

Installation de Rsyslog sur Debian

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 dé commentant 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") Choisissez quels journaux vous voulez utiliser en commentant ou dé-commentant 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
```

From:

/ - Les cours du BTS SIO

Permanent link:

</doku.php/reseau/syslog/installrsyslog?rev=1636319605>

Last update: 2021/11/07 22:13

