

PRESENTATION DE L'ETAT D'AVANCEMENT PROJET

Nom du projet : Analyse des logs et troubleshooting

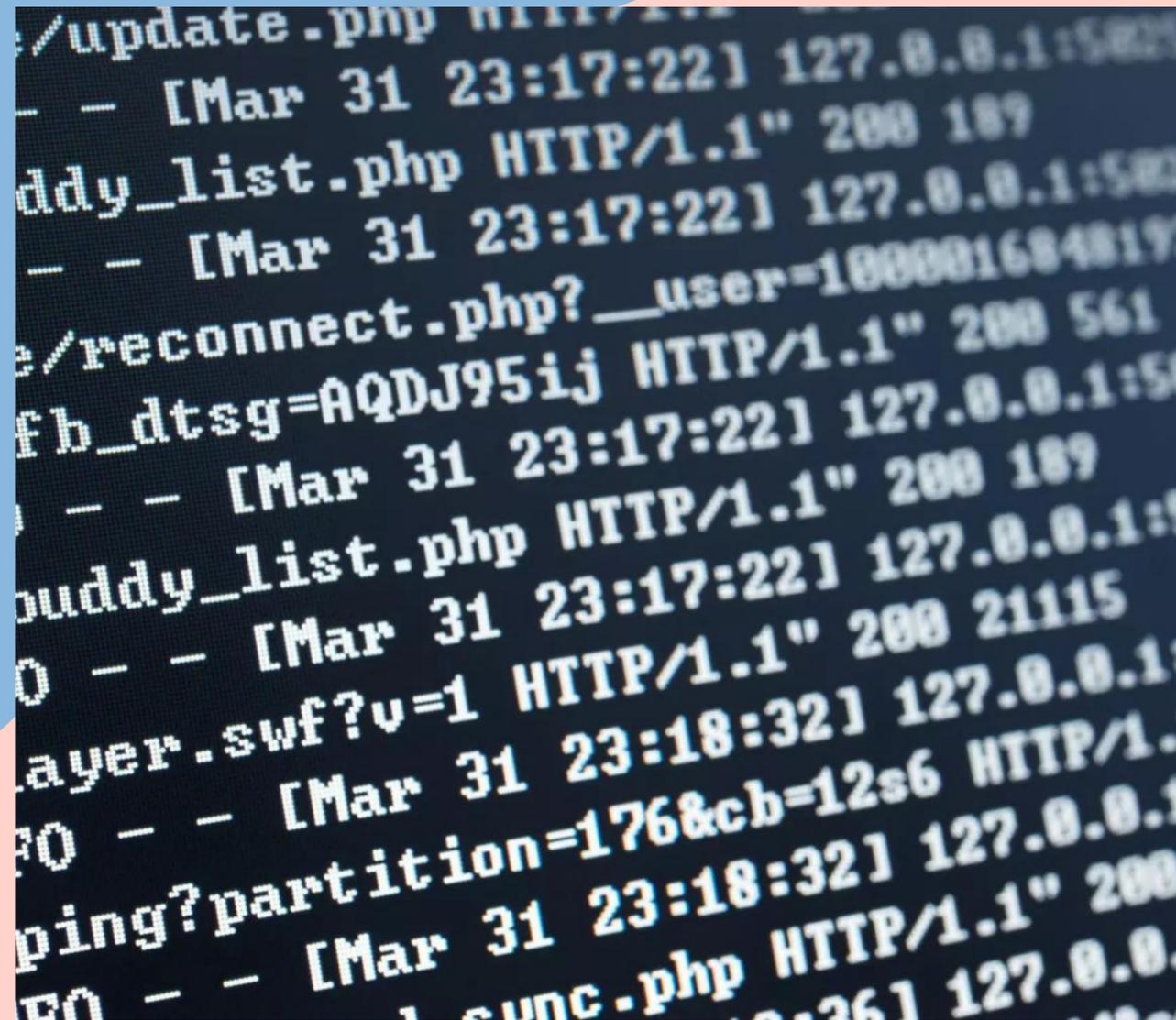
Présenté par : Oumayma Lyna Khaznaji

Date : 7 juillet 2022

SOMMAIRE

- C'est quoi un log ?
- Qu'est ce qu'un analyse des logs ?
- Quel logiciel pour analyser les fichiers logs ?
- Qu'est ce que c'est ELK? ?
- Configuration de ELK
- C'est quoi un troubleshooting ?
- Quel logiciel pour le troubleshooting ?
- Qu'est ce qu c'est APM?
- Configuration de l'APM

C'EST QUOI UN LOG ?



```
update.php HTTP/1.1" 200 189  
- - [Mar 31 23:17:22] 127.0.0.1:5827  
buddy_list.php HTTP/1.1" 200 189  
- - [Mar 31 23:17:22] 127.0.0.1:5827  
reconnect.php?__user=188881684817  
fb_dtsg=AQDJ95ij HTTP/1.1" 200 561  
- - [Mar 31 23:17:22] 127.0.0.1:5827  
buddy_list.php HTTP/1.1" 200 189  
- - [Mar 31 23:17:22] 127.0.0.1:5827  
layer.swf?v=1 HTTP/1.1" 200 21115  
- - [Mar 31 23:18:32] 127.0.0.1:5827  
ping?partition=176&cb=12s6 HTTP/1.1  
- - [Mar 31 23:18:32] 127.0.0.1:5827  
unc.php HTTP/1.1" 200  
- - [Mar 31 23:18:32] 127.0.0.1:5827
```

Dans le domaine informatique, le terme log désigne un type de fichier, ou une entité équivalente, dont la mission principale consiste à stocker un historique des événements

QU'EST CE QU'UN ANALYSE DES LOGS ?

L'analyse des fichiers log est l'évaluation d'un ensemble d'informations enregistrées à partir d'un ou plusieurs événements intervenus sur un environnement IT.

Cette pratique peut être utilisée pour :

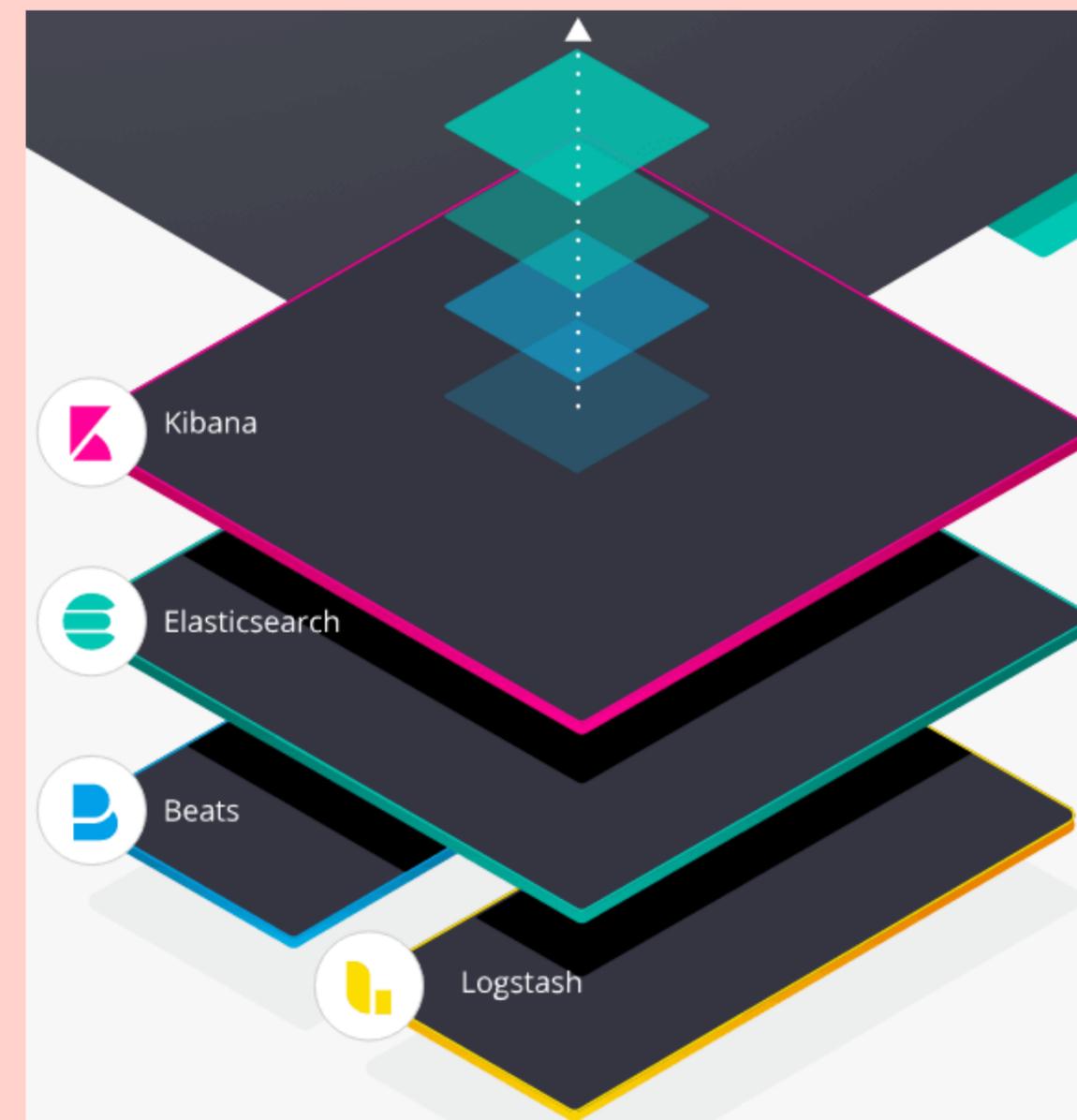
- Analyser le comportement utilisateur et identifier des modèles de comportement
- Identifier et anticiper des incidents
- Être conforme à la réglementation en place
- Anticiper et planifier les capacités de l'environnement IT

Analyser des logs est un véritable challenge et demande un travail fastidieux pour les équipes IT en raison de la volumétrie, mais aussi de la diversité des types de logs, ainsi que les formats propriétaires, les architectures élastiques, etc.

QUEL LOGICIEL POUR ANALYSER LES FICHIERS LOGS ?

Après une étude comparative des différents logiciels open source présents dans le marché , on a choisi d'utiliser le projet ELK

- Elasticsearch
- Kibana
- Logstash



QU'EST CE QUE C'EST ELK? ?

**"ELK" est un acronyme pour trois projets en open source :
Elasticsearch, Logstash et Kibana.**

Elasticsearch est un moteur de recherche et d'analyse.

Logstash destiné au traitement des données .

**Kibana permet aux utilisateurs de visualiser des données avec
des tableaux et des graphes dans Elasticsearch.**

CONFIGURATION DE ELK

Configuration de Logstash

On a configure logstash en utilisant la methode de Groking pour specifier l'index pattern .

```
start_position => "beginning"
}
}
filter{
  grok {
    match => {
      "message" => "(?<timestamp>%{MONTH} %{MONTHDAY}, %{YEAR} %{HOUR}:?%{MINUTE}(?:?%{SECOND})) " }
    }

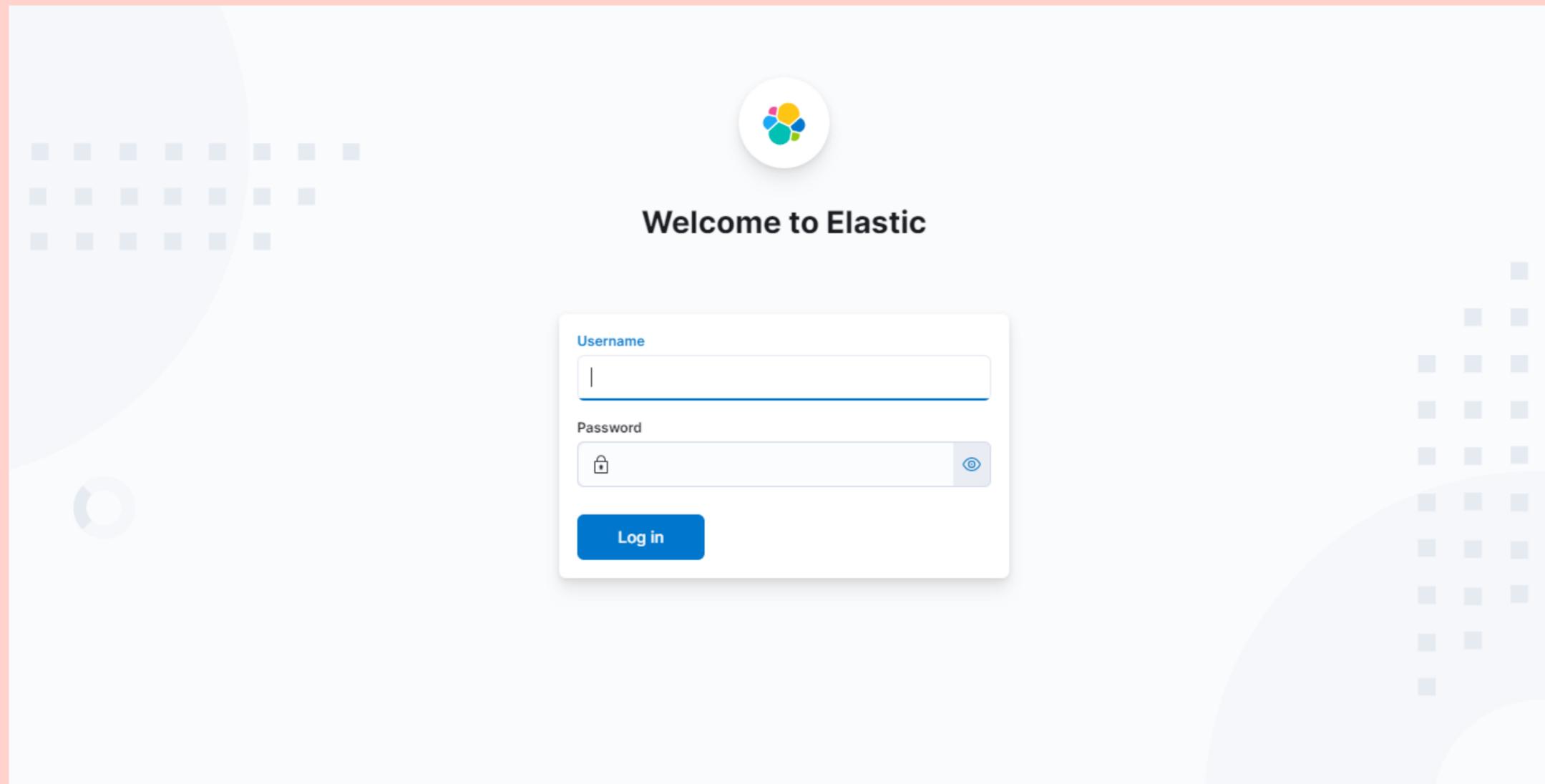
    grok {
      match => {
        "message" => "%{LOGLEVEL:level} \|%{GREEDYDATA:thread} \|%{GREEDYDATA:Msg2}%{SPACE}\| \| %{SPACE}%{GREEDYDATA:user}\|%{GREEDYDATA:message}\|"
      }
    }
  }
}

output {
  elasticsearch
```

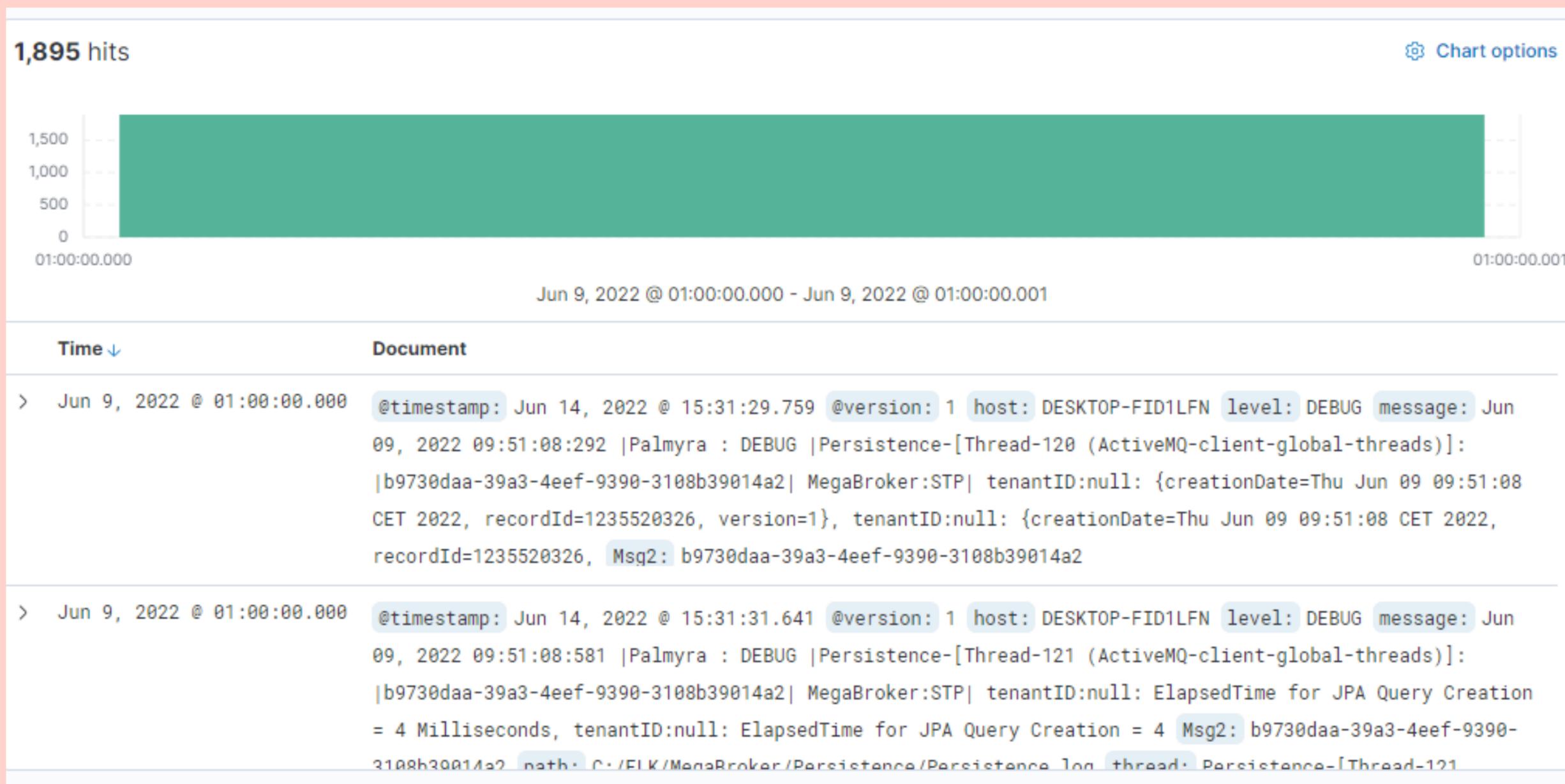
CONFIGURATION DE ELK

Configuration de Kibana

Ajout d'authentification a kibana



Ajout des champs "timestamp", "version", "host", "level", "message", "msg2", "image", "screenrecord":



C'EST QUOI UN TROUBLESHOOTING ?

Le troubleshooting (ou dépannage) est un processus de recherche logique et systématique de résolution de problèmes concernant des machines complexes, de l'électronique, des ordinateurs et des systèmes logiciels. Le troubleshooting consiste en une recherche de la source d'un problème afin d'en identifier les symptômes et en éliminer les causes potentielles, jusqu'à sa résolution.

QUEL LOGICIEL POUR LE TROUBLESHOOTING ?

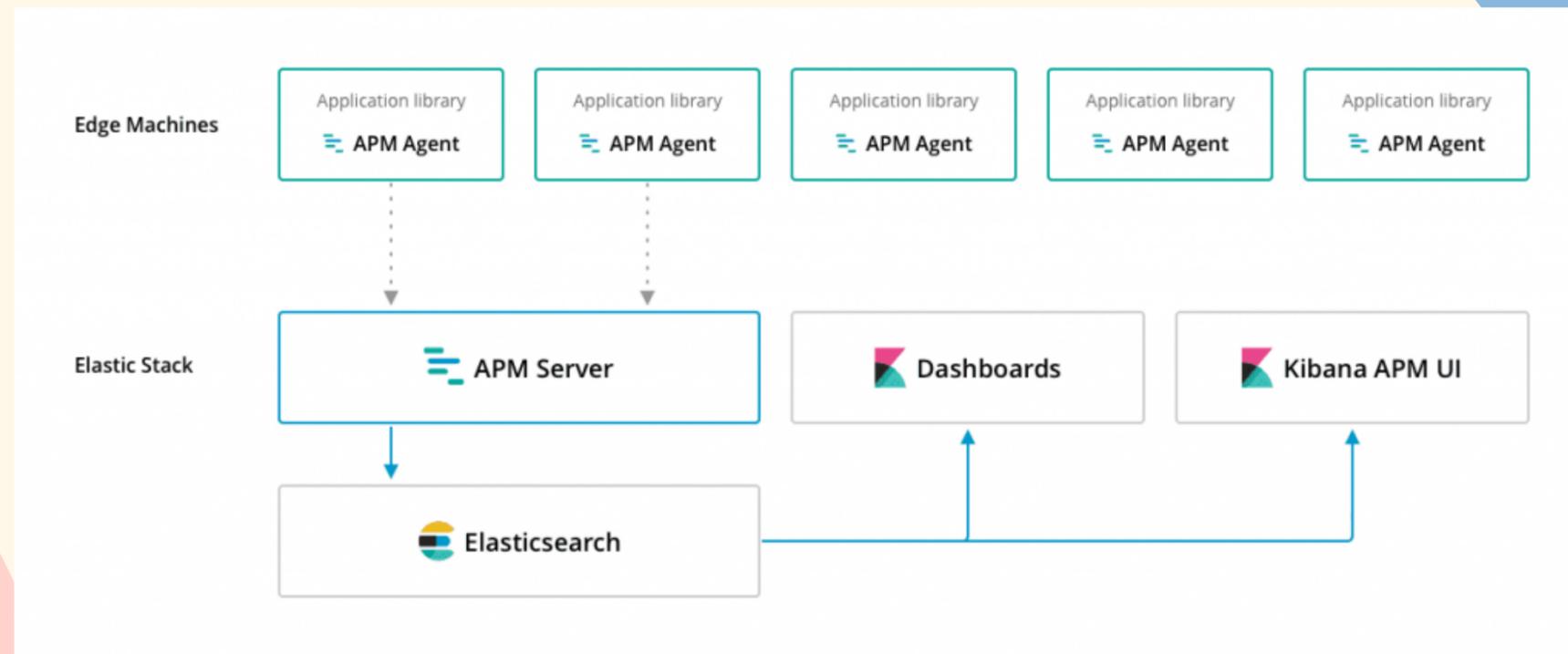


Elastic APM

Après une étude comparative des différents logiciels open source présents dans le marché , on a choisi d'utiliser Elastic APM

C'EST QUOI ELASTIC APM ?

APM nous permet d'observer le fonctionnement de nos applications à tous les niveaux. Grâce aux intégrations de machine learning et d'alerting, et à sa puissance de recherche, Elastic APM rend l'infrastructure de vos applications plus transparente. Cette solution permet de visualiser les transactions, les traces, les erreurs et les exceptions, le tout à partir d'une interface utilisateur d'APM conçue avec soin. Même lorsque nous n'avons pas de problèmes à résoudre, nous pouvons exploiter les données d'Elastic APM pour classer les correctifs par ordre de priorité, optimiser les performances de nos applications et éviter les goulets d'étranglement



CONFIGURATION DE L'APM

Création d'une application Java est capable de gérer les logs .

```
18  */
19  public class Test {
20
21      /**
22       * @param args the command line arguments
23       */
24
25      public static void main(String[] args) throws IOException {
26
27          BufferedReader in = new BufferedReader(new FileReader("C:\\elastik_stack\\MegaBroker\\Persistence\\Persistence.log-2"));
28          String line = in.readLine();
29          while(line != null)
30          {
31              System.out.println(line);
32          }
33      }
34  }
```

Output - test (run)

```
Jun 07, 2022 21:48:36:939 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: Count query : : ( select count(T.version) from config_PalmyraProperty T )
with params ( [] ).
Jun 07, 2022 21:48:36:939 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: ElapsedTime for JPA Query Creation = 2 Milliseconds
Jun 07, 2022 21:48:36:942 |Palmyra : TRACE |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: ElapsedTime for Query Execution 1 milliseconds.
Jun 07, 2022 21:49:36:945 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: //////////////////////////////////////
Jun 07, 2022 21:49:36:948 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: Find query : : ( select T.type , T.propertyName , T.creationDate , T.creatorUserId , T.updateDate , T.updatorUserId , T.version , T.propertyValue from config_PalmyraProperty T order by T.propertyName ASC )
with params ( [] ).
Jun 07, 2022 21:49:36:949 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: ElapsedTime for JPA Query Creation = 3 Milliseconds
Jun 07, 2022 21:49:36:952 |Palmyra : TRACE |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: ElapsedTime for Query Execution 3 milliseconds.
Jun 07, 2022 21:49:36:955 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: //////////////////////////////////////
Jun 07, 2022 21:49:36:957 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: Count query : : ( select count(T.version) from config_PalmyraProperty T )
with params ( [] ).
Jun 07, 2022 21:49:36:958 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: ElapsedTime for JPA Query Creation = 3 Milliseconds
Jun 07, 2022 21:49:36:961 |Palmyra : TRACE |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: ElapsedTime for Query Execution 2 milliseconds.
Jun 07, 2022 21:49:36:963 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: //////////////////////////////////////
Jun 07, 2022 21:49:36:965 |Palmyra : DEBUG |Persistence-[pollingConfigurationSource]: |38c9a61d-fad5-465b-a8c7-3686d9d543c9| MegaBroker:admin| tenantID:null: Count query : : ( select count(T.version) from config_PalmyraProperty T )
```

CONFIGURATION DE L'ELASTIC APM AVEC L'APPLICATION JAVA

```
/Desktop/test/elastic-apm-agent.jar -Delastic.apm.service_name=my-application -Delastic.apm.server_
tion_packages=org.example -jar C:/Users/DELL/Desktop/test/dist/test.jar
```

MERCI DE VOTRE
ATTENTION !