        sudo systemctl start rsyslog
    - Vérifiez que le service fonctionne :

        sudo systemctl status rsyslog
- **Sur le client (machine qui envoie les logs)** :
    - Installez également Rsyslog sur le client :

        sudo apt update

        sudo apt install rsyslog
    - Activez et démarrez le service Rsyslog sur le client :

        sudo systemctl enable rsyslog

sudo systemctl start rsyslog

2. Configurer le serveur pour recevoir les logs du client :

- Sur le serveur, ouvrez le fichier de configuration Rsyslog (/etc/rsyslog.conf) :

  sudo nano /etc/rsyslog.conf

- Décommentez (ou ajoutez si nécessaire) la ligne suivante pour permettre à Rsyslog de recevoir des logs via UDP ou TCP :

  module(load="imudp") # Pour UDP

  input(type="imudp" port="514") # Port UDP 514

  module(load="imtcp") # Pour TCP

  input(type="imtcp" port="514") # Port TCP 514

- Redémarrez Rsyslog pour appliquer les changements :

  sudo systemctl restart rsyslog

3. Configurer le client pour envoyer les logs au serveur :

- Sur le client, ouvrez le fichier de configuration Rsyslog (/etc/rsyslog.conf) :

  sudo nano /etc/rsyslog.conf

- Ajoutez la ligne suivante pour spécifier l'adresse du serveur de logs centralisé (en supposant que l'adresse IP du serveur est 192.168.1.10):

  . @192.168.1.10:514 # Pour envoyer les logs via UDP

  . @@192.168.1.10:514 # Pour envoyer les logs via TCP

- Redémarrez Rsyslog sur le client :

  sudo systemctl restart rsyslog

4. Configurer des filtres sur le serveur pour organiser les logs :

- Sur le serveur, vous pouvez organiser les logs reçus en créant des fichiers de configuration pour chaque type de log.
- Par exemple, pour enregistrer les logs système dans un fichier séparé, ouvrez le fichier de configuration de Rsyslog et ajoutez cette ligne :

  if $fromhost == 'client1' then /var/log/client1.log

  & stop

- Vous pouvez également utiliser des filtres par niveau de log (ex : info, error, etc.) ou par type de service (ex : cron, auth, etc.).

- Après avoir configuré les filtres, redémarrez Rsyslog sur le serveur :

```
sudo systemctl restart rsyslog
```

5. Vérification de la collecte des logs :

- Pour vérifier que le client envoie bien les logs et que le serveur les reçoit, consultez les fichiers de log sur le serveur :

```
cat /var/log/client1.log
```

- Vous pouvez également vérifier les logs de Rsyslog sur le serveur pour voir si des erreurs se produisent lors de la réception des logs :

```
sudo tail -f /var/log/syslog
```

Résultats obtenus

1. Rsyslog a été installé avec succès sur le serveur et le client.
2. Le client a correctement envoyé les logs au serveur.
3. Les logs ont été organisés et filtrés sur le serveur en fonction des configurations définies.

Conclusion

Ce TP m'a permis de comprendre l'utilisation de Rsyslog pour collecter et centraliser les logs d'un réseau. Grâce à Rsyslog, j'ai pu configurer un serveur de logs centralisé et utiliser des filtres pour organiser les logs reçus. Cela permet de faciliter la gestion des journaux système et d'assurer une meilleure surveillance et sécurité du réseau.