haute école neuchâtel berne jura arc ingénierie www.he-arc.ch

Hes·so Haute Ecole Spécialisée de Suisse occidentale

Log Analysis

Vincent MOULIN

Bachelor Project 2020
Computer Science – Software and Multimedia Development
Supervisors: Emmanuel DE SALIS, Hatem GHORBEL
Expert: Benjamin HABEGGER

Description

This Bachelor's thesis entitled "Log Analysis" was carried out at the SIX company in Biel/Bienne, which is headquartered in Zurich. SIX is a Swiss financial company. It operates the national stock exchange and also handles government bonds and derivatives such as stock options.

The primary objective of this project was to analyze and evaluate the logs produced by various SIX applications. The aim was to determine whether any logs were missing or incomplete and, if so, to remedy the situation.

Once this had been done using the Splunk tool, which allows the search, the tracking and the analysis of logs, the goal was to represent the logs in the form of dashboards. This allows the detection of a drop in performance, the analysis of the behavior of certain applications and the processes or error detection.

Procedure

Preliminary work:

- Obtaining access rights to software, obtaining the SIX laptop, VPN access, installation of development environment.
- Discovery of work methodology.
- Discovery of new tools (Jira, Jfrog Artifactory, etc.).

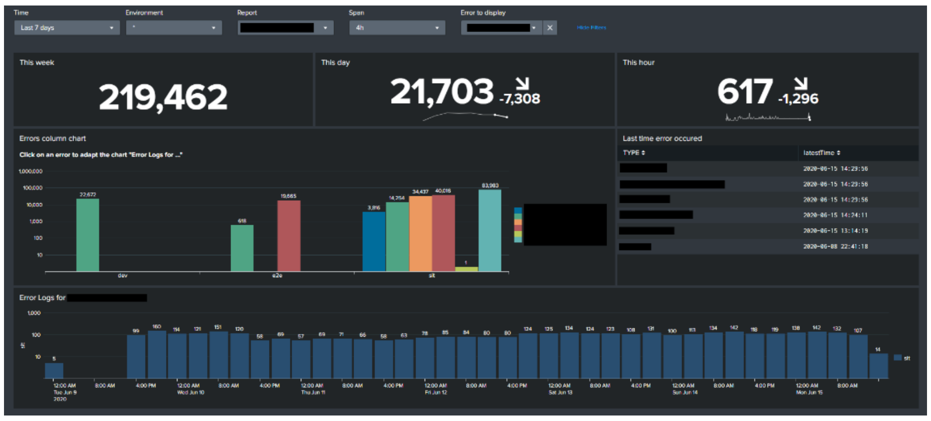
Log Analysis:

- Research phase, state of the art.
- Analysis / adding logs.
- Construction of dashboard.
- Writing documentation.
- Presentation of results / participation in meetings.

Results

The dashboard results are very explicit and clear. With the right choice of graphs and logs, we can easily highlight the important elements.

The dashboards are intuitive and most of them were found to be very interesting by the SIX developers. They will be used in the future to help them detect errors, performance drops or simply to monitor the correct operation.



Time: Last 7 days
Environment: *
Report: [redacted]
Span: 4h
Error to display: [redacted]

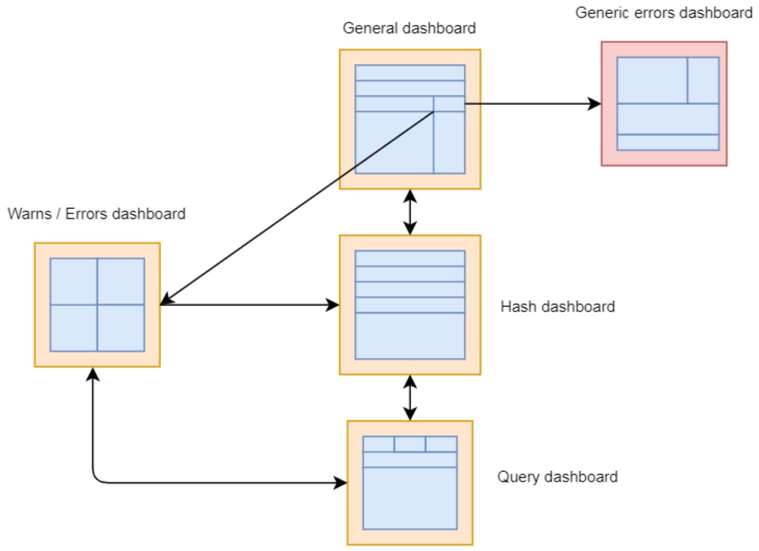
This week: 219,462
This day: 21,703 -7,308
This hour: 617 -1,296

Last time error occured

TYPE	latestTime
[redacted]	2020-06-15 14:29:56
[redacted]	2020-06-15 14:29:56
[redacted]	2020-06-15 14:29:56
[redacted]	2020-06-15 14:24:11
[redacted]	2020-06-15 13:14:19
[redacted]	2020-06-08 22:41:18

Error Logs for [redacted]

Example of one of the dashboard



General dashboard
Generic errors dashboard
Warns / Errors dashboard
Hash dashboard
Query dashboard

Diagram of navigation between some of the dashboards

Perspectives

Log analysis and dashboard creation has been documented. It is therefore easy to maintain and improve them based on that documentation. The dashboards have been built in such a way that maintenance is as simple as possible. Some dashboards common to logs from different applications have been made in a generic way and can therefore be upgraded. SIX employees will use these dashboards.