

# Installation et utilisation de Rsyslog sur Debian

## Installation du serveur Rsyslog

Pour installer Rsyslog sur une distribution Debian, utilisez la commande suivante :

```
$ sudo apt -y install rsyslog
```

Le fichier de paramétrage se nomme `/etc/rsyslog.conf`.

Afin de pouvoir récupérer les logs il faut modifier ce fichier et activer soit le protocole UDP soit le protocole TCP en décommentant les lignes suivantes :

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

ou

```
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="10514")
```

Pensez à changer le port par défaut.

Choisissez quels journaux vous voulez utiliser en commentant ou décommentant les lignes suivantes :

```
auth,authpriv.* /var/log/auth.log
*.*;auth,authpriv.none -/var/log/syslog
#cron.* /var/log/cron.log
daemon.* -/var/log/daemon.log
kern.* -/var/log/kern.log
lpr.* -/var/log/lpr.log
mail.* -/var/log/mail.log
user.* -/var/log/user.log
mail.info -/var/log/mail.info
mail.warn -/var/log/mail.warn
mail.err /var/log/mail.err
```

Pour rajouter d'autres journaux qui seront gérés par rsyslog vous devez rajouter une ligne par application.

L'exemple suivant permet de récupérer les journaux du serveur WEB Apache :

```
syslog.* /var/log/apache2/error.log
```

Rajouter les lignes suivantes si elles n'existent pas en fonction de votre choix UDP ou TCP, elles permettent d'indiquer quels réseaux pourront accéder au serveur de logs.

```
$AllowedSender UDP, 127.0.0.1, 192.168.1.0/24
```

Attention à bien mettre les bonnes adresses de réseaux.

Dans cette configuration, le serveur Rsyslog reçoit les logs de l'ordinateur lui-même (127.0.0.1) et depuis les ordinateurs du réseau 192.168.1.0/24.

Ou

```
$AllowedSender TCP, 127.0.0.1, 192.168.1.0/24
```

Pour différencier les logs reçus des ordinateurs, ajoutez les deux lignes suivantes dans la partie **rules** du fichier :

```
$template DynamicFile, "/var/log/syslogclients/%fromhost%-syslog.log"
*. * ?DynamicFile
```

- Le répertoire **syslogclients** contiendra le fichier qui sera créé pour chaque ordinateur client.
- La variable **%fromhost%** contient soit le nom de l'ordinateur client soit son adresse IP.

Puis vous devez redémarrer votre service :

```
$ sudo systemctl restart rsyslog
```

Vérifiez que votre service est opérationnel :

```
$ sudo systemctl status rsyslog
```

Pour vérifier que le serveur écoute bien le port choisi (514):

```
$ ss -nlu
```

## Paramétrage du client

Il faut vérifier que le service **rsyslog** est bien actif.

Le fichier de paramétrage se nomme **/etc/rsyslog.conf** ou **/etc/rsyslog.d/50-default.conf**

Vous devez lui indiquer quels logs vous allez transmettre au serveur ainsi que l'adresse IP du serveur Rsyslog en ajoutant la ligne suivante si vous voulez remonter toutes les logs :

```
*.* @@IP_SERVEUR:10514 (pour TCP)
*.* @IP_SERVEUR:514 (pour UDP)
```

Si vous voulez juste remonter l'authentification :

```
auth,authpriv.* @IP_SERVEUR:514 (pour UDP)
auth,authpriv.* @@IP_SERVEUR:10514 (pour TCP)
```

Pour les mails :

```
mail.* @IP_SERVEUR:514 (pour UDP)
mail.* @@IP_SERVEUR:514 (pour TCP)
```

ou juste les erreurs critiques ou plus pour les mails :

```
mail.err @IP_SERVEUR:514 (pour UDP)
mail.err @@IP_SERVEUR:514 (pour TCP)
```

## Tester la remontée des logs

Les logs des clients et du serveur Rsyslog sont centralisés dans le répertoire **/var/log/syslogclients/** du serveur Rsyslog.

Vous pouvez tester les erreurs **auth** en faisant depuis un poste quelconque une connexion ssh à votre poste client en mettant volontairement un mauvais mot de passe et vous vérifierez alors que sur notre serveur de log que les erreurs sont bien remontées.

Utilisation de la commande **less**, de **grep** et d'une expression régulière :

```
# less /var/log/syslogclients/IPPOSTE-syslog.log | grep sshd
```

Cette commande liste la ou les connexions échouées ainsi que la connexion validée.

En omettant la commande **grep**, vous obtenez l'intégralité du fichier de log de votre poste client et cela peut très rapidement être illisible.

La commande suivante permet d'être plus sélectif dans la recherche d'informations :

```
#tail /var/log/syslogclients/IPPOSTE-syslog.log |grep Failed
```

La commande **Tail** affiche par défaut les 10 dernières lignes (les plus récentes) de votre fichier pour les services qui sont en échec.

À partir du fichier log et des expressions régulières avec **grep** ou **sed** vous pouvez rechercher des données particulières de manière plus sélectives.

## Agent rsyslog pour Windows

Lien : <https://www.rsyslog.com/windows-agent/windows-agent-download/>

From:

/ - **Les cours du BTS SIO**

Permanent link:

</doku.php/reseau/syslog/installrsyslog?rev=1670364995>

Last update: **2022/12/06 23:16**

