R5B08 - Continuité de services

Journaux

Bruno BEAUFILS

2024/2025

Journaux (*logs*)

- Garder une trace de chaque action produite sur un système
  - débogage
  - surveillance
  - comptabilité
  - analyse
- Solution la plus simple
  - chaque **service**
    - enregistre un **message**
    - avant (après) de faire une **action**
  - dans des fichiers **textes** simples
- Sous UNIX il existe un système pour enregistrer ce genre de message
  - `syslog`
  - Linux avec `systemd` utilise `journalctl(1)`

Syslog (généralités)

- Protocole de communication de message de journalisation RFC 5424
  - produire
  - transmettre
  - collecter
- Objectifs initiaux
  - Architecture de communication
  - Format de message
  - Gestion de la fiabilité et de l'authenticité des messages

- Références
  - Syslog : The Complete System Administrator Guide

Syslog (détails)

- Message **horodaté** défini selon
  - **priority**
    - emerg, alert, crit, err, warning, notice, info, debug
  - **facility**
    - kern, user, mail, daemon, auth, syslog, etc.
- Stockage
  - généralement dans `/var/log`
  - serveur centralisé
  - **rotation** des fichiers
    - `logrotate(8)`
    - on renomme les fichiers en supprimant les plus anciens
- API et commande
  - `syslog(3)`
  - `logger(1)`