SAE - projet 2 - FA
Collecte et traitement des logs de fonctionnement

1 Introduction

Les applicatifs s'exécutant sur un serveur génèrent ce qu'on appelle des "logs". Il s'agit de fichier journaux, stockant différentes informations sur l'activité de l'application.

Les informations peuvent être de nature très diverses, et porter sur le fonctionnement interne de l'application ("logs applicatifs"), sur l'OS ou l'environnement dans lequel il tourne ("logs systèmes"), sur le trafic réseau ("logs HTTP"), ou sur le fonctionnement du SGBD.

Les intérets sont multiples : détecter des problèmes de performance (sous-capacité en RAM, en CPU, en disque, etc.), "tracer" des bugs en cas de dysfonctionnement pour pouvoir les corriger, mais aussi archiver les connections utilisateurs pour des raisons légales.

Attention, il s'agit d'une fonctionnalité différente de ce qu'on appelle la "supervision réseau", qui elle fait un "monitoring" des équipements réseaux afin de surveiller leurs performances.

2 Travail à effectuer

Avant toute production, vous devrez vous **documenter** un maximum. Vous avez ci-dessous un ensemble de sources, qu'il vous faudra explorer. Vous êtes bien sur libre d'en utiliser d'autres, mais dans tous les cas il faudra les citer.

Q2.1 - Produire un document de synthèse en Markdown présentant les solutions libres existantes de collecte, centralisation et présentation de logs. Vous donnerez leurs points-clés (*features*, communauté associée, etc.) et leurs avantages et inconvénients respectifs. Vous vous intéresserez notamment aux possibilités de centralisation (collecte des logs issus de plusieurs conteneurs/machines), à la facilité d'utilisation et d'installation, et aux possibilités offertes par les "dashboard".

Q2.2 - Produire un Dockerfile qui met un oeuvre une situation simple de collecte de logs, basée sur **une** des solutions existantes. Le lancement du (des ?) conteneur(s) doit permettre de se faire une idée des possibilités, via une doc associée, rédigée en Markdown.

Modalités pratiques

- L'ensemble du travail (3 fichiers a priori) : un *Dockerfile* et deux fichiers Markdown) sera à déposer sur Universitice, selon des modalités et un calendrier qui sera publié ultérieurement sur la page dédiée.
- Volume horaire dédié (en autonomie) : 4 x 3h.
- Travail en 11 équipes de 2 et une équipe de trois (dans le groupe B)
- Constitution des équipes : auto-organisation, équipes à definir en début de projet

Note : vous n'êtes pas tenu d'avoir vos documents de travail en public sur votre dépot, vous pouvez créer un dépot privé sur votre compte pour y déposer vos fichiers. Il s'agit d'un travail personnel par équipe, et tout plagiat ou travail trop similaire sera sanctionné.

Le travail sur Github permet notamment d'avoir un "rendu" de vos fichiers Markdown via Web.

Voir ici pour les spécifications de Markdown sur Github :
`https://docs.github.com/en/get-started/writing-on-github/getting-started-with-writing-and-formatti`
`basic-writing-and-formatting-syntax`

3 Sources

- `https://www.syloe.com/collecte-et-traitement-des-logs/`
- `https://blog.wescale.fr/comment-mettre-en-place-une-solution-de-centralisation-de-logs`
- `https://newrelic.com/fr/resources/white-papers/log-management-best-practices`

- https://www.splunk.com/fr_fr/data-insider/what-is-it-monitoring.html
- https://www.splunk.com/fr_fr/data-insider/what-is-server-monitoring.html
- Xavki : C'est quoi l'OBSERVABILITE : https://www.youtube.com/watch?v=dMzlclnDJLw