

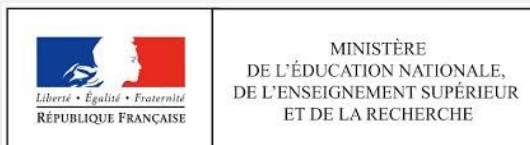
J-EOLE

14-15 Juin 2016

Gestion des logs (hackathon EOLE 2015)

Joël Cuissinat

CC BY-NC-SA 2.0 FR



Gestion des logs



Hackathon EOLE :

- Les 24, 25 et 26 novembre 2015
- Organisateurs PCLL du MEN, MEDDE et société Cadoles
- Une trentaine de participants

Gestion des logs

6 groupes de travail :

- étude et intégration d'un AD sur Eolebase
- étude de logiciels libres pour l'instrumentation
- écriture de documentation
- nouvelles techno et nouvelles interfaces
- journaux systèmes
- EOLE SaaS

Gestion des logs

Groupe de travail journaux systèmes

Objectif : mettre en place un serveur
concentrateur et consolidateur de log

Gestion des logs

Composants logiciels :

- Rsyslog client et serveur : transfert et centralisation de journaux d'événements

Gestion des logs

Composants logiciels :

- Logstash : outil de collecte et de traitement des logs (ETL)

Gestion des logs

Composants logiciels :

- Elasticsearch : stockage de données et moteur de recherche basé sur la bibliothèque d'indexation Apache Lucene

Gestion des logs

Composants logiciels :

- Kibana : plugin de visualisation pour le moteur de recherche Elasticsearch

Gestion des logs

Architecture testée

- Serveur Amon avec Logstash-forwarder
- Serveur Eolebase avec Logstash et Elasticsearch
- Serveur Eolebase avec Kibana et NGINX

Gestion des logs

Difficultés rencontrées :

- Composant Shield (sécurisation de l'interface Kibana) payant
- Utilisation de NGINX pour l'authentification

Gestion des logs

Difficultés rencontrées :

- Création de tableaux de bord Kibana complexe du fait du nombre d'information disponible
 - Pré-traiter les logs en amont au maximum
 - Avoir une idée précise des résultats souhaités

Gestion des logs

Difficultés rencontrées :

- Compréhension et prise en main du langage de parsing GROK
 - Utilisation de grok debugger

Gestion des logs

Difficultés rencontrées :

- Écroulement de la chaîne en cas de sollicitation intensive
- Nécessité d'une brique intermédiaire pour absorber le trafic (Redis, Riak, ...)

Gestion des logs

Résultats de l'atelier

- Mise en place d'une maquette fonctionnelle
- Rédaction d'un tutoriel d'installation de la chaîne Elasticsearch sur Eolebase
- Créolisation partielle des briques utilisées

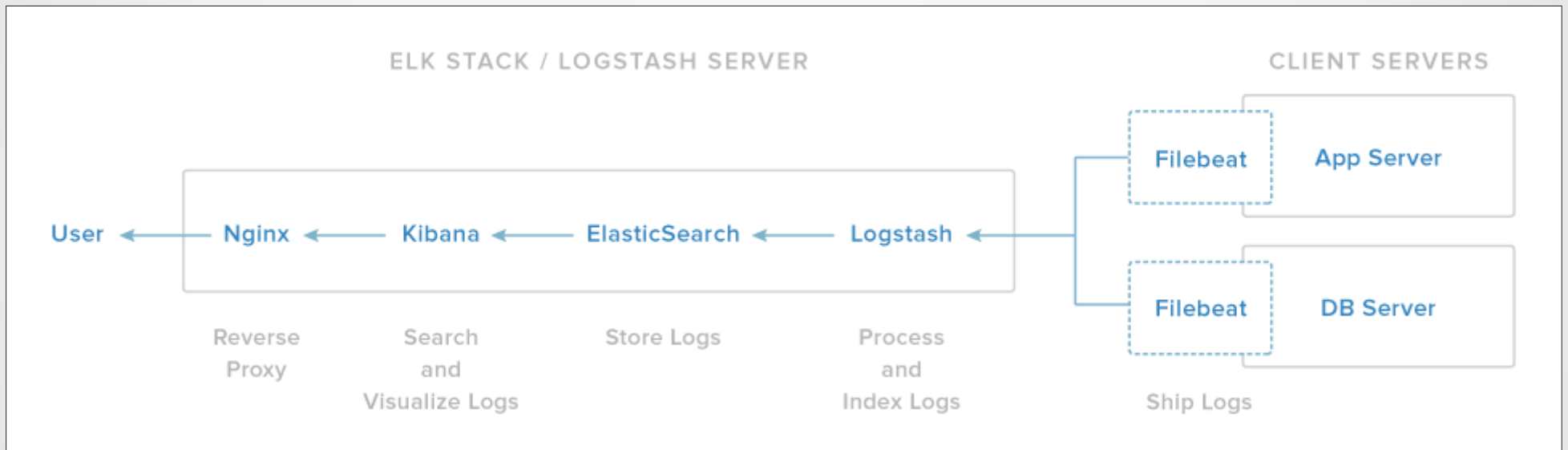
Gestion des logs

Perspectives

- Packaging debian des différents composants
- Reprise des travaux autour de « Zéphirlog »
- Évaluation d'autres architectures
- Logstash-forwarder vs Filebeat

Gestion des logs

Quelques illustrations...



Source : <https://assets.digitalocean.com/articles/elk/elk-infrastructure.png>

Gestion des logs

The screenshot displays the Kibana interface for log management. At the top, the Kibana logo and navigation tabs (Discover, Visualize, Dashboard, Settings) are visible. A search bar is present with the text "Search...". The main content area shows a histogram titled "November 3rd 2013, 17:00:00.000 - November 10th 2013, 15:00:00.000 - by @journeystart". The histogram shows the count of events over time, with the y-axis labeled "Count" ranging from 0 to 50k. Below the histogram is a "Documents Table" showing search results. The table has columns for "Time" and "_source". The first document shows a search result for "November 10th 2013, 15:00:00.000" with fields like "ZVPPT", "DFare", "ExTime", "EXTIMEHMM", "FFare", "EndStation", "DailyCapping", "StartSta", "JNYTYP", "downo", "#journeystart", "EntTimeHMM", "daytype", "SubSystem", "LTS", "RouteID", "FinalProduct", "Freedom Pass (Disabled)", "EntTimeHH", "EntTime", "1380", "EXTIMEHH", "00", and "_source". The second document shows a search result for "November 10th 2013, 15:00:00.000" with fields like "ZVPPT", "DFare", "ExTime", "EXTIMEHMM", "FFare", "exitLoc", "51.5173512308", "-0.0829657094569", "EndStation", "Liverpool Street", "DailyCapping", "N", "StartSta", "Newbury Park", "JNYTYP", "MIX", "downo", "1", "#journeystart", "November 10th 2013, 15:00:00.000", "EntTimeHMM", "23:00", "daytype", "Sun", "SubSystem", "LUL", "RouteID", "XX", "FinalProduct", "LUL Travelcard-7 Day", "EntTimeHH", "23", "EntTime", "1380", "exitLoc", "ocovn4", "EXTIMEHH", "23", "enterLoc", "51.5755724936.0.0903373136813". The third document shows a search result for "November 10th 2013, 15:00:00.000" with fields like "ZVPPT", "DFare", "ExTime", "EXTIMEHMM", "FFare", and "EndStation".

Labels on the right side of the image indicate the following components:

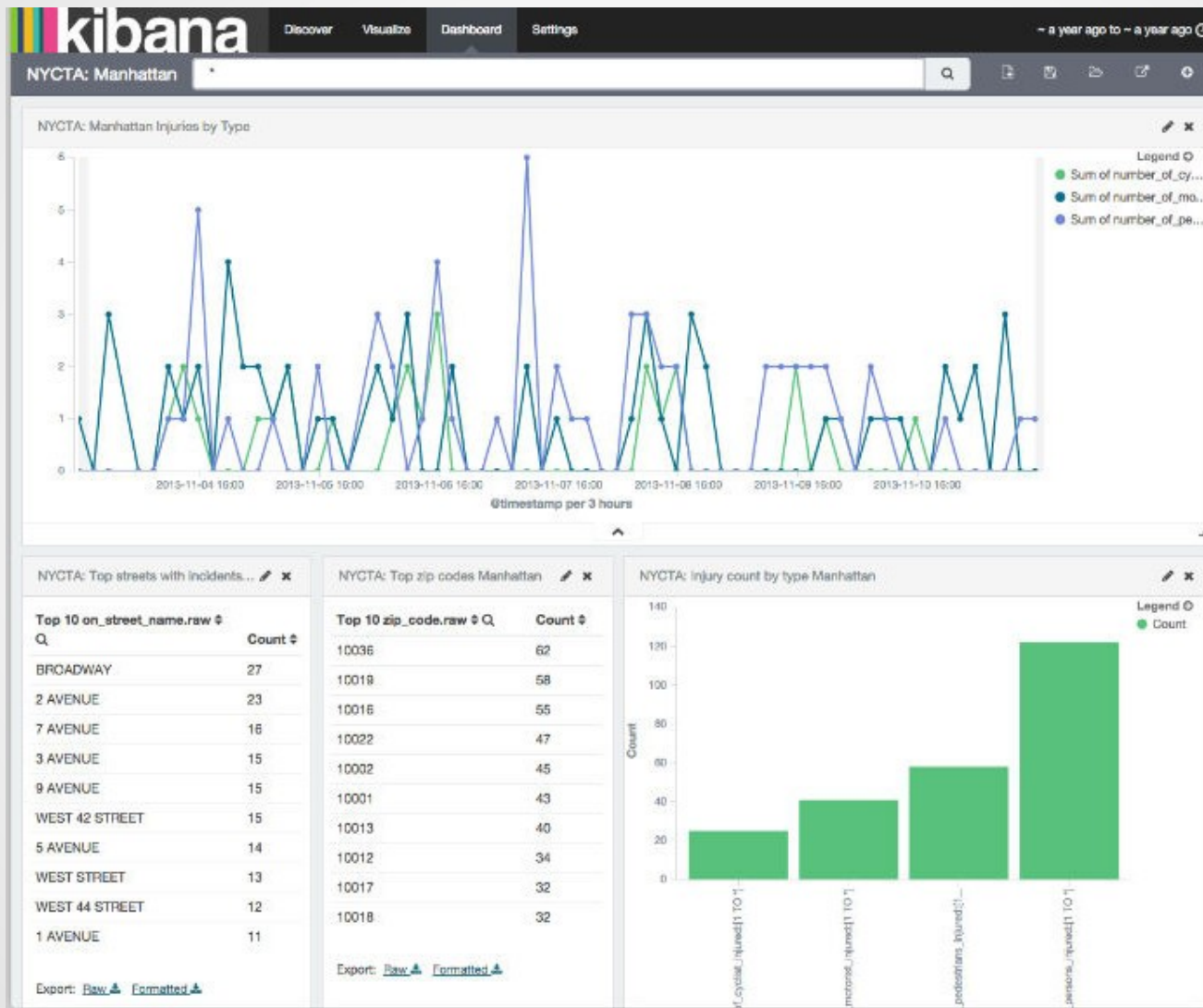
- Time Filter
- Total Hits
- Histogram
- Documents Table

Labels on the left side of the image indicate the following components:

- Toolbar
- Index Pattern
- Fields List

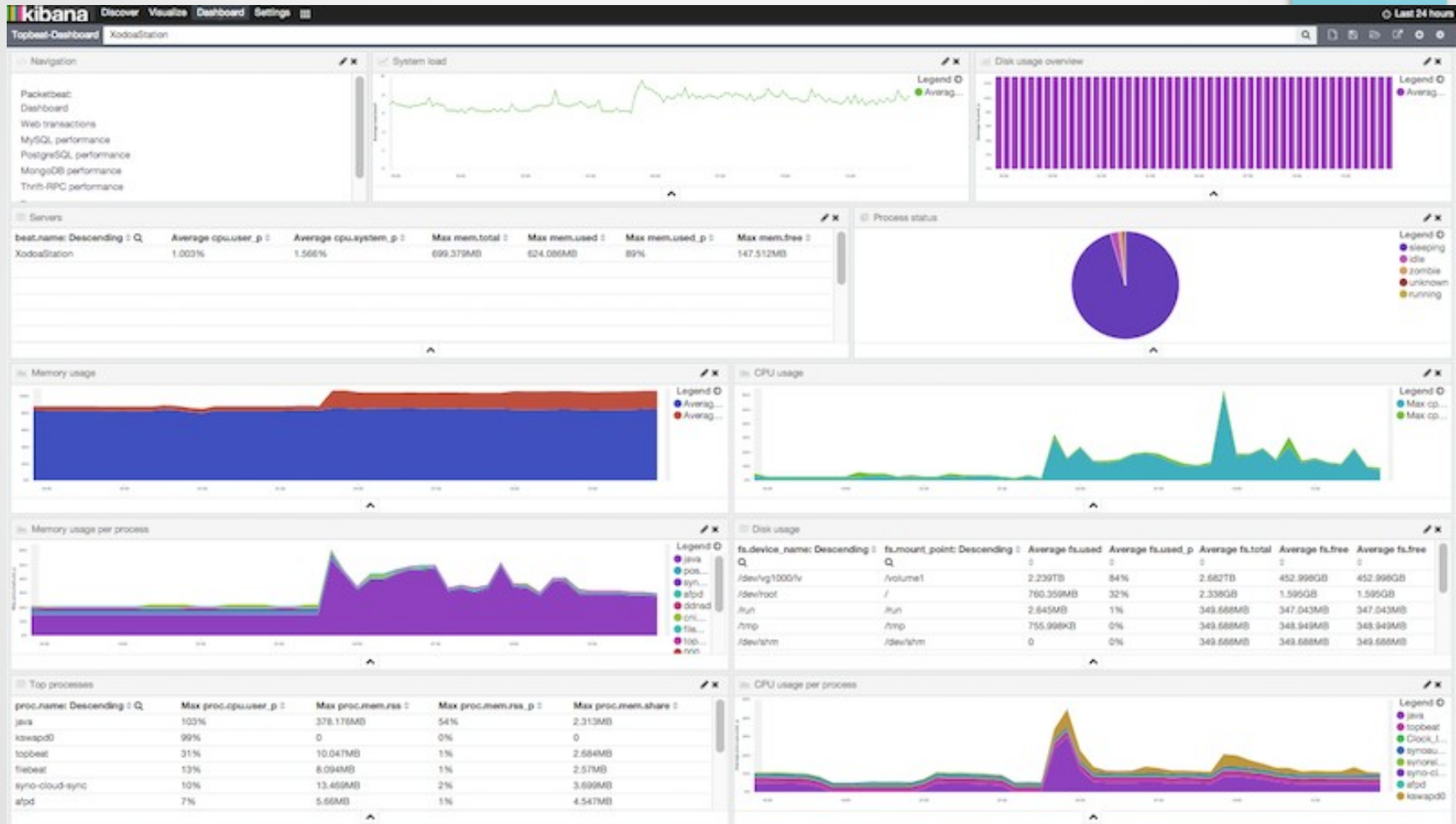
Source : <https://www.elastic.co/guide/en/kibana>

Gestion des logs



Source : <https://www.elastic.co/guide/en/kibana>

Gestion des logs



Source : <https://www.elastic.co/guide/en/kibana>

Licence

Cette présentation est mise à disposition sous licence
Creative Commons by-nc-sa 2.0-fr

Attribution

Partage dans les mêmes conditions

Pas d'utilisation commerciale

France

Vous pouvez obtenir une copie de la licence :

– Par internet :

<https://creativecommons.org/licenses/by-nc-sa/2.0/fr/>

– Par courrier postal : Creative Commons, 444 Castro Street,
Suite 900 Mountain View, California, 94041, USA