Les outils de journalisation

Syslog

Syslog est une solution **historique** sur Linux/UNIX, il récupère des informations **noyau** (via **klogd**), celles envoyées sur le socket **/dev/log**, et possiblement via le réseau (**protocole syslog, UDP port 514**) et les écrit (par défaut) dans des fichiers textes dans **/var/log/...**

Les logs sont classé par 2 codes :

les **“facility”** de 0 à 26, ils aident à déterminer les types de message journalisé.

les **“Severity Level”** de 0 à 7, 0 étant le plus critique (emergency) et le 7 du debug.

Voir ici le tableau en entier