The Benefits of Logging and a Look into Fluentd

Benjamin Moeller
EECS 465
University of Kansas

5/1/2022

1 Introduction

With all of the different types of data that can come from a variety of sources, it is in today's market to have a unified logging layer to sort and export all these different data sources. On the market, some of the tools that can accomplish this tend to be on the expensive side, but there are also open source tools that work to compete with these tools. One such tool is Fluentd, which is an unified logging layer that is comparable to Logstash, another popular logging tool. Both of these tools can be connected to Kibana and the Elastic Stack, making them powerful logging tools when used correctly. The rest of the paper is structured as follows. The next section gives the motivation as to why logging tools are important. Section 3 goes into more detail on how fluentd works under the hood, and also gives some use cases. Section 4 gives a comparison between the two popular logging layer tools, Logstash and Fluentd, as well as discuss how both connect the the ELK Stack. Section 5 will give a demo on how to utilize Fluentd in different logging scenarios, and then section 6 will conclude the paper.

2 Motivation

Logging tools are important due to the structure and organization they can provide to data on a day to day basis. For example, if a company has multiple machines running applications and other programs, it would be nice to have all the log data of all the machines centralized in a single logging server. Tools like fluentd can do this, as they provide features for listening and filtering logs as they are created (more on how this works in the next section). In short, there are a variety of different logging tools out that have different functionalities and purposes. The two tools that will be discussed in this paper, Fluentd and Logstash, are known for their ability to be unified logging layers that can listen for and send data to a variety of destinations. Organization can be key when it comes to security and other subjects, as there are some things that can only be seen when data has been brought together into one place and compared.

3 How Fluentd Works

At its most basic level, Fluentd is an unified logging layer that can take input from many dif-

ferent data sources and route them to different sources depending on how a fluentd configuration file is formatted. Below is a chart from the Fluentd website that shows how different data sources can be mapped.

4 Fluentd and the EFK Stack

5 Fluentd demo

6 Conclusion