Configurer l'envoi des journaux sur Debian/Ubuntu

Afin de centraliser les logs vers un serveur de log (port 514 UDP ou TCP). Il suffit d'éditer le fichier “/etc/rsyslog.conf”

copy

```
nano /etc/rsyslog.conf
```

A la fin du fichier vous pouvez ajouter cette ligne:

copy

```
*.*     @<ip>:514
```

Cela va rediriger tous les logs de votre serveur vers le serveur syslog. Cela risque de faire beaucoup car les niveaux debug et info sont capturés par l'étoile.

On peut spécifier les niveaux qui nous intéressent en modifiant notre ligne par ceci:

copy

```
*.notice,warn,err,crit,alert,emerg    @<ip>:514
```

Le serveur n'enverra que les journaux supérieurs ou égal au niveau notice. Après chaque modification, il faut redémarrer le service

copy

```
/etc/init.d/rsyslog restart
```

Vous pouvez tester l’envoi de log avec les commandes suivantes:

copy

```
logger -p auth.info "test link to syslog server. lvl info"
logger -p auth.crit "test link to syslog server. lvl crit"
```

Les 2 lignes de commandes vont générer 2 entrées: une de niveau “info” et l'autre de niveau critique

From:
https://wiki.esia-sa.com/ - **Esia Wiki**

Permanent link:
https://wiki.esia-sa.com/syslog/syslog_debian_ubuntu

Last update: **2023/04/17 09:07**