Gestion des logs

Matthieu Herrb

Capitoul - 16 février 2023

https://homepages.laas.fr/matthieu/talks/capitoul-intro-logs.pdf

Licence

Introduction

Journalisation : événements dans le système d'information (accès + actions)

- pour comprendre ce qui s'est passé en cas de problème
- données sur l'utilisation d'un service
- obligations légales de tracabilité (LCEN, LSI,...)
- respect de la vie privée (RGPD)

Principes de base

- horodatage fiable (au moins NTP) - Attention aux fuseaux horaires...
- garantir la sécurité des journaux
- format lisible facilement
- supporter la charge (volume de stockage et nombre d'E/S par seconde)

Centraliser, pourquoi ?

- « bastion » dédié aux journaux
- facilite le respect des principes de base
- permet d'envisager de la correlation des journaux pour détection automatique d'événements anormaux (pannes latentes, attaques,...)

Sécurisation

- sécuriser la centralisation via transport TLS
- attention aux contenus malveillants dans les données tracées (log4j & Co) : filtrer ce qui est tracé,
- au niveau du système de journalisation : gestion simple et prédictive en cas d'échec de l'enregistrement d'un événement :
  - préférer un arrêt brutal du service à un mode sans journal
  - superviser le sytème de journalisation pour éviter la saturation
  - exemple : appel système `sendsyslog(2)` dans OpenBSD
- garantir l'intégrité des journaux

Protection des données personnelles

Les journaux contiennent beaucoup de données personnelles (identifiants, adresses IP,...) $\rightarrow$ RGPD

- minimiser ce qui est collecté (contradictoire avec d'autres recommandations)
- obligation d'information
- obligation de sécurisation et déclaration en cas de compromission
- limitation de la durée de conservation

Techniques de journalisation & centralisation

- syslog « à l'ancienne » syslogd + centralisation via UDP port 514
- Niveau application : log4j, python logging,...
- syslog-ng & rsyslog : TCP / TLS
- systemd-journald : collecte & stockage « modernes »
- Elastic stack : stockage des journaux en BDD
- Windows : observateur d'événement + passerelles pour centralisation (WEF / WEC)

Références

- Recommandations de sécurité pour l'architecture d'un système de journalisation, Guide ANSSI, v2.0, janvier 2022.
- La CNIL publie une recommandation relative aux mesures de journalisation, Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation.
- L'obligation de journalisation des systèmes d'information, Marc-Antoine Ledieu, mars 2022.
- Comment le Conseil d'État a sauvé la conservation des données de connexion, Marc Rees, Nextimpact.com, avril 2021.
- Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory, Guide ANSSI, v1.1, juillet 2022.

Questions ?