NOM: PRÉNOM: CLASSE:

MR ROLIN 2025

[DIVERS] LogFile

Objectifs

- Expliquer le rôle et la structure des fichiers journaux.
- Identifier les différents types de logs.
- Lire, filtrer et interpréter des logs simples.
- Appliquer les bonnes pratiques de gestion et d'analyse des logs.

Introduction

Chaque système informatique, qu'il s'agisse d'un poste de travail, d'un serveur ou d'un réseau, enregistre discrètement ce qu'il fait à chaque instant. Ces enregistrements constituent les fichiers journaux, ou log files.
Ils sont essentiels au bon fonctionnement des environnements informatiques professionnels : ils permettent de retracer les événements passés, de comprendre la cause d'une erreur ou encore de prouver qu'une action donnée a bien eu lieu.
Dans le monde de la maintenance et de l'administration des systèmes, savoir lire et interpréter un log est donc une compétence de base. C'est ce qui permet d'intervenir efficacement lorsqu'un service tombe en panne, lorsqu'une application ne démarre plus ou lorsqu'une activité suspecte est détectée sur un réseau.

Qu'est-ce qu'un fichier journal ?

Un fichier journal est un document texte, souvent généré automatiquement par un système ou une application, qui enregistre chronologiquement tout ce qui se passe : démarrages, connexions, erreurs, opérations internes, etc.
Chaque ligne du fichier correspond à un événement précis, identifié par une date et une heure. Le message contient également un niveau de gravité (information, avertissement, erreur) et la source qui l'a émis (par exemple, un service système ou un programme).
Ainsi, si un serveur web échoue à démarrer, on pourra lire dans le log une ligne semblable à :

[2025-11-03 10:45:12] [ERROR] [apache2] Failed to start service.

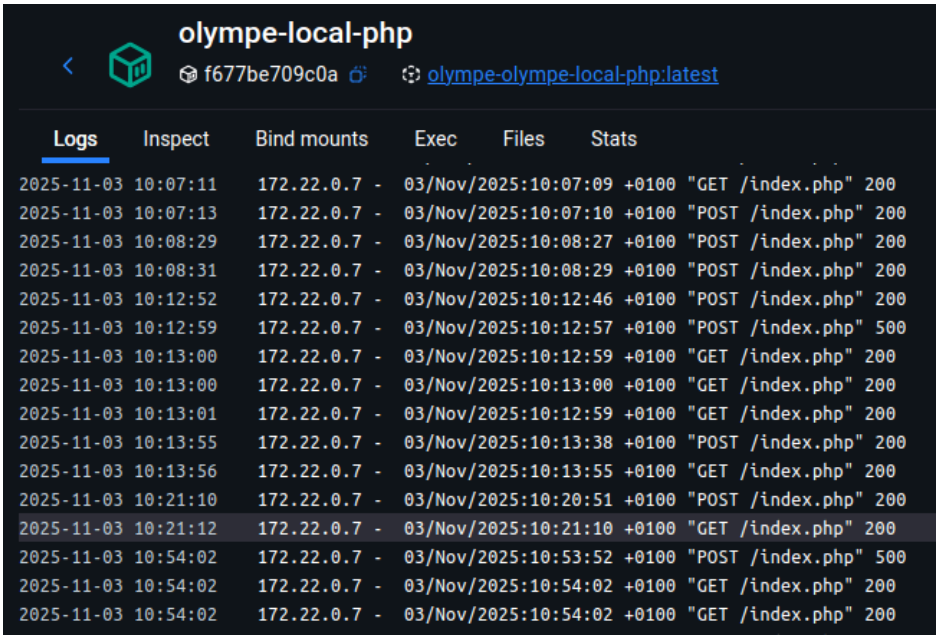
Cette trace devient alors un indice précieux pour comprendre la cause du problème.

Log interne généré par une application
Contient la date, le niveau et un message

```
[2025-10-24 13:14:01] [INFO] ✓ FLAGS vérifiés : 0/39, 0 modifications
[2025-10-24 13:14:01] [INFO] ✓ 0 mails traités pour supplier
[2025-10-24 13:14:01] [INFO] 📁 [18/18] Traitement : T&AOI-ches
[2025-10-24 13:14:02] [DEBUG] 0 messages trouvés dans T&AOI-ches
[2025-10-24 13:14:02] [DEBUG] Dossier T&AOI-ches vide, passage au suivant
[2025-10-24 13:14:02] [INFO] === Synchronisation terminée : 0 mails au total ===
[2025-10-24 13:14:02] [INFO] ✓ 0 mails récupérés du serveur IMAP
[2025-10-24 13:14:02] [DEBUG] Aucun mail à sauvegarder
[2025-10-24 13:14:02] [INFO] ✓ 0 mails enregistrés dans la base de données
[2025-10-24 13:14:02] [INFO] ✓ Synchronisation terminée pour Epicloot
[2025-10-24 13:14:03] [DEBUG] Récupération des mails pour le compte : epicloot
[2025-10-24 13:14:03] [DEBUG] Ouverture de la base de données : oxydmail.db
[2025-10-24 13:14:03] [DEBUG] Création/vérification des tables et index
[2025-10-24 13:14:03] [INFO] ✓ Base de données initialisée : oxydmail.db
[2025-10-24 13:14:04] [INFO] ✓ 966 mails récupérés pour le compte epicloot
[2025-10-24 13:14:04] [INFO] ✓ 966 mails chargés
```

Log php affiché par docker

Chaque ligne correspond a une action (ex: appel d'une page web)



Les différents types de logs

Tous les systèmes ne génèrent pas les mêmes fichiers journaux. On distingue généralement quatre grandes familles :

- Les logs système, qui concernent le fonctionnement de l'ordinateur ou du serveur (démarrage, pilotes, gestion des ressources).
- Les logs applicatifs, produits par les logiciels eux-mêmes pour signaler leur état de fonctionnement.
- Les logs de sécurité, qui enregistrent les tentatives de connexion, les réussites ou échecs d'authentification, les accès aux fichiers sensibles.
- Les logs réseau, utilisés pour suivre le trafic et repérer des anomalies telles que des paquets rejetés ou des coupures de communication.

Pour un technicien, ces différentes sources forment une mosaïque d'informations à recouper pour établir un diagnostic fiable.

Lire et analyser un log

L'analyse de logs commence souvent par une observation manuelle. Les fichiers étant en texte brut, on peut les ouvrir avec des commandes simples : cat, less ou tail -f pour suivre les événements en temps réel.
Lorsqu'un fichier est volumineux, il devient nécessaire d'utiliser des outils de filtrage comme grep pour rechercher un mot clé, par exemple "error". Les techniciens plus expérimentés s'appuient sur des scripts avec awk ou sed pour automatiser le traitement.
Dans les entreprises, la quantité de logs générée quotidiennement est considérable. C'est pourquoi on recourt à des solutions de collecte et d'analyse centralisées comme ELK Stack (Elasticsearch, Logstash, Kibana) ou Splunk, qui permettent de visualiser les événements sous forme de tableaux de bord et de repérer rapidement les anomalies.

Les bonnes pratiques de gestion

La gestion des fichiers journaux ne se limite pas à leur lecture. Elle implique aussi de décider où et combien de temps ils seront conservés. Une politique de rotation des logs permet de supprimer ou d'archiver automatiquement les anciens fichiers afin d'éviter qu'ils ne saturent le disque.
Il est également important de sécuriser l'accès à ces fichiers : ils peuvent contenir des informations sensibles sur les utilisateurs ou sur la configuration du système.

Enfin, les administrateurs mettent souvent en place des systèmes d'alerte automatisés : dès qu'un message critique apparaît dans un log, une notification est envoyée par e-mail ou SMS. Cela permet d'intervenir avant que le problème ne prenne de l'ampleur.

Étude de cas pratique

Imaginons qu'un utilisateur signale que son serveur web ne répond plus. Le technicien ouvre alors un terminal et consulte le fichier /var/log/apache2/error.log. En recherchant la chaîne "error", il découvre qu'un module du service n'a pas pu être chargé à cause d'une erreur de configuration. Après correction du fichier de paramètres et redémarrage du service, le technicien vérifie à nouveau le log pour s'assurer que l'erreur a disparu.
Cet exemple illustre la méthode classique de diagnostic à partir des journaux système : observer, filtrer, identifier la cause, corriger, puis vérifier.

Conclusion

Les fichiers journaux sont la mémoire vivante d'un système informatique. Ils racontent ce qui s'est produit, à quel moment, et dans quelles conditions. Leur lecture demande un peu de rigueur, mais elle fournit des informations indispensables à la stabilité et à la sécurité des environnements professionnels.
Pour un technicien ou un administrateur système, apprendre à manipuler les logs, c'est acquérir une véritable compétence d'enquêteur. C'est aussi un premier pas vers des domaines plus avancés comme la supervision en temps réel ou la cybersécurité.