CAHIER DES CHARGES

ELK

1. Contexte du projet

La Maison des Ligues de Lorraine fournit des espaces et des services mutualisés aux ligues sportives régionales. Elle héberge plus de 20 associations dans quatre bâtiments.

La M2L a donc besoin de centraliser les journaux (logs) de ses systèmes et équipements informatiques, tout en garantissant leur sécurité, leur intégrité et leur accessibilité.

2. Besoins exprimés par la M2L

La M2L doit pouvoir superviser ses systèmes informatiques via une solution centralisée de collecte et d'analyse des logs.

L'objectif est de mettre en place une solution de supervision et d'analyse de logs, fiable, de préférence open-source et compatible avec le reste de l'infrastructure existante. Il est donc nécessaire de mettre en place une infrastructure permettant :

- La collecte des logs depuis différents systèmes (Windows, Linux, équipements réseau) ;
- La centralisation de ces logs sur un serveur dédié ;
- L'analyse et la visualisation des données via une interface accessible.

Enfin, la M2L doit pouvoir :

- Détecter rapidement les anomalies ou incidents ;
- Effectuer des recherches efficaces dans les logs ;
- Conserver un historique des événements pour des besoins d'audit ou d'investigation.

3. Solution proposée

Afin de répondre aux besoins de supervision et d'analyse des logs de la Maison des Ligues de Lorraine, la solution retenue est la mise en place d'une stack ELK (Elasticsearch, Logstash, Kibana).

ELK est une suite d'outils open-source spécialisée dans la gestion et l'analyse de logs. Elle permet de centraliser les données, de les indexer et de les visualiser via une interface web.

La solution repose sur les composants suivants :

- Elasticsearch : moteur de recherche et d'indexation des logs ;
- Logstash : outil de collecte, transformation et envoi des logs ;
- Kibana : interface web de visualisation et d'analyse ;
- Beats (Filebeat / Winlogbeat) : agents installés sur les machines pour envoyer les logs.

Une fois les logs collectés et indexés, ils peuvent être exploités via Kibana, permettant :

- La visualisation des événements sous forme de tableaux et graphiques ;
- La recherche rapide dans de grands volumes de données ;
- La création de dashboard personnalisés.

Elasticsearch permet également :

- De filtrer les données par source (Windows, Linux, TrueNAS, etc.) ;
- De séparer les logs selon leur origine (par ligue ou par type de service) ;
- De sécuriser les accès via des comptes utilisateurs et des rôles.

Dans le cadre du projet, ELK peut être configuré en HTTPS afin de garantir la confidentialité des échanges, et intégré à l'infrastructure existante.

L’un des principaux avantages d’ELK est qu’il s’agit d’une solution partiellement gratuite, largement utilisée, et adaptée aux environnements professionnels. Elle est également flexible et évolutive.

L’administration se fait via des fichiers de configuration et une interface web, permettant une gestion centralisée et efficace.

C’est donc une solution adaptée, qui répond efficacement aux besoins de la M2L en matière de supervision, de sécurité et d’analyse des systèmes, tout en restant économique et évolutive.