Application Performance Monitoring Using Log File on ELK Stack

Ashwinikumar Tiwari[1], Dashrath Mane[2]

[1]PG Student, Department of MCA, Vivekanand Education Society's Institute of Technology, Mumbai, India
[2]Assistant Professor, Department of MCA, Vivekanand Education Society's Institute of Technology, Mumbai, India

---

Abstract: *Log monitoring of an application is an important step to manage any of the applications. Details related to the application state and situation can be collected with the help of device monitoring for the developers to give decisions related to appeared events. Logs of application can be important information to track application thoroughly. Developer needs to centralize the logs of the application so that the developer can manage, receive and analyze the logs. APM agent is used for tracking the application using specific language like ELK provides java APM agent for monitoring. The further step of this is the creation of software and the application. The last procedure is the testing of the system and managing the log of application. The output shows that collecting the logs and processing that logs into the information on the ELK dashboards utilizing ELK application effectively implemented. The dashboard came about by ELK Application will be created on the application utilizing Java language. The test outcomes show that the framework can get logs and based on that log file it will help to understand the efficiency and performance of product application.*

Keywords — Monitoring; log; ELK Stack; Java; APM Agent; Kibana; Logstash

1. INTRODUCTION

Application performance monitoring APM is the branch of information technology that guarantees systems are proceeding true to form. Application monitoring systems and tools of ELK stack keep up the application checking. The final aim of the performance monitoring of software is to provide good quality experience to end user. Application observing systems provide developers the data they have to rapidly discover the issues that seriously influence an application's performance [1].

These types of systems could be concrete to the selected software application and monitor various applications on the network, grouping information concerning customer CPU utilization memory required yield information and total bandwidth.when user perform the troubleshooting the performance issues we see a service or operation that is or a many of the machines that are eased back down and arriving at high-CPU usage. This may imply that it's less number of resources because of high burden of resources, but most of the time means that there is high chance of bugs or error in the coding part, or there might be error that uses high CPU utilization [9].

ELK Stack is the open source application which is the combination of Elasticsearch Logstash and Kibana to gather and envision or visualize logs of any application [2]. Elasticsearch is utilized for storing all the logs generated from various network devices. Logstash is the open source tool for gathering and parsing the logs and saving at the Elasticsearch. Kibana is the user interface which is used for visualizing logs in the graphical or in other visualization structure form. [3].

In this paper, developer need to develop the Application Performance Monitoring (APM) by using the java APM agent that involves the log file of the application or any project that will manage and represent the application based on the ELK Stack to combine various logs from server of the project that is used by developer and analyze data form the every log file of application to provide administrator to provide solution based on the error occurred in the application.[4]

2. RESEARCH METHODOLOGY

Research methodology process definition, specifications and configuration of system, log evaluation, and results dependent on log records.

The first step of this research is the definition of system. This step characterizes the system that will be made that include the system definition, recognizing the requirement of the system and the all components and it also include the reason and advantage of the application, how it performs its operation and the programming language utilized for the APM agents [9].

The subsequent step is definitions of system. The requirement specification process and the definition of the application will be portrayed in the starting system design by finding the specification of the system requirement that will implies the definition of system and requirement of application.

The following stage is configuration of the system. In this step, specification of the predefined requirement will be implemented according to the system or application design and requirement and applied as the progression of application that will help the system to run the application. Logs are collected at different lengths of time.

The last procedure is the assessment and result is the final step. The study will be considered successful if the application has satisfied and fulfilled the aim of the research.

2.1 Requirements of system

System requirement of the application involves the log management application that will collect log activities from system applications using the log file that are generated by the application. Application is built using java and it requires a java agent for APM agent configuration. The system can bunch logs dependent on the seriousness level of the log file. Seriousness levels speak to the earnestness level and significance of a log message. Application also require the server to deploy the application. The last requirement of the system is that it can visualize or envision logs into the data that should be understood by the developer [9].

2.2 Hardware Requirements

Hardware is used for running the application and to support the application to run the system.

TABLE 1. MACHINE SPECIFICATION

Component	Server
Processor	Intel i3, Minimum 1 GHz; Recommended 2GHz or more
RAM	4GB
HDD	100GB

The application is actualized in a machine. It involves the various hardware requirements for running the application. The machine used for the application has the configuration in Table 1.

2.3 Software Requirements

The ELK stack system requires the software to run the Java applications and to create the server and many other helping components. Application used for ELK Stack uses Windows 10 as the operating system. The application or system for gathering the logs uses the Logstash then it can be saved to Elasticsearch and envisioned using the Kibana. Elasticsearch, Logstash and Kibana should be available on the system.

Applications used for monitoring are created using the Java programming language with the help of Eclipse IDE. For accepting the log from application it requires the Java APM agent. Also requires all logs of the application to be stored in the log file. Logstash contains the path of the log file of the application.

Server configuration for the log file is implemented using the application. The Google chrome browser is used by the application that runs on the operating system is the Windows 10 x64 and that is used for running and testing the application. Web browser helps to see all the performance related details on the browser.

2.4 Design of System

Design of systems gives the outline or part of a performance monitoring system of application. Figure 2 displays the design of the system.

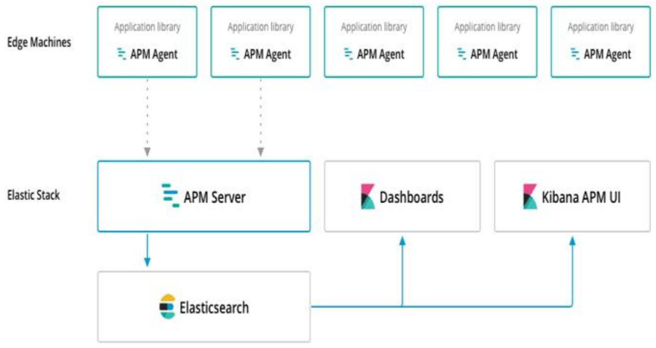


Figure 2. Block Diagram for the System Design Application

2.5 Flow of the System

For collecting the ELK Stash uses Logstash which is the application of a syslog application which gathers all the logs and forwards them to the server which manages logs. The Log gathering is the automatic process; it does not require any agent for the data request. These logs are processed and stored at the Elasticsearch side. [7]

The figure 2 shows the application flow. The APM agent will collect all the information from the running application through the log file. APM server gets the information from the APM agent. Elasticsearch gets the information about the application from an APM server that can be visually represented on Dashboard and Kibana APM UI.

APM agent used for gathering the performance information or data and that will be forwarded to the APM server. For collecting logs applications can use various APM agents. The main responsibility of APM server is to accept the data and use it for creating the documents and finally forwarding the data to Elasticsearch for visualization, storage and analysis [9].

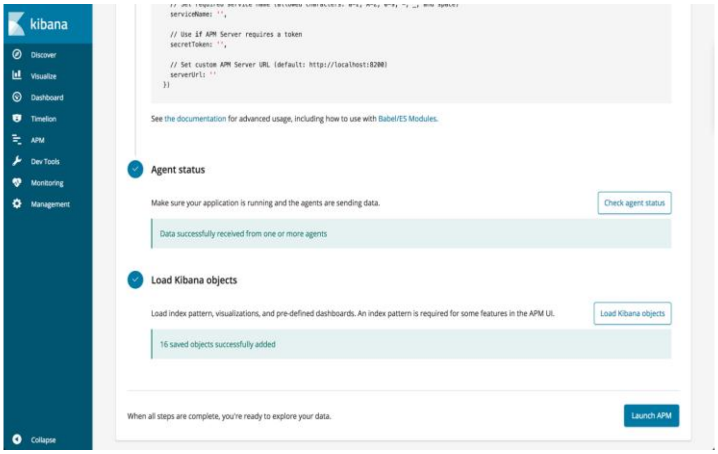
The Elastic APM solution comprises four main open source components: Elasticsearch is used for information storage purpose, Kibana is used for representing and analyzing data into visual form and two main APM components are APM agent and server.

3. RESULTS

Application and system assessment is performed for checking the performance of any software which is implemented. The main goal of the application assessment is to guarantee that the various components of the system are functioning and providing better performance. And the result of log helps to improve system performance and efficiency.

3.1 APM Server Evaluation

This assists to check that the APM agent and APM server are functioning as the user wants. There is an option for loading the Kibana objects at the below of the page. These options are used for loading the index patterns and visualizing the dashboard of ELK Stack (refer figure 3).



```
    serviceName: '',

    // Use if APM Server requires a token
    secretToken: '',

    // Set custom APM Server URL (default: http://localhost:8200)
    serverUrl: ''
  })
```

See the documentation for advanced usage, including how to use with Babel/ES Modules.

Agent status

Make sure your application is running and the agents are sending data.

Data successfully received from one or more agents

Load Kibana objects

Load index pattern, visualizations, and pre-defined dashboards. An index pattern is required for some features in the APM UI.

16 saved objects successfully added

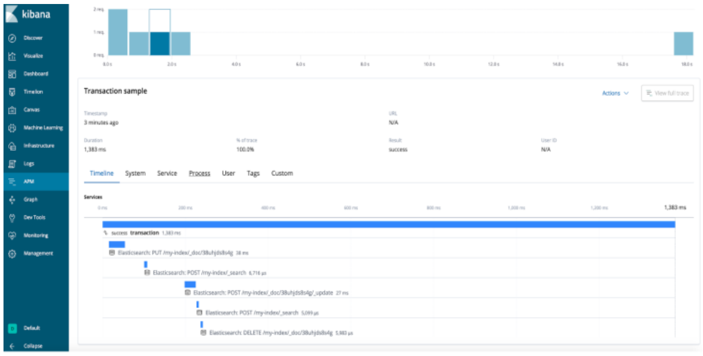
When all steps are complete, you're ready to explore your data.

Figure 3. Loading Agents Status in Kibana for Elastic APM

3.2 APM Server Dashboard Evaluation

It consists of the various operations performed on the application. Figure 4. Display how any database operation is taking time on the application. With the activities it also shows the time taken by that activity so that developers can improve or reduce the operation time [9].

If any error or exception occurred while performing the operation on the application that is also determined by the APM that uses log files. All the results given by the APM server helps to improve the application performance. It also gathers the troubleshooting information of the application. The logging section of the apm-server.yml config file contains various choices for configuration the logging output. Syslog is used for writing logs or rotating log files. Sometimes the output file also used when logging is not configured explicitly.



Transaction sample

Timestamp: 3 minutes ago
URL: N/A
Duration: 1,383 ms
% of trace: 100.0%
Result: success
User ID: N/A

success transaction 1,383 ms
Elasticsearch: PUT /my-index/_doc/38uhjds8s4g 38 ms
Elasticsearch: POST /my-index/_search 6,716 μs
Elasticsearch: POST /my-index/_doc/38uhjds8s4g/_update 27 ms
Elasticsearch: POST /my-index/_search 5,099 μs
Elasticsearch: DELETE /my-index/_doc/38uhjds8s4g 5,983 μs

Figure 4. Details of Operation Performed on Application

3.3 Log Evaluation

The server must have the option to gather and oversee log records of applications while using it. The agent device that will run on various applications are used for collecting logs, that is the process of collecting and managing logs in the application and outputs are used by Elasticsearch application that contains messages and gathering these logs. Based on the logs it will display data on the dashboard (refer figure 4). [8] It classifies these logs into three parts that are transaction, error and metrics. Error tab contains any error occurred while performing the operation in the application. Transaction tabs contain the time taken by database query to execute any operation in the application.

3.4 Application Evaluation

Application assessment and evaluation clarifies the outcomes and presence of the system that has been made. The very initial occurrence of the system is an APM server page that displays the result performed based on the log files.[6] Log files collect the information from the application and that are used by the APM server. APM server dashboard displays data in the various options like transaction, error and metrics. Every menu will explore to the dashboard page as per the menu chosen. The primary page view is displayed in Figure 4.

4. CONCLUSION

To collect the log information or data from devices the log management system or server is used. Logstash application is created successfully for the collection of log files from the system or application. Logs received by the application are gathered into Elasticsearch based on the message produced in the log file. After collecting logs the APM server uses that log for application performance monitoring and improving the performance. A viable APM arrangement causes you to recognize execution and accessibility issues before they sway the end-client. The performance information gathered additionally gives bits of knowledge into how you can improve and keep up client experience and fulfillment. Improvement in application quality makes a superior client experience, yet more gainful business corporations with inner and outside clients. This makes application performance management (APM) a key part of service performance management (SPM).

REFERENCES

[1] ELK to Monitor Performance [Online] Available: https://logz.io/blog/elk-monitor-platform-performance[Accessed:15-June-2020].

[2] C. Preneur, "ELK (ElasticSearch, Logstash, Kibana)," 2020.[Online].https://medium.com/elkelasticsearch - Logstash-kibaa-a48c12612b16. [Accessed: 7-June-2020].

[3] S. Alspaugh et al., "Analyzing Log Analysis: An Empirical Study of User Log Mining This paper is Included in the Proceedings of the Analyzing Log Analysis: An Empirical Study of User Log Mining User surveys," 2014.

[4] Chen-Kun Tsung, Member, IEEE, Chao-Tung Yang, Member, IEEE Visualizing Potential Transportation Demand from ETC Log Analysis Using ELK Stack

[5] Tarun Prakash, Ms. Misha Kakkar, Kritika Patel, Geo-Identification of Web Users through Logs using ELK Stack

[6] Júlia Murínová, Application Log Analysis

[7] APM Server Reference [Online] Available: https://www.elastic.co/guide/en/apm/server/cureNt/index.html [Accessed: 20-June-2020].

[8] ELK Stack: Elasticsearch, Logstash, Kibana | Elastic [Online] Available: https://www.elastic.co/what-is/elk-stack[Accessed:21-June-2020].

[9] Adian F. Rochim, Mukhlish A. Aziz, Adnan Fauzi. "Design Log management System of Computer Network Devices Infrastructures Based on ELK Stack", 2019 International Conference on Electrical Engineering and Computer Science (ICECOS), 2019