Configuration ELK Stack (Elasticsearch, Logstash, Kibana, Filebeat)

Ce projet configure une stack ELK complète pour la collecte, le traitement, la visualisation et l'alerte des logs transactionnels en temps réel.

Composants

- **Elasticsearch 8.11.4** : Moteur de recherche et stockage des données.
- **Logstash 8.11.4** : Traitement et transformation des logs.
- **Kibana 8.11.4** : Visualisation et analyse des données.
- **Filebeat 8.11.4** : Collecte et envoi des logs vers Logstash.

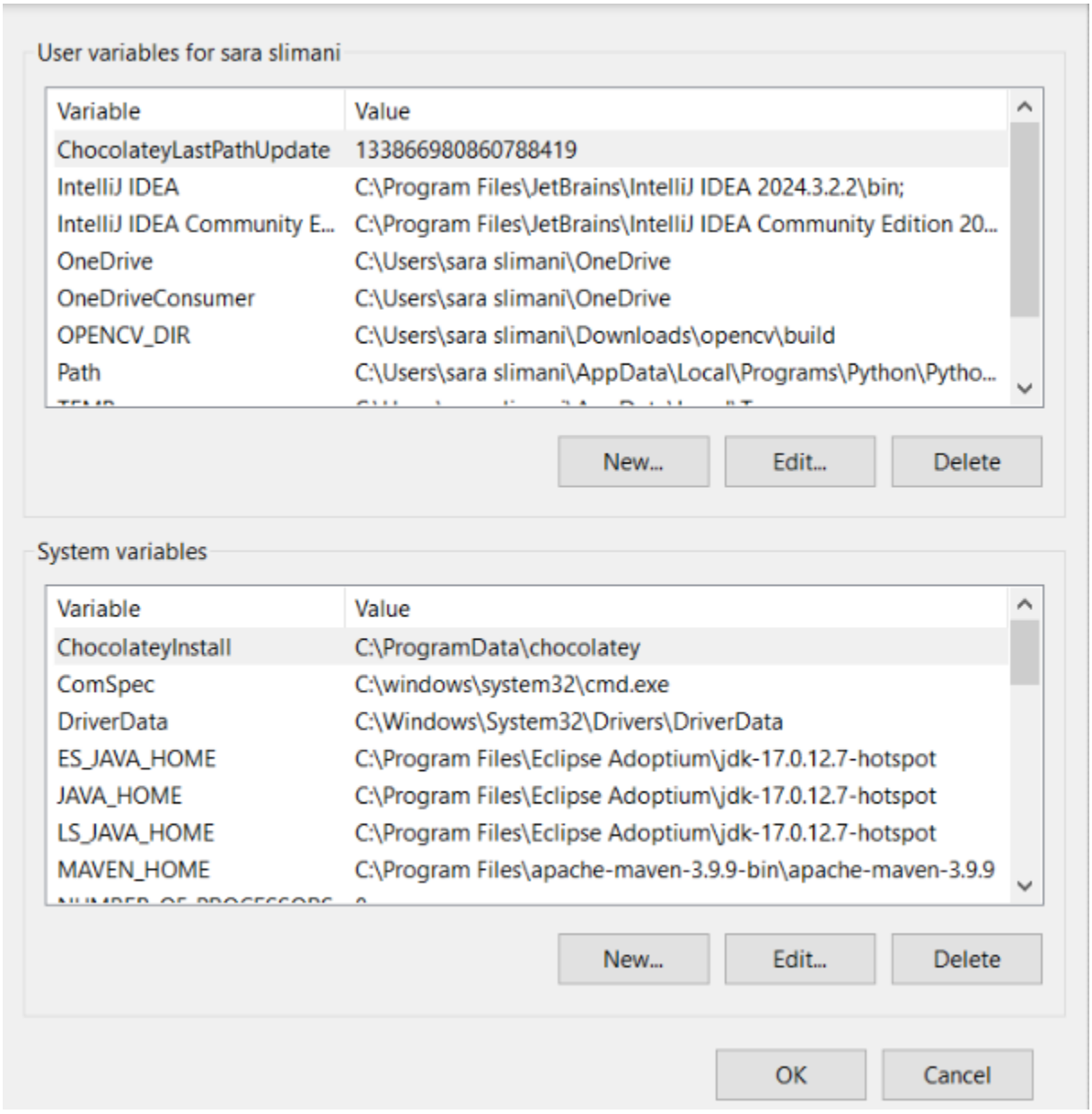
Configuration requise

- JDK 17 (utilisé par Elasticsearch et Logstash)
- Accès administrateur pour les variables d'environnement

Configuration des variables d'environnement

Ajoutez les variables système suivantes :

Nom	Valeur
ES_JAVA_HOME	Chemin vers ton jdk\jdk-17.0.12.7-hotspot
LS_JAVA_HOME JAVA_HOME	chemin vers ton jdk \jdk-17.0.12.7-hotspot chemin vers ton jdk \jdk-17.0.12.7-hotspot


User variables for sara slimani
Variable
Value
ChocolateyLastPathUpdate
133866980860788419
IntelliJ IDEA
C:\Program Files\JetBrains\IntelliJ IDEA 2024.3.2.2\bin;
IntelliJ IDEA Community E...
C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 20...
OneDrive
C:\Users\sara slimani\OneDrive
OneDriveConsumer
C:\Users\sara slimani\OneDrive
OPENCV_DIR
C:\Users\sara slimani\Downloads\opencv\build
Path
C:\Users\sara slimani\AppData\Local\Programs\Python\Pytho...
New...
Edit...
Delete
System variables
Variable
Value
ChocolateyInstall
C:\ProgramData\chocolatey
ComSpec
C:\windows\system32\cmd.exe
DriverData
C:\Windows\System32\Drivers\DriverData
ES_JAVA_HOME
C:\Program Files\Eclipse Adoptium\jdk-17.0.12.7-hotspot
JAVA_HOME
C:\Program Files\Eclipse Adoptium\jdk-17.0.12.7-hotspot
LS_JAVA_HOME
C:\Program Files\Eclipse Adoptium\jdk-17.0.12.7-hotspot
MAVEN_HOME
C:\Program Files\apache-maven-3.9.9-bin\apache-maven-3.9.9
New...
Edit...
Delete
OK
Cancel

Structure des fichiers de configuration

1. Filebeat (`filebeat.yml`)

- Lit les fichiers JSON de logs depuis `C:\Users\sara slimani\ELK\logs\*.json`
- Envoie les logs vers Logstash sur `localhost:5044`
- Ajoute des métadonnées (host, Docker, Kubernetes)

2. Elasticsearch (`elasticsearch.yml`)

- Sécurité activée avec SSL désactivé pour le développement
- Hébergé sur `localhost:9200`
- Utilise un JDK externe (non embarqué)

3. Logstash (`pipeline.conf`)

- Reçoit les logs de Filebeat sur le port `5044`
- Parse les logs JSON et extrait les champs métiers :
  - `transaction_id`
  - `auth_step`
  - `response_time`
  - `operation_code`
  - `bank`, `product`, etc.
- Calcule les durées entre étapes d'authentification
- Détecte les erreurs (`TIME_OUT`, `NOT_AUTHENTICATED`)
- Envoie les données vers Elasticsearch

4. Kibana (`kibana.yml`)

- Connecté à Elasticsearch via `https://localhost:9200`
- Hébergé sur `localhost:5601`
- Utilise un token de service pour l'authentification

Démarrage des services

Elasticsearch

cd **[chemin vers ton dossier]** \elasticsearch-8.11.4\bin

elasticsearch.bat

Logstash

renommer le fichier jdk qui se trouve dans “[chemin vers ton dossier]\logstash-8.11.4\jdk” avec un autre nom

Créer un dfichier “pipline.conf “ dans le chemin “[chemin vers ton dossier] \logstash-8.11.4\config\pipeline.conf”

cd **[chemin vers ton dossier]** \logstash-8.11.4\bin

logstash.bat -f "C:\Users\sara slimani\ELK\logstash-8.11.4\config\pipeline.conf"

Kibana

cd **[chemin vers ton dossier]** \kibana-8.11.4\bin

kibana.bat

Filebeat

cd **[chemin vers ton dossier]** \filebeat-8.11.4-windows-x86_64

filebeat.exe -e