

Sommaire

[1. Analyse de logs 1](#_Toc131750236)

# 1. Analyse de logs

Avant de pouvoir analyser des logs il est important de savoir à quoi ils peuvent servir :

* Avoir un historique
* Avoir une traçabilité
* Débugger
* Superviser
* Avoir accès à des informations confidentielles

Dans les logs nous pouvons retrouver une notion de **Temporalité**. Il peut être parfois très embêtant à lire pour un Administrateur car il y a beaucoup d’informations.

Dans les logs il existe aussi différents niveaux de détails :

* ERROR
* WARNING
* INFO
* DEBUG

Une méthode à utiliser pour le **stockage des logs** est de faire de la **rotation des logs dans le temps** (Stockage de logs -> Archivage -> Suppression) ou alors de faire de la **rotation par taille des logs**

**/ ! \ Attention : Il est important d’externaliser les logs du système qui journalise. Pour ça nous pouvons utiliser des logiciels de puit de logs comme la suite ELK, SYSLOG-NG ou GRAYLOG**