LOG FILE ANALYZER

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology

In

Computer Science and Engineering

By

Manish (151340)

Under the supervision of

Mr. Pankaj Anadure

To

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

CERTIFICATE

Candidate's Declaration

We hereby declare that the work presented in this report entitled **"Log File Analyzer"** in partial fulfillment of the requirements for the award of degree of Bachelor of Technology in Computer Science and Engineering submitted in the department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat is an authentic record of my own work carried out over a period from Feb 2019 to till now under the supervision of Mr. Pankaj Anadure**.**

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Manish (151340)

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

Mr. Pankaj Anadure

Dated :

ACKNOWLEDGEMENT

Learning through the project under the guidance of our esteemed mentor Mr. Pankaj Anadure, whose expertise knowledge in the domain of Frontend and Backend Development, not only cleared all our ambiguities but also generated a high level of interest and gusto in the subject. We are truly grateful for his guidance and support throughout the project. We would also like to thank our Head of the Department, Brig(Retd.) SP Ghrera for undying faith in the department of Computer Science and allowing us to join internship program.

The prospect of working in a group with high level of accountability fostered a spirit of teamwork and created a feeling of oneness which thus, expanded our ken, motivated us to perform to the level best of our ability and create a report of the highest quality.

To do the best quality work, with utmost sincerity and precision has been our constant endeavor.

Date: Manish (151340)

TABLE OF CONTENT

LIST OF FIGURES

ABSTRACT

Log analysis is the process of converting your raw or unstructured log files into structured data and then on that structured data making some intelligent decisions. In every field like software testing, the analysis of log files is designed to monitor and check the application performance and work. Also irrespective of just monitoring, logs help to fix some errors in application work. Logs are the unstructured form of text lines which contains systematic information regarding application work and many actions like as – IP Address, date, time, viewed sites, potential domains, status code, components, levels, nodes , the general info about query, loading-time, user-agent, port-number, etc. of various operations that occur in different situations or environments - application itself or the program that runs that application. Logs include the levels of several types of log files such as - INFO, WARNING, FATAL, SEVERE and ERROR.

Logs has a lot of advantages like it helps us to specify who uses system or an application and how likely it is using that application. Moreover, in testing purpose, testers can define or detect whether the session was successful, and to detect errors or mismatches or mistakes an users of the application can face.

Chapter – 1

INTRODUCTION

Log analysis is a kind of process to make sense out of log files or audit trail records or the records generated form computer. The process of creating such records form computer or from application or from any system is called data logging.

Logs are created by different network devices, operating system, various software and applications and all sort of programmable and intelligent device. The message flow from one device to another in chronological order consists of a log file. Logs can be sent to log files and stored on the hard drive or sent as a network flow to the logging memory on the server.

Log messages must usually be interpreted with respect to the internal state of its source (e.g., application) and announce security-relevant or operations-relevant events (e.g., a user login, or a systems error).

Log messages should normally be occurred according to the internal state of the source (e. g., an application) and should report security or business events (e.g system error).

Software developers create logs to help debug the system or to understand how visitors interact with web applications, like as google engines. For example, user authentication for a system can be called as a login, a connection or a login event. Therefore, log analysis should decode messages in the context of the system, manufacturer, application to perform meaningful comparisons with interpret messages from some sources in the event log. The structure of log messages is not always fully documented.

1.1   PROBLEM STATEMENT

This is the project has its motivation from the log files which are cumbersome to read. Log Files contains huge amount of useful information about which must be taken care. This project was created to debug an application or to understand it as follows how users interact with the system. The general purpose of this study is to create and develop a model or application for processing of log files.

The key points to include in this project :

- proper definition of a log file.

- Define structure and syntax for a log file.

- Define a language for efficient and simple protocol for analysis

- Build basic REST API to facilitate the processing of protocols in the programming language.

1.2   OBJECTIVE

The essential goal of the venture is:

a. To design a framework

b. To extract the raw data and convert that data into useful or readable form.

c. To analyze the data and perform certain actions like searching, sorting, etc.

d. To visualize different parameters of the data to get some results.

1.3   METHODOLOGY

A diagram of our strategy is given in Figure 1. We first preprocess the raw data into some useful information. Utilizing this preprocessed information, we perform certain actions on that information like searching particular rows across the data, perform sorting among different parameters, also try to visualize the effect of different parameters.
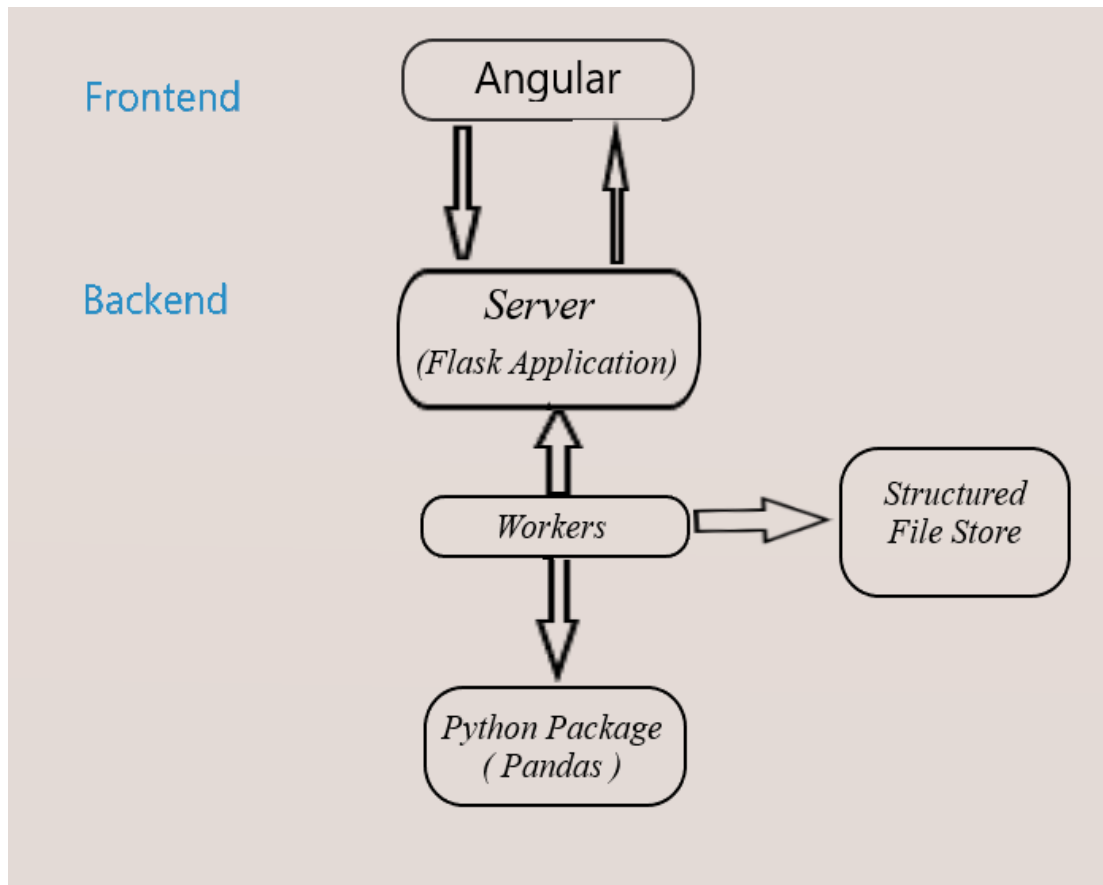
Figure 1 : Overview of the methodology

Chapter – 2

LITERATURE SURVEY

There were various type of applications (analyzer for log files) which process various log files from a particular vendor or facility and create easy-to-read summary reports. Doubtlessly these tools are useful, but use of these tools is limited to the log files of certain structure. However they have embedded questions and create integrated report, also provided with configuration option. The first reason for doing this work is the lack of a Cisco NetFlow Analyzer for monitoring and analyzing large computer networks such as the University of West Bohemia Capital Territory Network (WEBNET) or the Czech Academic Network Backbone (CESNET) with Cisco NetFlow data export. Since the volume of protocol data (each packet is recorded!), the evolution over time of the NetFlow log format and the wide range of monitoring tasks/questions, it is necessary to implement a new systematic, effective and open approach to protocol analysis. Also there is a belief that it develop an open and highly flexible modular tool which can analyze virtually any log file and answer any question, even the most complex and it makes sense to explore the field of log analysis . This analyzer must be programmable, expandable, efficient (thanks to the large number of log files) and convenient for the end user. This cannot be limited only for the analysis of log files of a particular structure or type and should not be limited to the essence of the issue.

2.1 Several other online event log file analyzers:

Log MX

This is an intuitive tool for analyzing log files. In addition to reading log files, MX Log also analyzes log events from any file or stream to provide a structured view of the logs. Log MX is a standalone application that weighs only about 6MB without the need to install a web server or update protocols.

The disadvantage of this analyzer is that you can not analyze the log files for free, you need to open an account and buy this tool.

G suite

This is another tool for analyzing online log files. The purpose is the same, but the disadvantage is that you can scan a limited number of log files. This is a domain to scan several much smaller log files. It can only process a certain number of log files like Chrome OS, GSSMO, GSMME, GSMME, GSMMO, GSMMO, GSMMO, GSMMO, GSMMO, GSMMO, GSMMO, GSMMO, GCDS, GSPS.

2.2 What can we extract from the log files?

This chapter provides an overview of the software development of log files , also monitoring and testing of files. Useful information provided in the log files can divided into different classes.

- General statistics (peak and average, median, mode, deviation...)

  Objective: to search and process the different elements of the report.

  Useful in: establishment of accounting field and various hardware requirements.

- Software/warning and system failure (less memory and failure of power)

  Objective: to find all the events that occurred in the reports.

  Useful for: system maintenance

- Safety instructions

  Purpose: To find all reported events in the report.

- Approval of programme execution

  Purpose: Construction, testing and trials of government equipment.

  Useful for: software testing

- Time-based functions

  Purpose: To calculate or guess the time intervals between various report events.
- Useful for: profiles and software benchmarking.

2.4 Text Processing

There are different text processing languages created for easy text processing. There mode of operation is based on Regex that is Regular Expression which make their usage and performance surprisingly batter and more efficient. The known representative text-processing languages are (PYTHON) and (AWK). Analysis of log files (or least simple log files analysis) is a task of text processing, so it is obvious to examine these type of languages. So, in this project, we put more focus on PYTHON, because it have various applications in the field of text processing. The major functioning of AWK is to find and search text files for lines that have certain and specific patterns. AWK performs specified actions on that line, when a line matches one of its regular expression patterns. AWK keeps the processing of input lines in , until the end of the input files are reached. AWK programs are data-driven, means first you have to define the type of data you want to process, and when you find or get that type of data then what to do with the data. Programs defined in AWK are different from programs given in other type of languages. Mostly other type of languages is procedural, i.e. Firstly you have to describe the language; in complete detail means each step of the program that you have taken. It is usually much harder to clearly define the data your program will analyze and process. when working with these procedural languages, For such reason, AWK programs are often easy to both write and read. When AWK runs , you specify an AWK program that tells it what to do. The program consists of some series of rules. Each and every rule specifies one pattern to search for, and one action to perform when that pattern is found.

2.5 Sample questions

The main objective of this section is to give brief overview of Internet usage problems, web server protocols is not the main purpose of this paper.

Whoever visits to your website? The basic point is to examine who are the readers of your server and who they are, from what countries and institutions, etc. and how they are used. Large number of servers also identifies second time visitors (returning visitors) and offers them with personalized pages for regular visitors.

The navigation of website and paths for the visitor leads through various pages of your website. Visitors begin to read the server, how easy it is for them to move if they often don't

search and navigate the appropriate hyperlink and then get return back. In short, the goal is to find paths, patterns and various trends.

For how long time the visitors keep going on each page? This will help one to answer and conclude which pages are useful and which are not useful means confusing or boring.

The end page displayed can be a logical place where the visitor ends his visit, or a place where he can escape.

The success of users on your site. Purchases, completed download, displayed information, completed activities. These features will show that site is properly structured, maintained and organized and the products offered are well represented.

2.6 Summary of the chapter

Log analysis has many applications, such as location security. As part of search engine optimization, the server file is usually downloaded and imported into the analysis log file, where all information about each hit on the site (bot or person) can be analyzed to inform the SEO solution and learn about previously unknown problems.

Analysis of log is a complex process which often leads to the identification of serious technical problems that otherwise cannot be found. Accurate data is contained by the log files which allows the brand to better understand how search engines navigate your site and what information they find.

The log file data includes the requested URL/resource, the actions performed, time and date, the IP address of the computer from which it was created, such as the user/browser agent, and other information.

Chapter – 3

SYSTEM REQUIREMENTS

3.1 TOOLS & FRAMEWORKS

3.1.1 Visual Studio Code

Visual Studio Code is a one of code editor or platform which is developed by Microsoft for multiple platforms like for macOS, for Linux, and Windows. It supports many features like support for debug, support for Git, highlight the syntax, different code snippets, support for different code completion, and also support for refactoring of the code. The main feature of Visual Code Editor is it allows us to customize our code editor according to our needs that means we can change the theme of our code editor according to our requirements, keyboard shortcuts, and preferences as we like.

VSC is build on framework named "Electron" that supports the deploy or implementation of Node.js.

VSC is a that type of code editor which supports different types of programming languages and that allows users to work with their desired programming language. The another major feature of VSC is it allows users to open more than one files and folders at the same time and work simultaneously and, which can then be saved in their respective folders.

Due to support of different variety of programming languages, VSC include all set of features for each different programing language that is different per language. It also allows or useful to remove files and folders that we want to exclude from our project and that can be achieved in settings.

3.1.2 ANGULAR

Angular is a framework for building web applications that is written fully in typescript. It is open source framework for web development developed or managed by Google and group of companies and by some group of individuals. Angular is a new version that is built by same team who have developed AngularJS.

Angular is a framework for web applications that allows us to create web applications over HTTP or Internet. Angular applications are mixture of variety of models, allows integration with other technologies, different end to end tools for building application and also support for dependency injections. Not this much but it allows developers to build web applications that not only run on web but also run on mobile like Android, different operating system like Windows, Linux or also run on different networks.

Why Angular?

- Angular introduces not only the tools, but also the design standards that make project maintenance easier. With the right Angular design, there is no confusion between classes and methods that are difficult to modify and even more difficult to test. The code is clearly structured and you don't have to spend a lot of time to understand what's going on.

- This is JavaScript, but better. It allows additional features other than previous JS like it allows interfaces, decorators, namespaces, arrow functions, static typewriting, classes, and so on.

- There is no need to reinvent the bike. Thanks to Angular, you already have a lot of tools to create applications immediately. You have instructions for the dynamic behavior of HTML elements. You can run forms by controlling the forms and entering various validation rules. Asynchronous HTTP requests of different types can be sent without problems. It is possible to set up the script without much effort. And there are many other delicacies that Angular can offer!

- Elements are disabled. Angular force to remove the dense coupling between different parts of the application. NodeJS-style injection molding can be easily replaced with different components.

- All manipulations with MOUs take place where they should be. When using Angular presentation technology, it is not associated with application logic, which greatly simplifies and simplifies the marking process.

- We will focus on the test. The corner test is designed for thorough testing and supports both unit and comprehensive testing using tools such as jasmine and conveyor.

- Corner is mobile and compatible with desktops, which means it has a multi-platform structure.

- It is actively supported and has a large community and ecosystem. You can find a lot of material about this framework, as well as many useful tools from other companies.

Figure 2 : Angular Components
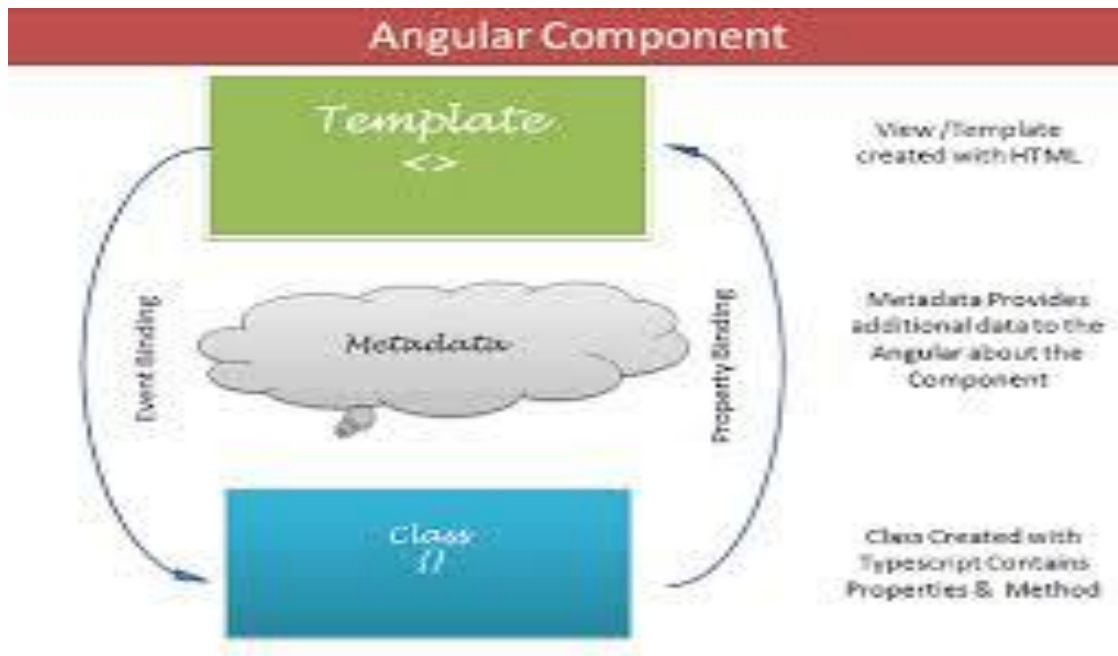
Dependency injection (DI) is that lets you keep your component classes lean and

efficient.

Figure 3 : Template, Data Binding

3.1.3 TYPESCRIPT

TypeScript is an programming language which is open source that means one can use it for free and also contribute for its further development and it is developed and managed by Microsoft. It is a JavaScript advanced version or we can call superset that consists of additional functionality to that provided by the JavaScript language.

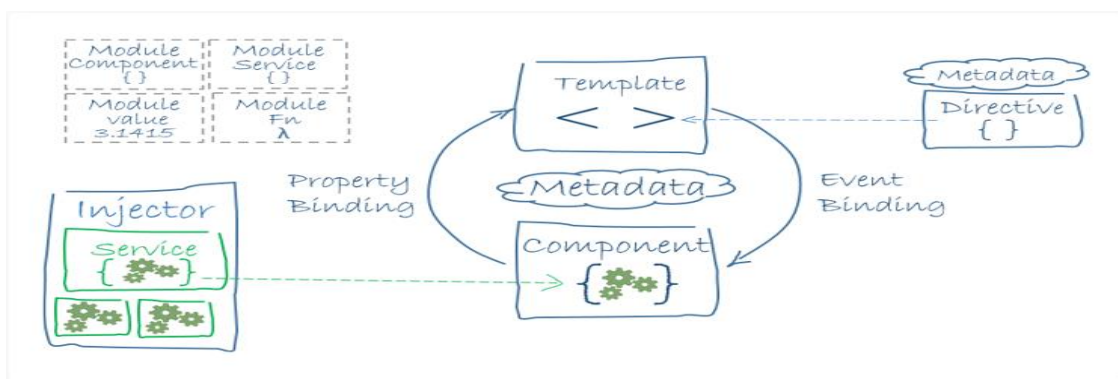TypeScript is designed primarily to develop large types of applications and then compile them into JavaScript. Since TypeScript is a JavaScript add-in, all existing JavaScript programs are as valid as TypeScript programs, which means that JavaScript programs can be compiled and executed with TypeScript.

TypeScript allows you to write JavaScript programs as users wish. TypeScript is a set of higher-level JavaScript that compiles a TypeScript(.ts) file into a simple JavaScript. TypeScript is purely object-oriented (OOP) with statically printed classes, interfaces and C# or Java languages. Angular 2.0 is one of the most popular JavaScript frameworks written in TypeScript. Mastery of the TypeScript language can help programmers write object-oriented programs (OOPs), compile them into a JavaScript file, and use them for client-side and server-side execution (Node.js).

3.1.4 PYTHON

Python is very simple programming language. It is very easy to learn python. The concept of objects and classes can be used in the Python very easily so that's why it is called object oriented programming language. Python source code is converted to byte code when we compile the source code. After that this byte code is executed by the interpreter. So this language is also known as the Interpreted language. Python has facility of in built high level data structures which makes this language very easy to learn.

3.1.5 NODE JS

Node.js provide, multi-platform JavaScript runtime environment and also executes code for the JavaScript exterior to the browser. For client-side scripts JavaScript is mainly used

,script is embedded within in HTML web page is written in JavaScript and compiled and executed on the client-side in the user's web browser using javascript engine.

Node.js permits the developers for using JavaScript to write server-side scripts or command line commands by running server-side scripts for creating dynamic web page content before sending the page to the user's browser. As a result, Node.js represents the "JavaScript everywhere", combining the development of web applications around a single programming language rather than several scripting languages on the server and client side.

3.1.6 FLASK

A flask is a microstructure written in Python. It does not have an abstract level of database, form checking or other components in which other libraries supports overall functionality.

Flask is used as an integration to connect to any framework using REST API. There are extensions for support for form validation, support for mappers, data loading. Extensions are updated much more regularly.

3.2 LIBRARIES

3.2.1 NUMPY

Numpy is a Library which provide the facility of easy manipulation of multi-dimensional array in Python. Without this library the facility of use of multidimensional array is little bit difficult. By importing this package, multidimensional array can be manipulated easily. Also, other high dimensional operation of mathematics can be used with the help of this package.

3.2.2 PANDAS

Data analysis can be done very easily with the help of Python. Python provides multiple packages and libraries which provides user to different type of facilities. Pandas is one of them. This library is used for data analysis. With the help of this library user can optimized performance.

Data can be analyzing in Pandas with: - series and data frames. Series means 1-D array in Pandas. With the help of Series user can store any datatype. DataFrames means rows and columns.so Data frame is 2-D array.

3.2.3 MATPLOTLIB

Matplotlib is one of the most important library in Python. This library generally used by the user for creation of graphs. Data can be visualized very easily with the help of this library. This library supports users to create different type of graphs such as- Histogram, Power spectra, Error charts etc.

3.3 LOG FILES FORMAT

3.3.1 Android

Format: ['Date', 'Time', 'Pid', 'Tid', 'Level', 'Component', 'Content']

```
03-17 16:13:38.811  1702  2395 D WindowManager: printFreezingDisplayLogsopening app wtoken =
AppWindowToken{9f4ef63 token=Token{a64f992 ActivityRecord{de9231d u0
com.tencent.qt.qtl/.activity.info.NewsDetailXmlActivity t761}}}, allDrawn= false, startingDisp
false, startingMoved =  false, isRelaunching =  false
03-17 16:13:38.819  1702  8671 D PowerManagerService: acquire lock=233570404, flags=0x1, tag='
Lock", name=com.android.systemui, ws=null, uid=10037, pid=2227
03-17 16:13:38.820  1702  8671 D PowerManagerService:
ready=true,policy=3,wakefulness=1,wksummary=0x23,uasummary=0x1,bootcompleted=true,boostinprogr
waitmodeenable=false,mode=false,manual=38,auto=-1,adj=0.0userId=0
03-17 16:13:38.839  1702  2113 V WindowManager: Skipping AppWindowToken{df0798e token=Token{78
ActivityRecord{3b04890 u0 com.tencent.qt.qtl/com.tencent.video.player.activity.PlayerActivity
going to hide
03-17 16:13:38.859  2227  2227 D TextView: visible is system.time.showampm
03-17 16:13:38.861  2227  2227 D TextView: mVisiblity.getValue is false
03-17 16:13:38.869  2227  2227 D TextView: visible is system.charge.show
03-17 16:13:38.871  2227  2227 D TextView: mVisiblity.getValue is false
03-17 16:13:38.875  2227  2227 D TextView: visible is system.call.count gt 0
```

3.3.2 Windows

Format: ['Date', 'Time', 'Level', 'Component', 'Content']

```
2016-09-28 04:30:30, Info                CBS     Loaded Servicing Stack v6.1.7601.23505 with
\Windows\winsxs\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_6.1.7601.23505_none_681aa442f6fed7f0\cbscore.dll
2016-09-28 04:30:31, Info                CSI     00000001@2016/9/27:20:30:31.455 WcpInitiali
version 0.0.0.6) called (stack @0x7fed806eb5d @0x7fef9fb9b6d @0x7fef9f8358f @0xff83e97c @0xff
@0xff83db2f)
2016-09-28 04:30:31, Info                CSI     00000002@2016/9/27:20:30:31.458 WcpInitiali
version 0.0.0.6) called (stack @0x7fed806eb5d @0x7fefa006ade @0x7fef9fd2984 @0x7fef9f83665 @0
@0xff83d799)
2016-09-28 04:30:31, Info                CSI     00000003@2016/9/27:20:30:31.458 WcpInitiali
version 0.0.0.6) called (stack @0x7fed806eb5d @0x7fefa1c8728 @0x7fefa1c8856 @0xff83e474 @0xff
@0xff83db2f)
2016-09-28 04:30:31, Info                CBS     Ending TrustedInstaller initialization.
2016-09-28 04:30:31, Info                CBS     Starting the TrustedInstaller main loop.
2016-09-28 04:30:31, Info                CBS     TrustedInstaller service starts successfull
2016-09-28 04:30:31, Info                CBS     SQM: Initializing online with Windows opt-i
2016-09-28 04:30:31, Info                CBS     SQM: Cleaning up report files older than 10
```

Figure 4 : Windows Log File

3.3.3 Apache

Format: ['Day', 'Month', 'Date', 'Time', 'Year', 'Level', 'Content']

```
[Sun Dec 04 04:47:44 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 04:47:44 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 04:51:08 2005] [notice] jk2_init() Found child 6725 in scoreboard slot 10
[Sun Dec 04 04:51:09 2005] [notice] jk2_init() Found child 6726 in scoreboard slot 8
[Sun Dec 04 04:51:09 2005] [notice] jk2_init() Found child 6728 in scoreboard slot 6
[Sun Dec 04 04:51:14 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 04:51:14 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 04:51:14 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 04:51:18 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 04:51:18 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 04:51:18 2005] [error] mod_jk child workerEnv in error state 6
[Sun Dec 04 04:51:37 2005] [notice] jk2_init() Found child 6736 in scoreboard slot 10
[Sun Dec 04 04:51:38 2005] [notice] jk2_init() Found child 6733 in scoreboard slot 7
[Sun Dec 04 04:51:38 2005] [notice] jk2_init() Found child 6734 in scoreboard slot 9
[Sun Dec 04 04:51:52 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 04:51:52 2005] [notice] workerEnv.init() ok /etc/httpd/conf/workers2.properties
[Sun Dec 04 04:51:55 2005] [error] mod_jk child workerEnv in error state 6
```

3.3.4 HDFS

Format: ['Date', 'Time', 'Pid', 'Level', 'Component', 'Content']

```
081109 203615 148 INFO dfs.DataNode$PacketResponder: PacketResponder 1 for block blk_38865049
terminating
081109 203807 222 INFO dfs.DataNode$PacketResponder: PacketResponder 0 for block blk_-
6952295868487656571 terminating
081109 204005 35 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated:
10.251.73.220:50010 is added to blk_7128370237687728475 size 67108864
081109 204015 308 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_82291938
terminating
081109 204106 329 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_-
6670958622368987959 terminating
081109 204132 26 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated:
10.251.43.115:50010 is added to blk_3050920587428079149 size 67108864
081109 204324 34 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated:
10.251.203.80:50010 is added to blk_7888946331804732825 size 67108864
081109 204453 34 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated:
10.250.11.85:50010 is added to blk_2377150260128098806 size 67108864
081109 204525 512 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_57249283
```

3.3.5 BGL

Format: ['Label', 'Timestamp', 'Date', 'Node', 'Time', 'Node Repeat', 'Type', 'Component', 'Level', 'Content']

```
- 1117838570 2005.06.03 R02-M1-N0-C:J12-U11 2005-06-03-15.42.50.675872 R02-M1-N0-C:J12-U11 RA
INFO instruction cache parity error corrected
- 1117838573 2005.06.03 R02-M1-N0-C:J12-U11 2005-06-03-15.42.53.276129 R02-M1-N0-C:J12-U11 RA
INFO instruction cache parity error corrected
- 1117838976 2005.06.03 R02-M1-N0-C:J12-U11 2005-06-03-15.49.36.156884 R02-M1-N0-C:J12-U11 RA
INFO instruction cache parity error corrected
- 1117838978 2005.06.03 R02-M1-N0-C:J12-U11 2005-06-03-15.49.38.026704 R02-M1-N0-C:J12-U11 RA
INFO instruction cache parity error corrected
- 1117842440 2005.06.03 R23-M0-NE-C:J05-U01 2005-06-03-16.47.20.730545 R23-M0-NE-C:J05-U01 RA
INFO 63543 double-hummer alignment exceptions
- 1117842974 2005.06.03 R24-M0-N1-C:J13-U11 2005-06-03-16.56.14.254137 R24-M0-N1-C:J13-U11 RA
INFO 162 double-hummer alignment exceptions
- 1117843015 2005.06.03 R21-M1-N6-C:J08-U11 2005-06-03-16.56.55.309974 R21-M1-N6-C:J08-U11 RA
INFO 141 double-hummer alignment exceptions
- 1117848119 2005.06.03 R16-M1-N2-C:J17-U01 2005-06-03-18.21.59.871925 R16-M1-N2-C:J17-U01 RA
INFO CE sym 2, at 0x0b85eee0, mask 0x05
APPREAD 1117869872 2005.06.04 R04-M1-N4-I:J18-U11 2005-06-04-00.24.32.432192 R04-M1-N4-I:J18-
```

3.3.6 Hadoop

Format: ['Date', 'Time', 'Level', 'Process', 'Component', 'Content']

```
2015-10-18 18:01:47,978 INFO [main] org.apache.hadoop.mapreduce.v2.app.MRAppMaster: Created M
for application appattempt_1445144423722_0020_000001
2015-10-18 18:01:48,963 INFO [main] org.apache.hadoop.mapreduce.v2.app.MRAppMaster: Executing
tokens:
2015-10-18 18:01:48,963 INFO [main] org.apache.hadoop.mapreduce.v2.app.MRAppMaster: Kind:
YARN_AM_RM_TOKEN, Service: , Ident: (appAttemptId { application_id { id: 20 cluster_timestamp
1445144423722 } attemptId: 1 } keyId: -127633188)
2015-10-18 18:01:49,228 INFO [main] org.apache.hadoop.mapreduce.v2.app.MRAppMaster: Using map
newApiCommitter.
2015-10-18 18:01:50,353 INFO [main] org.apache.hadoop.mapreduce.v2.app.MRAppMaster: OutputCom
in config null
2015-10-18 18:01:50,509 INFO [main] org.apache.hadoop.mapreduce.v2.app.MRAppMaster: OutputCom
org.apache.hadoop.mapreduce.lib.output.FileOutputCommitter
2015-10-18 18:01:50,556 INFO [main] org.apache.hadoop.yarn.event.AsyncDispatcher: Registering
org.apache.hadoop.mapreduce.jobhistory.EventType for class
org.apache.hadoop.mapreduce.jobhistory.JobHistoryEventHandler
2015-10-18 18:01:50,556 INFO [main] org.apache.hadoop.yarn.event.AsyncDispatcher: Registering
```

3.3.7   HPC

Format: ['Log Id', 'Node', 'Component', 'State', 'Time', 'Flag', 'Content']

```
134681 node-246 unix.hw state_change.unavailable 1077804742 1 Component State Change: Compone
\042SCSI-WWID:01000010:6005-08b4-0001-00c6-0006-3000-003d-0000\042 is in the unavailable stat
(HWID=1973)
350766 node-109 unix.hw state_change.unavailable 1084680778 1 Component State Change: Compone
\042alt0\042 is in the unavailable state (HWID=3180)
344518 node-246 unix.hw state_change.unavailable 1084270955 1 Component State Change: Compone
\042alt0\042 is in the unavailable state (HWID=5089)
344448 node-153 unix.hw state_change.unavailable 1084270952 1 Component State Change: Compone
\042alt0\042 is in the unavailable state (HWID=4088)
366633 node-200 unix.hw state_change.unavailable 1085100843 1 Component State Change: Compone
\042alt0\042 is in the unavailable state (HWID=2538)
366463 node-122 unix.hw state_change.unavailable 1085084674 1 Component State Change: Compone
\042alt0\042 is in the unavailable state (HWID=2480)
438190 node-228 unix.hw state_change.unavailable 1097194780 1 Component State Change: Compone
\042alt0\042 is in the unavailable state (HWID=3713)
225111 node-10 unix.hw state_change.unavailable 1117296789 1 Component State Change: Componen
\042alt0\042 is in the unavailable state (HWID=3891)
```

3.3.8   Linux

Format: ['Month', 'Date', 'Time', 'Level', 'Component', 'PID', 'Content']

```
Jun 14 15:16:01 combo sshd(pam_unix)[19939]: authentication failure; logname= uid=0 euid=0 tt
ruser= rhost=218.188.2.4
Jun 14 15:16:02 combo sshd(pam_unix)[19937]: check pass; user unknown
Jun 14 15:16:02 combo sshd(pam_unix)[19937]: authentication failure; logname= uid=0 euid=0 tt
ruser= rhost=218.188.2.4
Jun 15 02:04:59 combo sshd(pam_unix)[20882]: authentication failure; logname= uid=0 euid=0 tt
ruser= rhost=220-135-151-1.hinet-ip.hinet.net   user=root
Jun 15 02:04:59 combo sshd(pam_unix)[20884]: authentication failure; logname= uid=0 euid=0 tt
ruser= rhost=220-135-151-1.hinet-ip.hinet.net   user=root
Jun 15 02:04:59 combo sshd(pam_unix)[20883]: authentication failure; logname= uid=0 euid=0 tt
ruser= rhost=220-135-151-1.hinet-ip.hinet.net   user=root
Jun 15 02:04:59 combo sshd(pam_unix)[20885]: authentication failure; logname= uid=0 euid=0 tt
ruser= rhost=220-135-151-1.hinet-ip.hinet.net   user=root
Jun 15 02:04:59 combo sshd(pam_unix)[20886]: authentication failure; logname= uid=0 euid=0 tt
ruser= rhost=220-135-151-1.hinet-ip.hinet.net   user=root
Jun 15 02:04:59 combo sshd(pam_unix)[20892]: authentication failure; logname= uid=0 euid=0 tt
ruser= rhost=220-135-151-1.hinet-ip.hinet.net   user=root
```

3.3.9 Mac

Format: ['Month', 'Date', 'Time', 'User', 'Component', 'PID', 'Address', 'Content']

```
Jul  1 09:00:55 calvisitor-10-105-160-95 kernel[0]: IOThunderboltSwitch<0>(0x0)::listenerCall
Thunderbolt HPD packet for route = 0x0 port = 11 unplug = 0
Jul  1 09:01:05 calvisitor-10-105-160-95 com.apple.CDScheduler[43]: Thermal pressure state: 1
pressure state: 0
Jul  1 09:01:06 calvisitor-10-105-160-95 QQ[10018]: FA||Url||taskID[2019352994] dealloc
Jul  1 09:02:26 calvisitor-10-105-160-95 kernel[0]: ARPT: 620701.011328:
AirPort_Brcm43xx::syncPowerState: WWEN[enabled]
Jul  1 09:02:26 authorMacBook-Pro kernel[0]: ARPT: 620702.879952: AirPort_Brcm43xx::platformW
WWEN[disable]
Jul  1 09:03:11 calvisitor-10-105-160-95 mDNSResponder[91]: mDNS_DeregisterInterface: Frequen
transitions for interface awdl0 (FE80:0000:0000:0000:D8A5:90FF:FEF5:7FFF)
Jul  1 09:03:13 calvisitor-10-105-160-95 kernel[0]: ARPT: 620749.901374: IOPMPowerSource Info
onSleep,  SleepType: Normal Sleep,  'ExternalConnected': Yes, 'TimeRemaining': 0,
Jul  1 09:04:33 calvisitor-10-105-160-95 kernel[0]: ARPT: 620750.434035: wl0: wl_update_tcpke
Original Seq: 3226706533, Ack: 3871687177, Win size: 4096
Jul  1 09:04:33 authorMacBook-Pro kernel[0]: ARPT: 620752.337198: ARPT: Wake Reason: Wake on
offload
```

3.3.10 OpenSSH

Format: ['Date', 'Day', 'Time', 'Component', 'Pid', 'Content']

```
Dec 10 06:55:46 LabSZ sshd[24200]: reverse mapping checking getaddrinfo for ns.marryaldkfaczc
[173.234.31.186] failed - POSSIBLE BREAK-IN ATTEMPT!
Dec 10 06:55:46 LabSZ sshd[24200]: Invalid user webmaster from 173.234.31.186
Dec 10 06:55:46 LabSZ sshd[24200]: input_userauth_request: invalid user webmaster [preauth]
Dec 10 06:55:46 LabSZ sshd[24200]: pam_unix(sshd:auth): check pass; user unknown
Dec 10 06:55:46 LabSZ sshd[24200]: pam_unix(sshd:auth): authentication failure; logname= uid=
tty=ssh ruser= rhost=173.234.31.186
Dec 10 06:55:48 LabSZ sshd[24200]: Failed password for invalid user webmaster from 173.234.31
38926 ssh2
Dec 10 06:55:48 LabSZ sshd[24200]: Connection closed by 173.234.31.186 [preauth]
Dec 10 07:02:47 LabSZ sshd[24203]: Connection closed by 212.47.254.145 [preauth]
Dec 10 07:07:38 LabSZ sshd[24206]: Invalid user test9 from 52.80.34.196
Dec 10 07:07:38 LabSZ sshd[24206]: input_userauth_request: invalid user test9 [preauth]
Dec 10 07:07:38 LabSZ sshd[24206]: pam_unix(sshd:auth): check pass; user unknown
Dec 10 07:07:38 LabSZ sshd[24206]: pam_unix(sshd:auth): authentication failure; logname= uid=
tty=ssh ruser= rhost=ec2-52-80-34-196.cn-north-1.compute.amazonaws.com.cn
Dec 10 07:07:45 LabSZ sshd[24206]: Failed password for invalid user test9 from 52.80.34.196 p
```

3.3.11 OpenStack

Format: ['Log record', 'Date', 'Time', 'Pid', 'Level', 'Component', 'ADDR', 'Content']

```
nova-api.log.1.2017-05-16_13:53:08 2017-05-16 00:00:00.008 25746 INFO nova.osapi_compute.wsg:
[req-38101a0b-2096-447d-96ea-a692162415ae 113d3a99c3da401fbd62cc2caa5b96d2
54fadb412c4e40cdbaed9335e4c35a9e - - -] 10.11.10.1 "GET
/v2/54fadb412c4e40cdbaed9335e4c35a9e/servers/detail HTTP/1.1" status: 200 len: 1893 time: 0.:
nova-api.log.1.2017-05-16_13:53:08 2017-05-16 00:00:00.272 25746 INFO nova.osapi_compute.wsg:
[req-9bc36dd9-91c5-4314-898a-47625eb93b09 113d3a99c3da401fbd62cc2caa5b96d2
54fadb412c4e40cdbaed9335e4c35a9e - - -] 10.11.10.1 "GET
/v2/54fadb412c4e40cdbaed9335e4c35a9e/servers/detail HTTP/1.1" status: 200 len: 1893 time: 0.:
nova-api.log.1.2017-05-16_13:53:08 2017-05-16 00:00:01.551 25746 INFO nova.osapi_compute.wsg:
[req-55db2d8d-cdb7-4b4b-993b-429be84c0c3e 113d3a99c3da401fbd62cc2caa5b96d2
54fadb412c4e40cdbaed9335e4c35a9e - - -] 10.11.10.1 "GET
/v2/54fadb412c4e40cdbaed9335e4c35a9e/servers/detail HTTP/1.1" status: 200 len: 1893 time: 0.:
nova-api.log.1.2017-05-16_13:53:08 2017-05-16 00:00:01.813 25746 INFO nova.osapi_compute.wsg:
[req-2a3dc421-6604-42a7-9390-a18dc824d5d6 113d3a99c3da401fbd62cc2caa5b96d2
54fadb412c4e40cdbaed9335e4c35a9e - - -] 10.11.10.1 "GET
/v2/54fadb412c4e40cdbaed9335e4c35a9e/servers/detail HTTP/1.1" status: 200 len: 1893 time: 0.:
nova-api.log.1.2017-05-16_13:53:08 2017-05-16 00:00:03.091 25746 INFO nova.osapi_compute.wsg:
```

3.3.12 Proxifier

Format: ['Time', 'Program', 'Content']

```
[10.30 16:49:06] chrome.exe - proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.ed
HTTPS[10.30 16:49:06] chrome.exe - proxy.cse.cuhk.edu.hk:5070 open through proxy
proxy.cse.cuhk.edu.hk:5070 HTTPS[10.30 16:49:06] chrome.exe - proxy.cse.cuhk.edu.hk:5070 open
proxy proxy.cse.cuhk.edu.hk:5070 HTTPS[10.30 16:49:07] chrome.exe - proxy.cse.cuhk.edu.hk:507
bytes sent, 0 bytes received, lifetime 00:01[10.30 16:49:07] chrome.exe - proxy.cse.cuhk.edu.
open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS[10.30 16:49:07] chrome.exe -
proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS[10.30 16:49:07
chrome.exe - proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS[1
16:49:07] chrome.exe - proxy.cse.cuhk.edu.hk:5070 close, 403 bytes sent, 426 bytes received,
sec[10.30 16:49:07] chrome.exe - proxy.cse.cuhk.edu.hk:5070 open through proxy
proxy.cse.cuhk.edu.hk:5070 HTTPS[10.30 16:49:07] chrome.exe - proxy.cse.cuhk.edu.hk:5070 open
proxy proxy.cse.cuhk.edu.hk:5070 HTTPS[10.30 16:49:07] chrome.exe - proxy.cse.cuhk.edu.hk:507
451 bytes sent, 18846 bytes (18.4 KB) received, lifetime <1 sec[10.30 16:49:08] chrome.exe -
proxy.cse.cuhk.edu.hk:5070 close, 445 bytes sent, 5174 bytes (5.05 KB) received, lifetime <1
16:49:08] chrome.exe - proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:50
[10.30 16:49:08] chrome.exe - proxy.cse.cuhk.edu.hk:5070 close, 1190 bytes (1.16 KB) sent, 16
(1.63 KB) received, lifetime 00:02[10.30 16:49:08] chrome.exe - proxy.cse.cuhk.edu.hk:5070 op
```

3.3.13 Spark

Format: ['Date', 'Time', 'Level', 'Content']

```
17/06/09 20:10:40 INFO executor.CoarseGrainedExecutorBackend: Registered signal handlers for
INT]
17/06/09 20:10:40 INFO spark.SecurityManager: Changing view acls to: yarn,curi
17/06/09 20:10:40 INFO spark.SecurityManager: Changing modify acls to: yarn,curi
17/06/09 20:10:40 INFO spark.SecurityManager: SecurityManager: authentication disabled; ui ac
disabled; users with view permissions: Set(yarn, curi); users with modify permissions: Set(ya
17/06/09 20:10:41 INFO spark.SecurityManager: Changing view acls to: yarn,curi
17/06/09 20:10:41 INFO spark.SecurityManager: Changing modify acls to: yarn,curi
17/06/09 20:10:41 INFO spark.SecurityManager: SecurityManager: authentication disabled; ui ac
disabled; users with view permissions: Set(yarn, curi); users with modify permissions: Set(ya
17/06/09 20:10:41 INFO slf4j.Slf4jLogger: Slf4jLogger started
17/06/09 20:10:41 INFO Remoting: Starting remoting
17/06/09 20:10:41 INFO Remoting: Remoting started; listening on addresses :
[akka.tcp://sparkExecutorActorSystem@mesos-slave-07:55904]
17/06/09 20:10:41 INFO util.Utils: Successfully started service 'sparkExecutorActorSystem' on
55904.
17/06/09 20:10:41 INFO storage.DiskBlockManager: Created local directory at
```

3.3.14 ThunderBird

Format: ['Label', 'Timestamp', 'Date', 'User', 'Month', 'Day', 'Time', 'Location', 'Component', 'Content']

```
- 1131566461 2005.11.09 dn228 Nov 9 12:01:01 dn228/dn228 crond(pam_unix)[2915]: session close
root
- 1131566461 2005.11.09 dn228 Nov 9 12:01:01 dn228/dn228 crond(pam_unix)[2915]: session opene
root by (uid=0)
- 1131566461 2005.11.09 dn228 Nov 9 12:01:01 dn228/dn228 crond[2916]: (root) CMD (run-parts
/etc/cron.hourly)
- 1131566461 2005.11.09 dn261 Nov 9 12:01:01 dn261/dn261 crond(pam_unix)[2907]: session close
root
- 1131566461 2005.11.09 dn261 Nov 9 12:01:01 dn261/dn261 crond(pam_unix)[2907]: session opene
root by (uid=0)
- 1131566461 2005.11.09 dn261 Nov 9 12:01:01 dn261/dn261 crond[2908]: (root) CMD (run-parts
/etc/cron.hourly)
- 1131566461 2005.11.09 dn3 Nov 9 12:01:01 dn3/dn3 crond(pam_unix)[2907]: session closed for
- 1131566461 2005.11.09 dn3 Nov 9 12:01:01 dn3/dn3 crond(pam_unix)[2907]: session opened for
by (uid=0)
- 1131566461 2005.11.09 dn3 Nov 9 12:01:01 dn3/dn3 crond[2908]: (root) CMD (run-parts /etc/cr
- 1131566461 2005.11.09 dn596 Nov 9 12:01:01 dn596/dn596 crond(pam_unix)[2727]: session close
```

Chapter - 4

System Design & Implementation

4.1 Application Development

The below is the step by step implementation of our web application that how our application works.

1. Job Setup:

This is the first page of our application that how our application is going to look like. In this page we provide an user interface in which user has to choose log file and also the format of that log file listed in dropdown format.
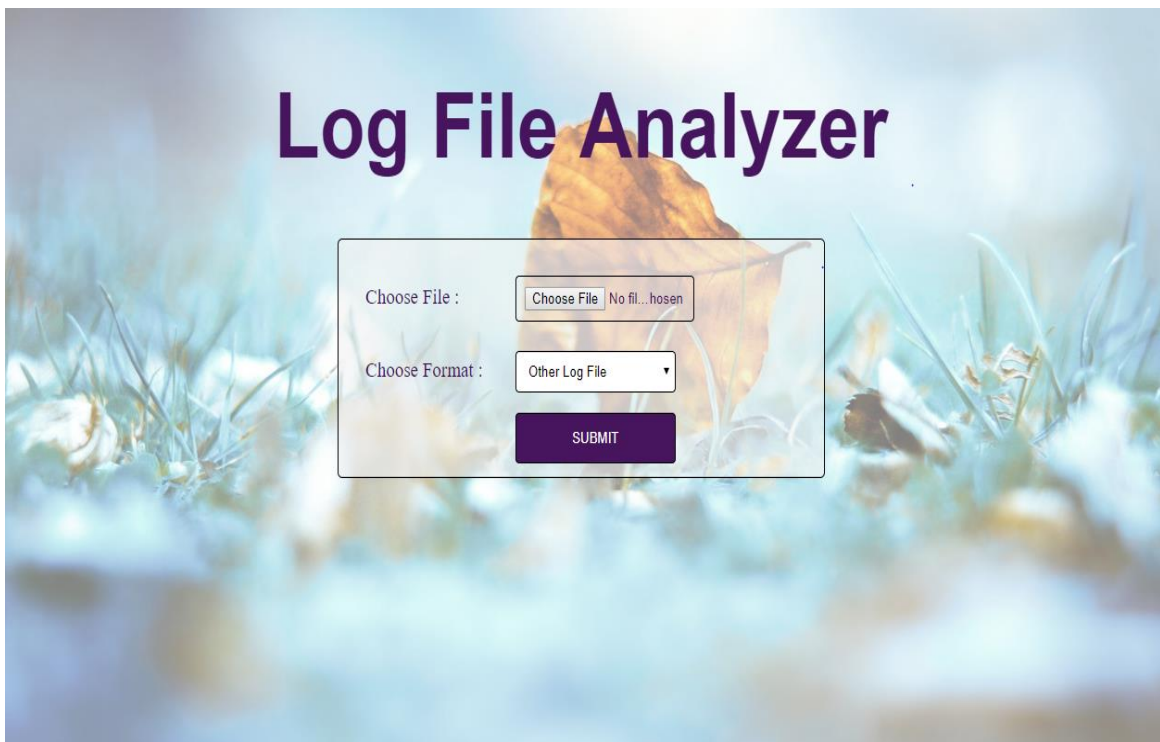
Figure 5 : Job Setup
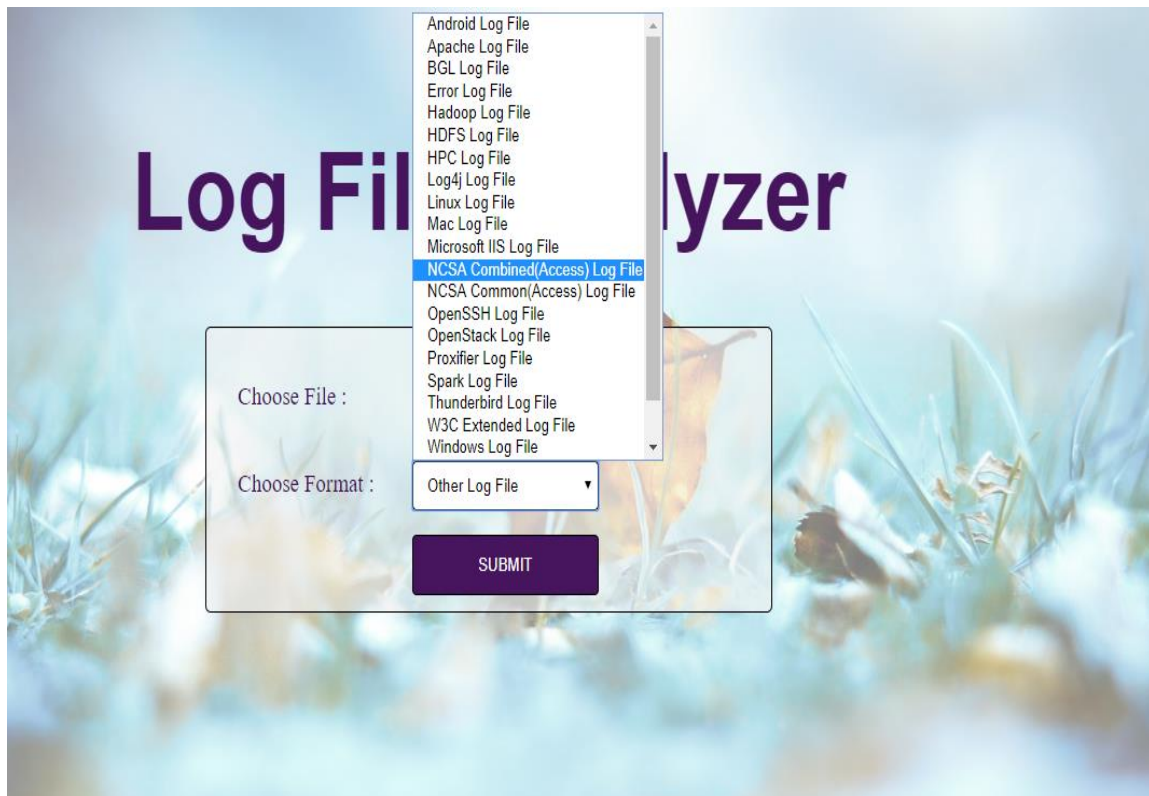
Figure 6 : Log Files

2. Send Metadata (Angular):

After selecting the file and the format of log file, the file content is processed or extracted in Angular and sent data to Server. For that purpose, we have created Rest API Service in Angular Client Side to send the data to the Backend Server that is Flask.

3. Read Metadata (Flask) :

After sending the metadata from Angular i.e from Client Side, now we have to fetch that data. So for that we integrate Angular Rest Services and Python Rest Services using Flask Web Framework.

4. Filtering & Cleaning

After receiving the raw data in Flask, we first have to preprocess it. That means we have to perform filtering and cleaning on it. So in this process, some of unwanted records are deleted and filtered out.

5. Data Analysis :

After filtering and cleaning phase, now we have to analyze our structured data. For analysis, we are using Material Table to show the structured data in form of table. Below is the output of the log file shown :

Figure 7 : Data Analyzing

6. Processing of Results (Visualization) :

After analysis the structured data in form of table, now we would like to visualize the data in form of charts. So, for that we are using ng2-charts in Angular framework. Ng2-charts can transform data into pie charts, bar graphs, line charts and doughnut charts.

23
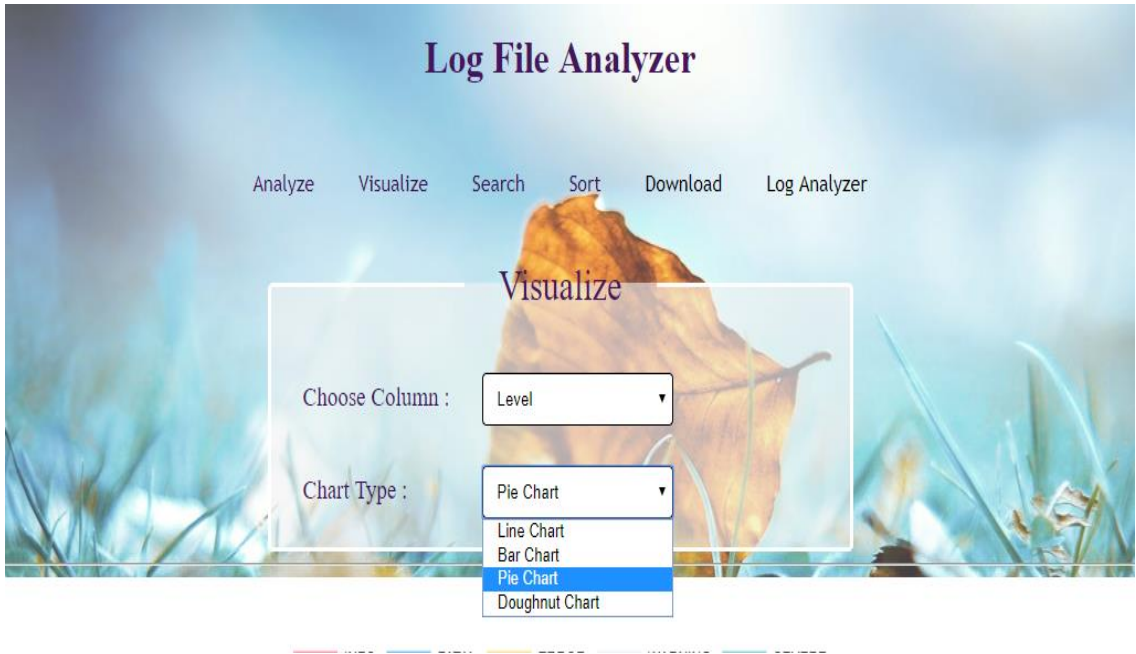
Figure 8 : Data Visualization
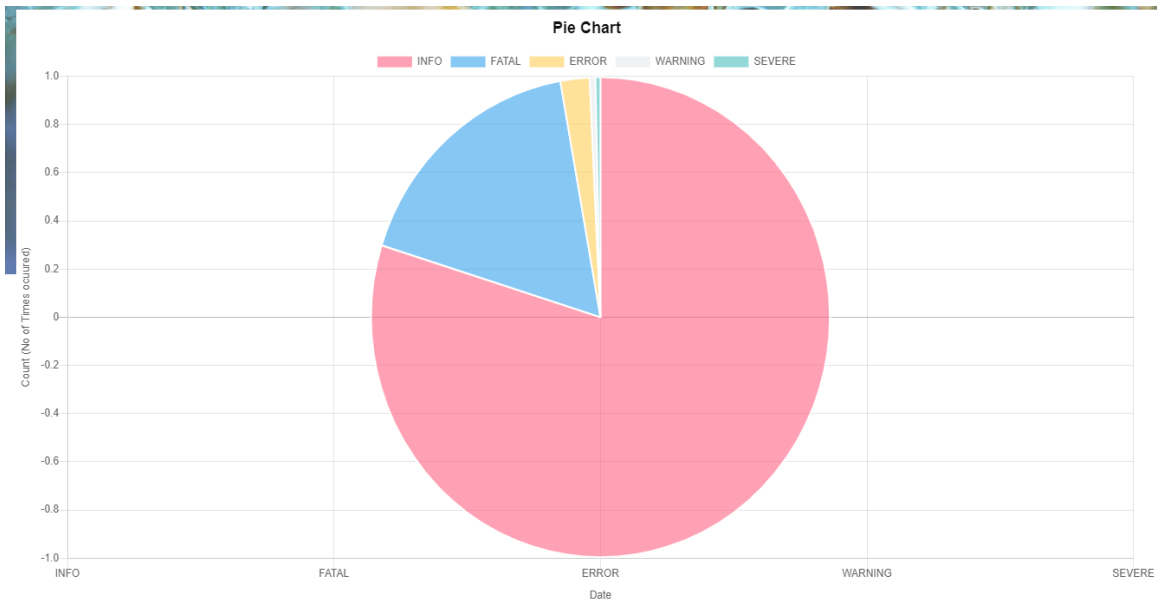
Figure 9 : Pie Chart Visualization
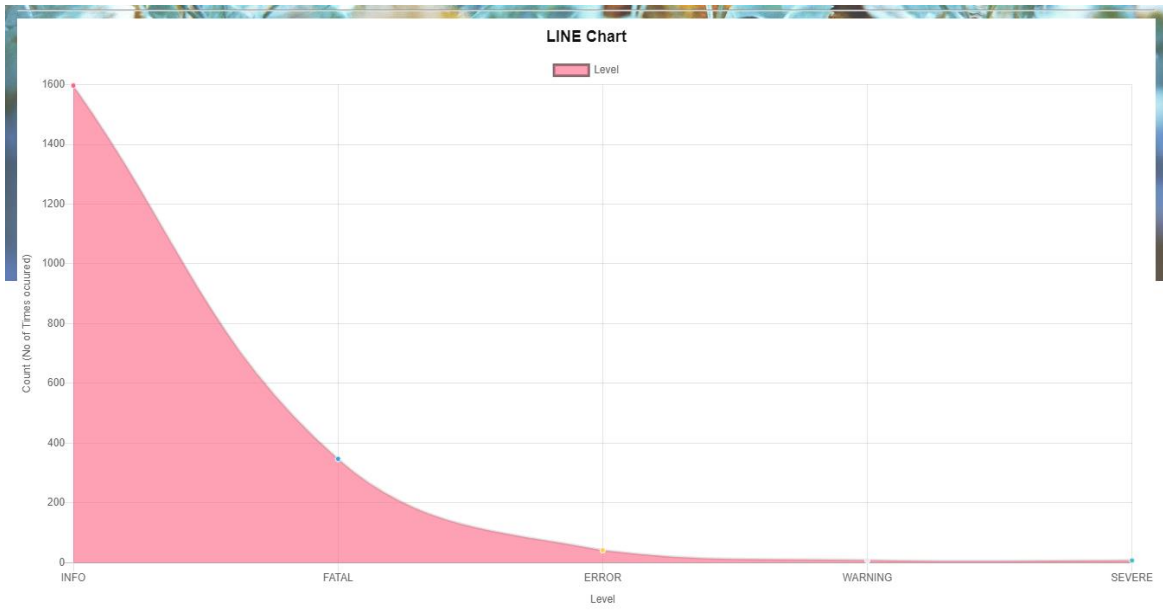
Figure 10 : Line Chart Visualization
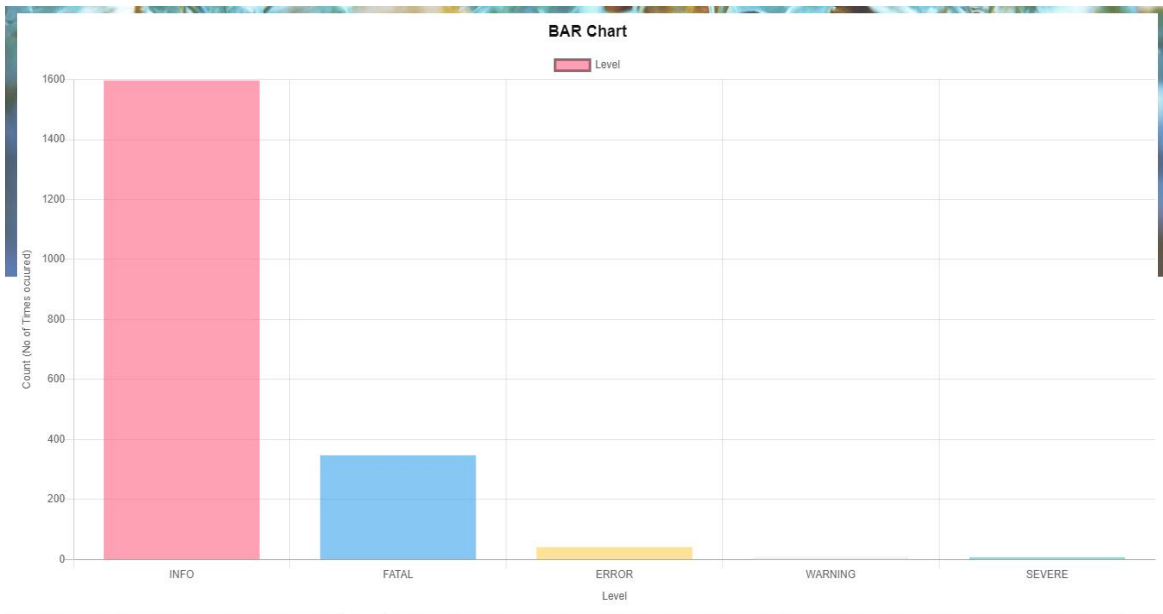
Figure 11 : Bar Chart Visualization
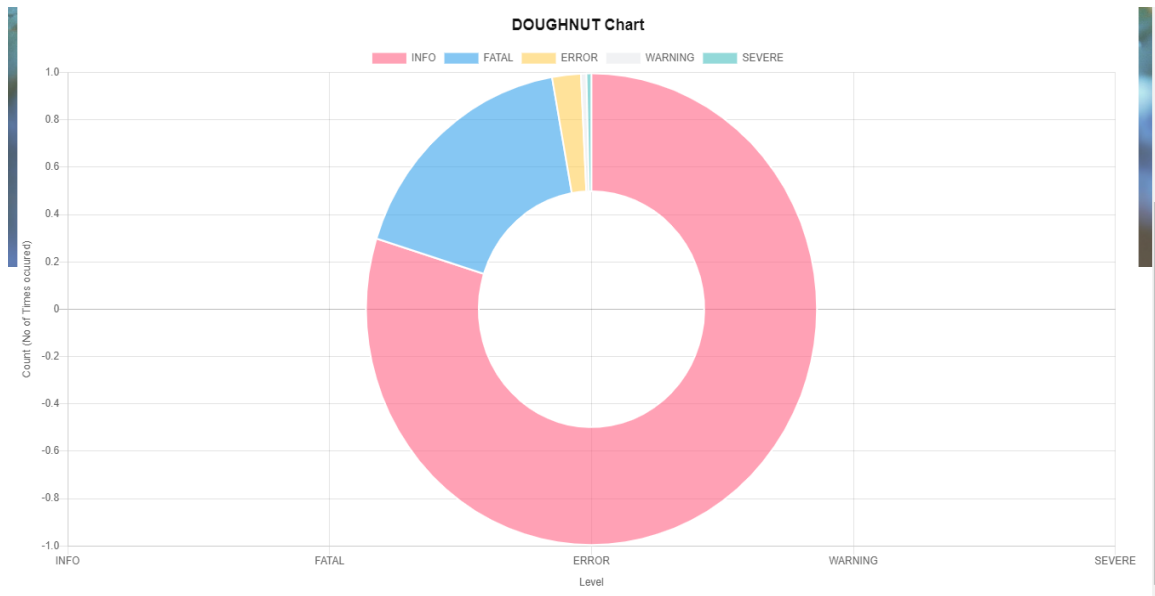
Figure 12 : Doughnut Chart Visualization
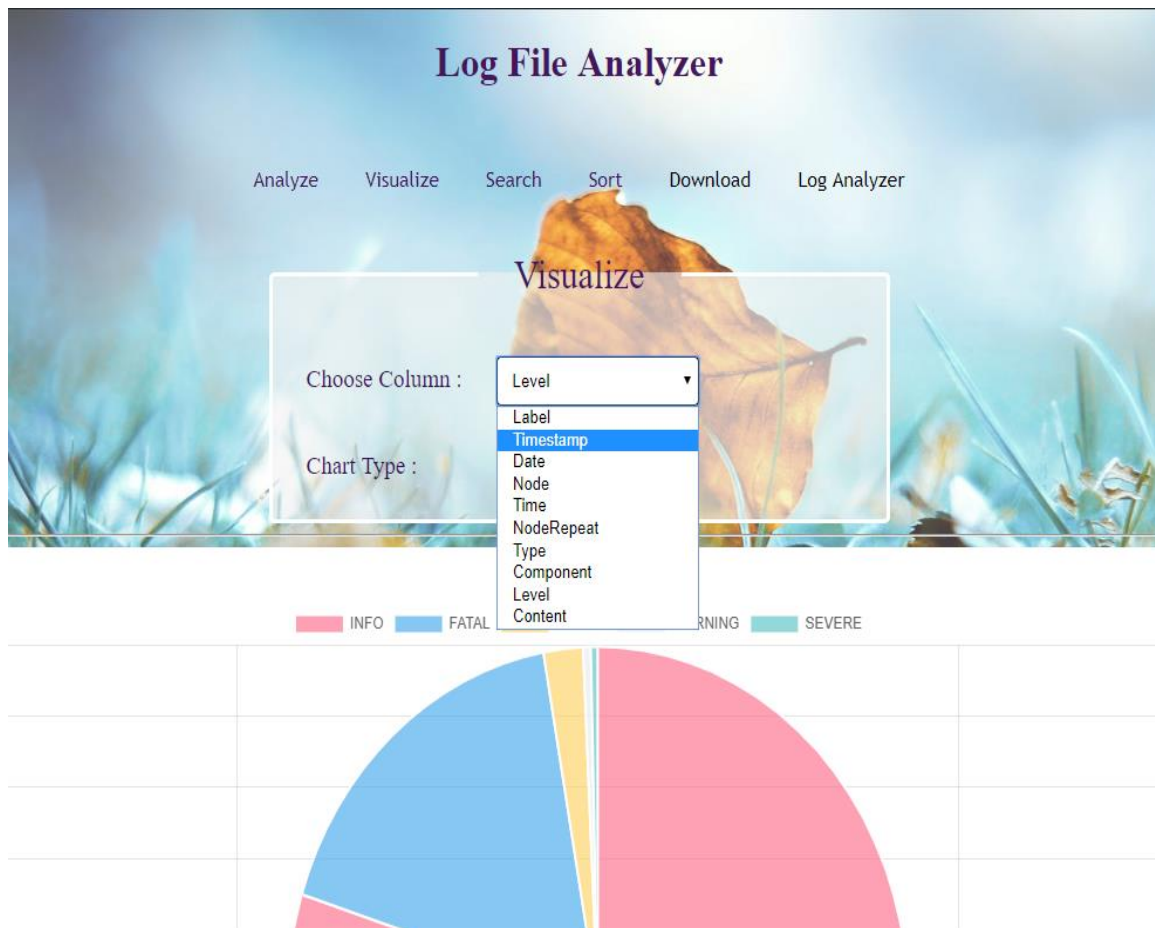
Figure 13 : Different Columns Visualization

7. Searching :

In this operation, client can search the queries to get result of particular fields. The Search operation is fully performed by the Backend Server i.e using Python REST API Service and the results are directly displayed on the Angular i.e on Client Side.
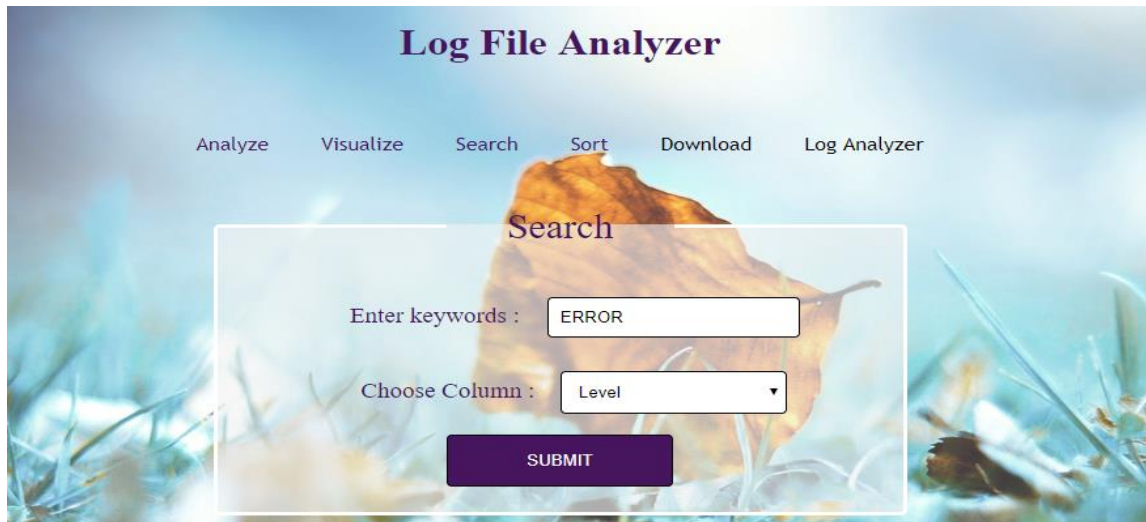
Figure 14 : Search Operation

Figure 15 : Search for ERROR of type Level Column

8. Sorting

In this operation, client sort the data on the basis of columns fields. The Sort operation is fully performed by the Backend Server i.e using Python REST API Service and the results are directly displayed on the Angular i.e on Client Side.

Figure 16 : Sorting on column Type

Figure 17 : Sorting on Column Date

28

Chapter - 5

TEST PLAN

Table 3: Number of different tests to be performed

Type of Test	Will Test Be Performed?	Comments/Explanations	Software Component
Requirements Testing	Yes	We need to check if the requirements of users are met or not	All Modules
Unit Testing	Yes	We need to test all the modules.	All Modules
Integration	Yes	We need to test if all the stages work synchronously	All Modules
Performance	Yes	We need to test the accuracy of the model at the last module.	All Modules
Stress	Yes	We need to test the stress on the system while executing the application.	All Modules
Compliance	Yes	The application must be compatible with the system.	All Modules
Security	No	There are no security issues	None
Load	Yes	We need to make sure that the system does not get overwhelmed by loading the data from social networking website or news websites.	All Modules

Chapter – 6

RESULT ANALYSIS

Output LOG FILES

- Android Structured Log File

LineId	Date	Time	Pid	Tid	Level	Component	Content
1	Mar-17	13:38.8	1702	2395	D	WindowManager	printFreezingDisplayLogsopening app wtoken = AppWindowToken{9f4ef63 token=Token{a64f992 ActivityRecord
2	Mar-17	13:38.8	1702	8671	D	PowerManagerService	acquire lock=233570404, flags=0x1, tag="View Lock", name=com.android.systemui, ws=null, uid=10037, pid=2227
3	Mar-17	13:38.8	1702	8671	D	PowerManagerService	ready=true,policy=3,wakefulness=1,wksummary=0x23,uasummary=0x1,bootcompleted=true,boostinprogress=f
4	Mar-17	13:38.8	1702	2113	V	WindowManager	Skipping AppWindowToken{df0798e token=Token{78af589 ActivityRecord{3b04890 u0 com.tencent.qt.qtl/com.t
5	Mar-17	13:38.9	2227	2227	D	TextView	visible is system.time.showampm
6	Mar-17	13:38.9	2227	2227	D	TextView	mVisiblity.getValue is false
7	Mar-17	13:38.9	2227	2227	D	TextView	visible is system.charge.show
8	Mar-17	13:38.9	2227	2227	D	TextView	mVisiblity.getValue is false
9	Mar-17	13:38.9	2227	2227	D	TextView	visible is system.call.count gt 0
10	Mar-17	13:38.9	2227	2227	D	TextView	mVisiblity.getValue is false
11	Mar-17	13:38.9	2227	2227	D	TextView	visible is system.message.count gt 0
12	Mar-17	13:38.9	2227	2227	D	TextView	mVisiblity.getValue is false
13	Mar-17	13:38.9	2227	2227	D	TextView	visible is system.ownerinfo.show
14	Mar-17	13:38.9	2227	2227	D	TextView	mVisiblity.getValue is false
15	Mar-17	13:38.9	1702	10454	D	PowerManagerService	release:lock=233570404, flg=0x0, tag="View Lock", name=com.android.systemui, ws=null, uid=10037, pid=2227
16	Mar-17	13:38.9	1702	10454	D	PowerManagerService	ready=true,policy=3,wakefulness=1,wksummary=0x23,uasummary=0x1,bootcompleted=true,boostinprogress=f
17	Mar-17	13:38.9	1702	3693	V	WindowManager	Skipping AppWindowToken{df0798e token=Token{78af589 ActivityRecord{3b04890 u0 com.tencent.qt.qtl/com.t
18	Mar-17	13:38.9	2227	2227	I	StackScrollAlgorithm	updateClipping isOverlap:false, getTopPadding=333.0, Translation=-24.0
19	Mar-17	13:38.9	2227	2227	I	StackScrollAlgorithm	updateDimmedActivatedHideSensitive overlap:false
20	Mar-17	13:38.9	1702	3697	W	ActivityManager	getRunningAppProcesses: caller 10113 does not hold REAL_GET_TASKS; limiting output
21	Mar-17	13:38.9	1702	14638	D	PowerManagerService	release:lock=189667585, flg=0x0, tag="*launch*", name=android", ws=WorkSource{10113}, uid=1000, pid=1702
22	Mar-17	13:38.9	1702	14638	D	PowerManagerService	ready=true,policy=3,wakefulness=1,wksummary=0x23,uasummary=0x1,bootcompleted=true,boostinprogress=f
23	Mar-17	13:39.0	2227	2227	I	PhoneStatusBar	setSystemUiVisibility vis=40000500 mask=ffffffff oldVal=508 newVal=40000500 diff=40000000 fullscreenStackVis=
24	Mar-17	13:39.0	2227	2227	I	PhoneStatusBar	cancelAutohide
25	Mar-17	13:39.0	2227	2227	I	PhoneStatusBar	notifyUiVisibilityChanged:vis=0x40000500, SystemUiVisibility=0x40000500
26	Mar-17	13:39.0	1702	27365	I	WindowManager	Destroying surface Surface(name=SurfaceView - com.tencent.qt.qtl/com.tencent.video.player.activity.PlayerAc
27	Mar-17	13:39.0	1702	2639	I	WindowManager	Destroying surface Surface(name=com.tencent.qt.qtl/com.tencent.video.player.activity.PlayerActivity) called b
28	Mar-17	13:39.0	1702	2639	D	PowerManagerService	release:lock=62617001, flg=0x0, tag="WindowManager", name=android", ws=WorkSource{10113}, uid=1000, pid=

- Apache Structured Log File

LineId	Time	Level	Content
1	Sun Dec 04 04:47:44 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
2	Sun Dec 04 04:47:44 2005	error	mod_jk child workerEnv in error state 6
3	Sun Dec 04 04:51:08 2005	notice	jk2_init() Found child 6725 in scoreboard slot 10
4	Sun Dec 04 04:51:09 2005	notice	jk2_init() Found child 6726 in scoreboard slot 8
5	Sun Dec 04 04:51:09 2005	notice	jk2_init() Found child 6728 in scoreboard slot 6
6	Sun Dec 04 04:51:14 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
7	Sun Dec 04 04:51:14 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
8	Sun Dec 04 04:51:14 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
9	Sun Dec 04 04:51:18 2005	error	mod_jk child workerEnv in error state 6
10	Sun Dec 04 04:51:18 2005	error	mod_jk child workerEnv in error state 6
11	Sun Dec 04 04:51:18 2005	error	mod_jk child workerEnv in error state 6
12	Sun Dec 04 04:51:37 2005	notice	jk2_init() Found child 6736 in scoreboard slot 10
13	Sun Dec 04 04:51:38 2005	notice	jk2_init() Found child 6733 in scoreboard slot 7
14	Sun Dec 04 04:51:38 2005	notice	jk2_init() Found child 6734 in scoreboard slot 9
15	Sun Dec 04 04:51:52 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
16	Sun Dec 04 04:51:52 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
17	Sun Dec 04 04:51:55 2005	error	mod_jk child workerEnv in error state 6
18	Sun Dec 04 04:52:04 2005	notice	jk2_init() Found child 6738 in scoreboard slot 6
19	Sun Dec 04 04:52:04 2005	notice	jk2_init() Found child 6741 in scoreboard slot 9
20	Sun Dec 04 04:52:05 2005	notice	jk2_init() Found child 6740 in scoreboard slot 7
21	Sun Dec 04 04:52:05 2005	notice	jk2_init() Found child 6737 in scoreboard slot 8
22	Sun Dec 04 04:52:12 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
23	Sun Dec 04 04:52:12 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
24	Sun Dec 04 04:52:12 2005	notice	workerEnv.init() ok /etc/httpd/conf/workers2.properties
25	Sun Dec 04 04:52:15 2005	error	mod_jk child workerEnv in error state 6
26	Sun Dec 04 04:52:15 2005	error	mod_jk child workerEnv in error state 7
27	Sun Dec 04 04:52:15 2005	error	mod_jk child workerEnv in error state 7
28	Sun Dec 04 04:52:36 2005	notice	jk2_init() Found child 6748 in scoreboard slot 6

- **BGL Structured Log File**

LineId	Label	Timestamp	Date	Node	Time	NodeRepeat	Type	Component	Level	Content
1	-	1117838570	2005.06.03	R02-M1-N0-C:J12-U11	2005-06-03-15.42.50.675872	R02-M1-N0-C:J12-U11	RAS	KERNEL	INFO	instruction cache parity error corrected
2	-	1117838573	2005.06.03	R02-M1-N0-C:J12-U11	2005-06-03-15.42.53.276129	R02-M1-N0-C:J12-U11	RAS	KERNEL	INFO	instruction cache parity error corrected
3	-	1117838976	2005.06.03	R02-M1-N0-C:J12-U11	2005-06-03-15.49.36.156884	R02-M1-N0-C:J12-U11	RAS	KERNEL	INFO	instruction cache parity error corrected
4	-	1117838978	2005.06.03	R02-M1-N0-C:J12-U11	2005-06-03-15.49.38.026704	R02-M1-N0-C:J12-U11	RAS	KERNEL	INFO	instruction cache parity error corrected
5	-	1117842440	2005.06.03	R23-M0-NE-C:J05-U01	2005-06-03-16.47.20.730545	R23-M0-NE-C:J05-U01	RAS	KERNEL	INFO	63543 double-hummer alignment exceptions
6	-	1117842974	2005.06.03	R24-M0-N1-C:J13-U11	2005-06-03-16.56.14.254137	R24-M0-N1-C:J13-U11	RAS	KERNEL	INFO	162 double-hummer alignment exceptions
7	-	1117843015	2005.06.03	R21-M1-N6-C:J08-U11	2005-06-03-16.56.55.309974	R21-M1-N6-C:J08-U11	RAS	KERNEL	INFO	141 double-hummer alignment exceptions
8	-	1117848119	2005.06.03	R16-M1-N2-C:J17-U01	2005-06-03-18.21.59.871925	R16-M1-N2-C:J17-U01	RAS	KERNEL	INFO	CE sym 2, at 0x0b85eee0, mask 0x05
9	APPREAD	1117869872	2005.06.04	R04-M1-N4-I:J18-U11	2005-06-04-00.24.32.432192	R04-M1-N4-I:J18-U11	RAS	APP	FATAL	ciod: failed to read message prefix on control stream (
10	APPREAD	1117869876	2005.06.04	R27-M1-N4-I:J18-U01	2005-06-04-00.24.36.222560	R27-M1-N4-I:J18-U01	RAS	APP	FATAL	ciod: failed to read message prefix on control stream (
11	-	1117942120	2005.06.04	R30-M0-N7-C:J08-U01	2005-06-04-20.28.40.767551	R30-M0-N7-C:J08-U01	RAS	KERNEL	INFO	CE sym 20, at 0x1438f9e0, mask 0x40
12	-	1117955341	2005.06.05	R25-M0-N7-C:J02-U01	2005-06-05-00.09.01.903373	R25-M0-N7-C:J02-U01	RAS	KERNEL	INFO	generating core.2275
13	-	1117955392	2005.06.05	R24-M1-N8-C:J09-U11	2005-06-05-00.09.52.516674	R24-M1-N8-C:J09-U11	RAS	KERNEL	INFO	generating core.862
14	-	1117956980	2005.06.05	R24-M1-NB-C:J15-U11	2005-06-05-00.36.20.945796	R24-M1-NB-C:J15-U11	RAS	KERNEL	INFO	generating core.728
15	-	1117957045	2005.06.05	R20-M1-N8-C:J04-U01	2005-06-05-00.37.25.012681	R20-M1-N8-C:J04-U01	RAS	KERNEL	INFO	generating core.775
16	-	1117959501	2005.06.05	R24-M0-NE-C:J14-U11	2005-06-05-01.18.21.778604	R24-M0-NE-C:J14-U11	RAS	KERNEL	INFO	generating core.3276
17	-	1117959513	2005.06.05	R21-M1-N2-C:J11-U01	2005-06-05-01.18.33.830595	R21-M1-N2-C:J11-U01	RAS	KERNEL	INFO	generating core.1717
18	-	1117959563	2005.06.05	R24-M0-N8-C:J04-U11	2005-06-05-01.19.23.822135	R24-M0-N8-C:J04-U11	RAS	KERNEL	INFO	generating core.3919
19	-	1117973759	2005.06.05	R31-M0-NE-C:J05-U11	2005-06-05-05.15.59.416717	R31-M0-NE-C:J05-U11	RAS	KERNEL	INFO	generating core.2079
20	-	1117973786	2005.06.05	R36-M0-NA-C:J06-U01	2005-06-05-05.16.26.686603	R36-M0-NA-C:J06-U01	RAS	KERNEL	INFO	generating core.1414
21	-	1117973919	2005.06.05	R33-M0-N4-C:J02-U11	2005-06-05-05.18.39.396608	R33-M0-N4-C:J02-U11	RAS	KERNEL	INFO	generating core.3055
22	-	1117974206	2005.06.05	R22-M0-ND-C:J10-U11	2005-06-05-05.23.26.239153	R22-M0-ND-C:J10-U11	RAS	KERNEL	INFO	generating core.201
23	-	1117974463	2005.06.05	R27-M0-N6-C:J10-U01	2005-06-05-05.27.43.336565	R27-M0-N6-C:J10-U01	RAS	KERNEL	INFO	generating core.1125
24	-	1117975251	2005.06.05	R26-M1-N8-C:J17-U11	2005-06-05-05.40.51.726735	R26-M1-N8-C:J17-U11	RAS	KERNEL	INFO	generating core.412
25	-	1117976658	2005.06.05	R36-M1-N8-C:J17-U01	2005-06-05-06.04.18.406158	R36-M1-N8-C:J17-U01	RAS	KERNEL	INFO	generating core.7828
26	-	1117977497	2005.06.05	R33-M1-NB-C:J06-U01	2005-06-05-06.18.17.802159	R33-M1-NB-C:J06-U01	RAS	KERNEL	INFO	generating core.5570
27	-	1117979227	2005.06.05	R01-M1-N7-C:J04-U11	2005-06-05-06.47.07.157021	R01-M1-N7-C:J04-U11	RAS	KERNEL	INFO	generating core.8275
28	-	1117982609	2005.06.05	R35-M1-NE-C:J05-U01	2005-06-05-07.43.29.979844	R35-M1-NE-C:J05-U01	RAS	KERNEL	INFO	generating core.4183

- **Hadoop Structured Log File**

LineId	Date	Time	Level	Process	Component	Content
1	18-10-15	18:01:47,978	INFO	main	org.apache.hadoop.mapreduce.v2.app.MRAppMaster	Created MRAppMaster for application appattempt_1445144423722_0020_000001
2	18-10-15	18:01:48,963	INFO	main	org.apache.hadoop.mapreduce.v2.app.MRAppMaster	Executing with tokens:
3	18-10-15	18:01:48,963	INFO	main	org.apache.hadoop.mapreduce.v2.app.MRAppMaster	Kind: YARN_AM_RM_TOKEN, Service: , Ident: (appAttemptId { application_id { id: 2
4	18-10-15	18:01:49,228	INFO	main	org.apache.hadoop.mapreduce.v2.app.MRAppMaster	Using mapred newApiCommitter.
5	18-10-15	18:01:50,353	INFO	main	org.apache.hadoop.mapreduce.v2.app.MRAppMaster	OutputCommitter set in config null
6	18-10-15	18:01:50,509	INFO	main	org.apache.hadoop.mapreduce.v2.app.MRAppMaster	OutputCommitter is org.apache.hadoop.mapreduce.lib.output.FileOutputCommit
7	18-10-15	18:01:50,556	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.jobhistory.EventType for class org
8	18-10-15	18:01:50,556	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.v2.app.job.event.JobEventType f
9	18-10-15	18:01:50,556	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.v2.app.job.event.TaskEventType
10	18-10-15	18:01:50,556	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.v2.app.job.event.TaskAttemptEve
11	18-10-15	18:01:50,572	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.v2.app.commit.CommitterEventT
12	18-10-15	18:01:50,572	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.v2.app.speculate.Speculator$Eve
13	18-10-15	18:01:50,572	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.v2.app.rm.ContainerAllocator$Ev
14	18-10-15	18:01:50,588	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.v2.app.launcher.ContainerLaunch
15	18-10-15	18:01:50,634	INFO	main	org.apache.hadoop.mapreduce.v2.jobhistory.JobHistoryUtils	Default file system [hdfs://msra-sa-41:9000]
16	18-10-15	18:01:50,666	INFO	main	org.apache.hadoop.mapreduce.v2.jobhistory.JobHistoryUtils	Default file system [hdfs://msra-sa-41:9000]
17	18-10-15	18:01:50,713	INFO	main	org.apache.hadoop.mapreduce.v2.jobhistory.JobHistoryUtils	Default file system [hdfs://msra-sa-41:9000]
18	18-10-15	18:01:50,728	INFO	main	org.apache.hadoop.mapreduce.jobhistory.JobHistoryEventHandler	Emitting job history data to the timeline server is not enabled
19	18-10-15	18:01:50,806	INFO	main	org.apache.hadoop.yarn.event.AsyncDispatcher	Registering class org.apache.hadoop.mapreduce.v2.app.job.event.JobFinishEvent$
20	18-10-15	18:01:51,197	INFO	main	org.apache.hadoop.metrics2.impl.MetricsConfig	loaded properties from hadoop-metrics2.properties
21	18-10-15	18:01:51,306	INFO	main	org.apache.hadoop.metrics2.impl.MetricsSystemImpl	Scheduled snapshot period at 10 second(s).
22	18-10-15	18:01:51,306	INFO	main	org.apache.hadoop.metrics2.impl.MetricsSystemImpl	MRAppMaster metrics system started
23	18-10-15	18:01:51,322	INFO	main	org.apache.hadoop.mapreduce.v2.app.job.impl.JobImpl	Adding job token for job_1445144423722_0020 to jobTokenSecretManager
24	18-10-15	18:01:51,619	INFO	main	org.apache.hadoop.mapreduce.v2.app.job.impl.JobImpl	Not uberizing job_1445144423722_0020 because: not enabled; too many maps; too
25	18-10-15	18:01:51,650	INFO	main	org.apache.hadoop.mapreduce.v2.app.job.impl.JobImpl	Input size for job job_1445144423722_0020 = 1256521728. Number of splits = 10
26	18-10-15	18:01:51,650	INFO	main	org.apache.hadoop.mapreduce.v2.app.job.impl.JobImpl	Number of reduces for job job_1445144423722_0020 = 1
27	18-10-15	18:01:51,650	INFO	main	org.apache.hadoop.mapreduce.v2.app.job.impl.JobImpl	job_1445144423722_0020Job Transitioned from NEW to INITED
28	18-10-15	18:01:51,650	INFO	main	org.apache.hadoop.mapreduce.v2.app.MRAppMaster	MRAppMaster launching normal, non-uberized, multi-container job job_144514442

- ## HDFS Structured Log File

LineId	Date	Time	Pid	Level	Component	Content
1	81109	203615	148	INFO	dfs.DataNode$PacketResponder	PacketResponder 1 for block blk_38865049064139660 terminating
2	81109	203807	222	INFO	dfs.DataNode$PacketResponder	PacketResponder 0 for block blk_-6952295868487656571 terminating
3	81109	204005	35	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.73.220:50010 is added to blk_712837
4	81109	204015	308	INFO	dfs.DataNode$PacketResponder	PacketResponder 2 for block blk_8229193803249955061 terminating
5	81109	204106	329	INFO	dfs.DataNode$PacketResponder	PacketResponder 2 for block blk_-6670958622368987959 terminating
6	81109	204132	26	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.43.115:50010 is added to blk_305092
7	81109	204324	34	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.203.80:50010 is added to blk_788894
8	81109	204453	34	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.250.11.85:50010 is added to blk_2377150
9	81109	204525	512	INFO	dfs.DataNode$PacketResponder	PacketResponder 2 for block blk_572492839287299681 terminating
10	81109	204655	556	INFO	dfs.DataNode$PacketResponder	Received block blk_3587508140051953248 of size 67108864 from /10.251.42.84
11	81109	204722	567	INFO	dfs.DataNode$PacketResponder	Received block blk_5402003568334525940 of size 67108864 from /10.251.214.112
12	81109	204815	653	INFO	dfs.DataNode$DataXceiver	Receiving block blk_5792489080791696128 src: /10.251.30.6:33145 dest: /10.251.30.6:50010
13	81109	204842	663	INFO	dfs.DataNode$DataXceiver	Receiving block blk_1724757848743533110 src: /10.251.111.130:49851 dest: /10.251.111.130:50010
14	81109	204908	31	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.110.8:50010 is added to blk_8015913
15	81109	204925	673	INFO	dfs.DataNode$DataXceiver	Receiving block blk_-5623176793330377570 src: /10.251.75.228:53725 dest: /10.251.75.228:50010
16	81109	205035	28	INFO	dfs.FSNamesystem	BLOCK* NameSystem.allocateBlock: /user/root/rand/_temporary/_task_200811092030_0001_m_00059
17	81109	205056	710	INFO	dfs.DataNode$PacketResponder	PacketResponder 1 for block blk_5017373558217225674 terminating
18	81109	205157	752	INFO	dfs.DataNode$PacketResponder	Received block blk_9212264480425680329 of size 67108864 from /10.251.123.1
19	81109	205315	29	INFO	dfs.FSNamesystem	BLOCK* NameSystem.allocateBlock: /user/root/rand/_temporary/_task_200811092030_0001_m_00074
20	81109	205409	28	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.111.130:50010 is added to blk_45684
21	81109	205412	832	INFO	dfs.DataNode$PacketResponder	Received block blk_-5704899712662113150 of size 67108864 from /10.251.91.229
22	81109	205632	28	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.74.79:50010 is added to blk_-479486
23	81109	205739	29	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.38.197:50010 is added to blk_876366
24	81109	205742	1001	INFO	dfs.DataNode$PacketResponder	Received block blk_-5861636720645142679 of size 67108864 from /10.251.70.211
25	81109	205746	29	INFO	dfs.FSNamesystem	BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.74.134:50010 is added to blk_745381
26	81109	205749	997	INFO	dfs.DataNode$DataXceiver	Receiving block blk_-28342503914935090 src: /10.251.123.132:57542 dest: /10.251.123.132:50010
27	81109	205754	952	INFO	dfs.DataNode$PacketResponder	Received block blk_8291449241650212794 of size 67108864 from /10.251.89.155
28	81109	205858	31	INFO	dfs.FSNamesystem	BLOCK* NameSystem.allocateBlock: /user/root/rand/_temporary/_task_200811092030_0001_m_00048

- ## HPC Structured Log File

LineId	LogId	Node	Component	State	Time	Flag	Content
1	134681	node-246	unix.hw	state_change.unavailable	1077804742	1	Component State Change: Component \042SCSI-WWID:01000010:6005-08b4-0001-00c6-0006
2	350766	node-109	unix.hw	state_change.unavailable	1084680778	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=3180)
3	344518	node-246	unix.hw	state_change.unavailable	1084270955	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=5089)
4	344448	node-153	unix.hw	state_change.unavailable	1084270952	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=4088)
5	366633	node-200	unix.hw	state_change.unavailable	1085100843	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=2538)
6	366463	node-122	unix.hw	state_change.unavailable	1085084674	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=2480)
7	438190	node-228	unix.hw	state_change.unavailable	1097194780	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=3713)
8	225111	node-10	unix.hw	state_change.unavailable	1117296789	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=3891)
9	360778	node-130	unix.hw	state_change.unavailable	1141108031	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=2478)
10	401569	node-169	unix.hw	state_change.unavailable	1142550406	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=2969)
11	401855	node-187	unix.hw	state_change.unavailable	1142553646	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=4159)
12	460773	node-199	unix.hw	state_change.unavailable	1145552100	1	Component State Change: Component \042alt0\042 is in the unavailable state (HWID=2608)
13	2568643	node-70	action	start	1074119817	1	clusterAddMember (command 1902)
14	2570772	node-124	action	start	1074123150	1	clusterAddMember (command 1900)
15	2571927	node-28	action	start	1074125371	1	risBoot (command 1903)
16	2572286	node-17	action	start	1074126278	1	bootGenvmunix (command 1903)
17	2575909	node-162	action	start	1074178193	1	boot (command 1911)
18	2576195	node-181	action	start	1074178628	1	boot (command 1910)
19	2599298	node-198	action	start	1074297419	1	boot (command 1978)
20	2600743	node-57	action	start	1074298084	1	boot (command 1967)
21	2601401	node-184	action	start	1074298390	1	wait (command 1975)
22	2612635	node-88	action	start	1074535847	1	boot (command 1999)
23	2608062	node-238	action	start	1074461014	1	halt (command 1982)
24	2607813	node-243	action	start	1074459063	1	boot (command 1981)
25	2600616	node-152	action	start	1074298056	1	boot (command 1973)
26	2601430	node-159	action	start	1074298398	1	wait (command 1973)
27	3515	node-216	action	start	1075629790	1	wait (command 2057)
28	41108	node-93	action	start	1076538873	1	boot (command 2152)

- Linux Structured Log File

LineId	Month	Date	Time	Level	Component	PID	Content
1	Jun	14	15:16:01	combo	sshd(pam_unix)	19939	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4
2	Jun	14	15:16:02	combo	sshd(pam_unix)	19937	check pass; user unknown
3	Jun	14	15:16:02	combo	sshd(pam_unix)	19937	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4
4	Jun	15	2:04:59	combo	sshd(pam_unix)	20882	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
5	Jun	15	2:04:59	combo	sshd(pam_unix)	20884	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
6	Jun	15	2:04:59	combo	sshd(pam_unix)	20883	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
7	Jun	15	2:04:59	combo	sshd(pam_unix)	20885	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
8	Jun	15	2:04:59	combo	sshd(pam_unix)	20886	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
9	Jun	15	2:04:59	combo	sshd(pam_unix)	20892	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
10	Jun	15	2:04:59	combo	sshd(pam_unix)	20893	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
11	Jun	15	2:04:59	combo	sshd(pam_unix)	20896	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
12	Jun	15	2:04:59	combo	sshd(pam_unix)	20897	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
13	Jun	15	2:04:59	combo	sshd(pam_unix)	20898	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hine
14	Jun	15	4:06:18	combo	su(pam_unix)	21416	session opened for user cyrus by (uid=0)
15	Jun	15	4:06:19	combo	su(pam_unix)	21416	session closed for user cyrus
16	Jun	15	4:06:20	combo	logrotate		ALERT exited abnormally with [1]
17	Jun	15	4:12:42	combo	su(pam_unix)	22644	session opened for user news by (uid=0)
18	Jun	15	4:12:43	combo	su(pam_unix)	22644	session closed for user news
19	Jun	15	12:12:34	combo	sshd(pam_unix)	23397	check pass; user unknown
20	Jun	15	12:12:34	combo	sshd(pam_unix)	23397	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4
21	Jun	15	12:12:34	combo	sshd(pam_unix)	23395	check pass; user unknown
22	Jun	15	12:12:34	combo	sshd(pam_unix)	23395	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4
23	Jun	15	12:12:34	combo	sshd(pam_unix)	23404	check pass; user unknown
24	Jun	15	12:12:34	combo	sshd(pam_unix)	23404	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4
25	Jun	15	12:12:34	combo	sshd(pam_unix)	23399	check pass; user unknown
26	Jun	15	12:12:34	combo	sshd(pam_unix)	23399	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4
27	Jun	15	12:12:34	combo	sshd(pam_unix)	23406	check pass; user unknown
28	Jun	15	12:12:34	combo	sshd(pam_unix)	23406	authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4

- MAC Structured Log File

LineId	Month	Date	Time	User	Component	PID	Address	Content
1	Jul	1	9:00:55	calvisitor-10-105-160-95	kernel	0		IOThunderboltSwitch<0>(0x0)::listenerCallback - Thunderbolt HPD packet for route = 0x0 port
2	Jul	1	9:01:05	calvisitor-10-105-160-95	com.apple.CDScheduler	43		Thermal pressure state: 1 Memory pressure state: 0
3	Jul	1	9:01:06	calvisitor-10-105-160-95	QQ	10018		FA||Url||taskID[2019352994] dealloc
4	Jul	1	9:02:26	calvisitor-10-105-160-95	kernel	0		ARPT: 620701.011328: AirPort_Brcm43xx::syncPowerState: WWEN[enabled]
5	Jul	1	9:02:26	authorMacBook-Pro	kernel	0		ARPT: 620702.879952: AirPort_Brcm43xx::platformWoWEnable: WWEN[disable]
6	Jul	1	9:03:11	calvisitor-10-105-160-95	mDNSResponder	91		mDNS_DeregisterInterface: Frequent transitions for interface awdl0 (FE80:0000:0000:0000:D8
7	Jul	1	9:03:13	calvisitor-10-105-160-95	kernel	0		ARPT: 620749.901374: IOPMPowerSource Information: onSleep, SleepType: Normal Sleep, 'E
8	Jul	1	9:04:33	calvisitor-10-105-160-95	kernel	0		ARPT: 620750.434035: wl0: wl_update_tcpkeep_seq: Original Seq: 3226706533, Ack: 387168717
9	Jul	1	9:04:33	authorMacBook-Pro	kernel	0		ARPT: 620752.337198: ARPT: Wake Reason: Wake on Scan offload
10	Jul	1	9:04:37	authorMacBook-Pro	symptomsd	215		__73-[NetworkAnalyticsEngine observeValueForKeyPath:ofObject:change:context:]_block_ir
11	Jul	1	9:12:20	authorMacBook-Pro	kernel	0		IO80211AWDLPeerManager::setAwdlAutoMode Resuming AWDL
12	Jul	1	9:12:21	calvisitor-10-105-160-95	symptomsd	215		__73-[NetworkAnalyticsEngine observeValueForKeyPath:ofObject:change:context:]_block_ir
13	Jul	1	9:18:16	calvisitor-10-105-160-95	kernel	0		ARPT: 620896.311264: wl0: MDNS: 0 SRV Recs, 0 TXT Recs
14	Jul	1	9:19:03	calvisitor-10-105-160-95	kernel	0		AppleCamIn::systemWakeCall - messageType = 0xE0000340
15	Jul	1	9:19:03	authorMacBook-Pro	configd	53		setting hostname to "authorMacBook-Pro.local"
16	Jul	1	9:19:13	calvisitor-10-105-160-95	com.apple.cts	258		com.apple.icloud.fmfd.heartbeat: scheduler_evaluate_activity told me to run this job; howe
17	Jul	1	9:21:57	authorMacBook-Pro	corecaptured	31174		CCIOReporterFormatter::addRegistryChildToChannelDictionary streams 7
18	Jul	1	9:21:58	calvisitor-10-105-160-95	com.apple.WebKit.WebCc	25654		[09:21:58.929] <<<< CRABS >>>> crabsFlumeHostAvailable: [0x7f961cf08cf0] Byte flume report
19	Jul	1	9:22:02	calvisitor-10-105-160-95	com.apple.cts	258		com.apple.Safari.SafeBrowsing.Update: scheduler_evaluate_activity told me to run this job;
20	Jul	1	9:22:25	calvisitor-10-105-160-95	kernel	0		IO80211AWDLPeerManager::setAwdlAutoMode Resuming AWDL
21	Jul	1	9:23:26	calvisitor-10-105-160-95	kernel	0		AirPort: Link Down on awdl0. Reason 1 (Unspecified).
22	Jul	1	9:23:26	calvisitor-10-105-160-95	kernel	0		IOThunderboltSwitch<0>(0x0)::listenerCallback - Thunderbolt HPD packet for route = 0x0 port
23	Jul	1	9:24:13	calvisitor-10-105-160-95	kernel	0		PM response took 2010 ms (54, powerd)
24	Jul	1	9:25:21	calvisitor-10-105-160-95	com.apple.cts	258		com.apple.icloud.fmfd.heartbeat: scheduler_evaluate_activity told me to run this job; howe
25	Jul	1	9:25:45	calvisitor-10-105-160-95	kernel	0		ARPT: 621131.293163: wl0: Roamed or switched channel, reason #8, bssid 5c:50:15:4c:18:13, la:
26	Jul	1	9:25:59	calvisitor-10-105-160-95	kernel	0		ARPT: 621145.554555: IOPMPowerSource Information: onSleep, SleepType: Normal Sleep, 'E
27	Jul	1	9:26:41	calvisitor-10-105-160-95	kernel	0		ARPT: 621146.080894: wl0: wl_update_tcpkeep_seq: Original Seq: 3014995849, Ack: 259099528
28	Jul	1	9:26:43	calvisitor-10-105-160-95	networkd	195		nw_nat64_post_new_ifstate successfully changed NAT64 ifstate from 0x4 to 0x80000000000

- OpenSSH Structured Log File

LineId	Date	Day	Time	Component	Pid	Content
1	Dec	10	6:55:46	LabSZ	24200	reverse mapping checking getaddrinfo for ns.marryaldkfaczcz.com [173.234.31.186] failed - POSSIBLE BREAK-IN ATTEMPT!
2	Dec	10	6:55:46	LabSZ	24200	Invalid user webmaster from 173.234.31.186
3	Dec	10	6:55:46	LabSZ	24200	input_userauth_request: invalid user webmaster [preauth]
4	Dec	10	6:55:46	LabSZ	24200	pam_unix(sshd:auth): check pass; user unknown
5	Dec	10	6:55:46	LabSZ	24200	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=173.234.31.186
6	Dec	10	6:55:48	LabSZ	24200	Failed password for invalid user webmaster from 173.234.31.186 port 38926 ssh2
7	Dec	10	6:55:48	LabSZ	24200	Connection closed by 173.234.31.186 [preauth]
8	Dec	10	7:02:47	LabSZ	24203	Connection closed by 212.47.254.145 [preauth]
9	Dec	10	7:07:38	LabSZ	24206	Invalid user test9 from 52.80.34.196
10	Dec	10	7:07:38	LabSZ	24206	input_userauth_request: invalid user test9 [preauth]
11	Dec	10	7:07:38	LabSZ	24206	pam_unix(sshd:auth): check pass; user unknown
12	Dec	10	7:07:38	LabSZ	24206	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=ec2-52-80-34-196.cn-north-1.compute.amazona
13	Dec	10	7:07:45	LabSZ	24206	Failed password for invalid user test9 from 52.80.34.196 port 36060 ssh2
14	Dec	10	7:07:45	LabSZ	24206	Received disconnect from 52.80.34.196: 11: Bye Bye [preauth]
15	Dec	10	7:08:28	LabSZ	24208	reverse mapping checking getaddrinfo for ns.marryaldkfaczcz.com [173.234.31.186] failed - POSSIBLE BREAK-IN ATTEMPT!
16	Dec	10	7:08:28	LabSZ	24208	Invalid user webmaster from 173.234.31.186
17	Dec	10	7:08:28	LabSZ	24208	input_userauth_request: invalid user webmaster [preauth]
18	Dec	10	7:08:28	LabSZ	24208	pam_unix(sshd:auth): check pass; user unknown
19	Dec	10	7:08:28	LabSZ	24208	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=173.234.31.186
20	Dec	10	7:08:30	LabSZ	24208	Failed password for invalid user webmaster from 173.234.31.186 port 39257 ssh2
21	Dec	10	7:08:30	LabSZ	24208	Connection closed by 173.234.31.186 [preauth]
22	Dec	10	7:11:42	LabSZ	24224	Invalid user chen from 202.100.179.208
23	Dec	10	7:11:42	LabSZ	24224	input_userauth_request: invalid user chen [preauth]
24	Dec	10	7:11:42	LabSZ	24224	pam_unix(sshd:auth): check pass; user unknown
25	Dec	10	7:11:42	LabSZ	24224	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.100.179.208
26	Dec	10	7:11:44	LabSZ	24224	Failed password for invalid user chen from 202.100.179.208 port 32484 ssh2
27	Dec	10	7:11:44	LabSZ	24224	Received disconnect from 202.100.179.208: 11: Bye Bye [preauth]
28	Dec	10	7:13:31	LabSZ	24227	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=5.36.59.76.dynamic-dsl-ip.omantel.net.om use

- OpenStack Structured Log File

LineId	Logrecord	Date	Time	Pid	Level	Component	ADDR	Content
1	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:00.0	25746	INFO	nova.osapi_compute.wsgi.server	req-38101a0b	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
2	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:00.3	25746	INFO	nova.osapi_compute.wsgi.server	req-9bc36dd9	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
3	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:01.6	25746	INFO	nova.osapi_compute.wsgi.server	req-55db2d8c	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
4	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:01.8	25746	INFO	nova.osapi_compute.wsgi.server	req-2a3dc421	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
5	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:03.1	25746	INFO	nova.osapi_compute.wsgi.server	req-939eb332	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
6	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:03.4	25746	INFO	nova.osapi_compute.wsgi.server	req-b6a4fa91	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
7	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:04.5	2931	INFO	nova.compute.manager	req-3ea4052c	[instance: b9000564-fe1a-409b-b8cc-1e88b294cd1d
8	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:04.6	2931	INFO	nova.compute.manager	req-3ea4052c	[instance: b9000564-fe1a-409b-b8cc-1e88b294cd1d
9	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:04.7	2931	INFO	nova.compute.manager	req-3ea4052c	[instance: b9000564-fe1a-409b-b8cc-1e88b294cd1d
10	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:04.8	25746	INFO	nova.osapi_compute.wsgi.server	req-bbfc3fb8	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
11	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:05.1	25746	INFO	nova.osapi_compute.wsgi.server	req-31826992	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
12	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:05.2	2931	INFO	nova.virt.libvirt.imagecache	req-addc1839	image 0673dd71-34c5-4fbb-86c4-40623fbe45b4 at (/
13	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:05.2	2931	INFO	nova.virt.libvirt.imagecache	req-addc1839	image 0673dd71-34c5-4fbb-86c4-40623fbe45b4 at (/
14	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:05.4	2931	INFO	nova.virt.libvirt.imagecache	req-addc1839	Active base files: /var/lib/nova/instances/_base/a4
15	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:06.3	25746	INFO	nova.osapi_compute.wsgi.server	req-7160b3e7	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
16	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:06.6	25746	INFO	nova.osapi_compute.wsgi.server	req-e46f1fc1	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
17	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:07.9	25746	INFO	nova.osapi_compute.wsgi.server	req-546e2e6a	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
18	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:08.1	25746	INFO	nova.osapi_compute.wsgi.server	req-e2c35e53	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
19	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:09.4	25746	INFO	nova.osapi_compute.wsgi.server	req-ce9c8a59	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
20	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:09.7	25746	INFO	nova.osapi_compute.wsgi.server	req-e1da47c6	10.11.10.1 "GET /v2/54fadb412c4e40cdbaed9335e4c
21	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:10.3	25743	INFO	nova.api.openstack.compute.server_	req-ab451068	Creating event network-vif-plugged:e3871ffd-5cd5
22	nova-api.log.1.2017-05-16_13:53:08	16-05-17	00:10.3	25743	INFO	nova.osapi_compute.wsgi.server	req-ab451068	10.11.10.1 "POST /v2/e9746973ac574c6b8a9e8857f5
23	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:10.3	2931	INFO	nova.compute.manager	req-3ea4052c	[instance: b9000564-fe1a-409b-b8cc-1e88b294cd1d
24	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:10.3	2931	INFO	nova.virt.libvirt.driver	-	[instance: b9000564-fe1a-409b-b8cc-1e88b294cd1d
25	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:10.3	2931	INFO	nova.compute.manager	req-8e64797b	[instance: b9000564-fe1a-409b-b8cc-1e88b294cd1d
26	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:10.4	2931	INFO	nova.compute.manager	req-3ea4052c	[instance: b9000564-fe1a-409b-b8cc-1e88b294cd1d
27	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:10.4	2931	INFO	nova.compute.manager	req-3ea4052c	[instance: b9000564-fe1a-409b-b8cc-1e88b294cd1d
28	nova-compute.log.1.2017-05-16_13:55:31	16-05-17	00:10.4	2931	INFO	nova.virt.libvirt.imagecache	req-addc1839	image 0673dd71-34c5-4fbb-86c4-40623fbe45b4 at (/

- ## Proxifier Structured Log File

LineId	Time	Program	Content
1	10.30 16:49:06	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
2	10.30 16:49:06	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
3	10.30 16:49:06	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
4	10.30 16:49:07	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 0 bytes sent, 0 bytes received, lifetime 00:01
5	10.30 16:49:07	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
6	10.30 16:49:07	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
7	10.30 16:49:07	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
8	10.30 16:49:07	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 403 bytes sent, 426 bytes received, lifetime <1 sec
9	10.30 16:49:07	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
10	10.30 16:49:07	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
11	10.30 16:49:07	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 451 bytes sent, 18846 bytes (18.4 KB) received, lifetime <1 sec
12	10.30 16:49:08	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 445 bytes sent, 5174 bytes (5.05 KB) received, lifetime <1 sec
13	10.30 16:49:08	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
14	10.30 16:49:08	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 1190 bytes (1.16 KB) sent, 1671 bytes (1.63 KB) received, lifetime 00:02
15	10.30 16:49:08	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
16	10.30 16:49:08	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 0 bytes sent, 0 bytes received, lifetime <1 sec
17	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 1165 bytes (1.13 KB) sent, 3098 bytes (3.02 KB) received, lifetime 00:01
18	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
19	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 1165 bytes (1.13 KB) sent, 815 bytes received, lifetime <1 sec
20	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
21	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 1165 bytes (1.13 KB) sent, 783 bytes received, lifetime <1 sec
22	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 850 bytes sent, 10547 bytes (10.2 KB) received, lifetime 00:02
23	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 408 bytes sent, 421 bytes received, lifetime 00:03
24	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 1165 bytes (1.13 KB) sent, 0 bytes received, lifetime <1 sec
25	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
26	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 open through proxy proxy.cse.cuhk.edu.hk:5070 HTTPS
27	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 0 bytes sent, 0 bytes received, lifetime <1 sec
28	10.30 16:49:09	chrome.exe	proxy.cse.cuhk.edu.hk:5070 close, 19904 bytes (19.4 KB) sent, 27629 bytes (26.9 KB) received, lifetime 02:19

- ## Spark Structured Log File

LineId	Date	Time	Level	Component	Content
1	17-06-09	20:10:40	INFO	executor.CoarseGrainedExecutorBackend	Registered signal handlers for [TERM, HUP, INT]
2	17-06-09	20:10:40	INFO	spark.SecurityManager	Changing view acls to: yarn,curi
3	17-06-09	20:10:40	INFO	spark.SecurityManager	Changing modify acls to: yarn,curi
4	17-06-09	20:10:40	INFO	spark.SecurityManager	SecurityManager: authentication disabled; ui acls disabled; users with view permissions: Set(yarn, curi); use
5	17-06-09	20:10:41	INFO	spark.SecurityManager	Changing view acls to: yarn,curi
6	17-06-09	20:10:41	INFO	spark.SecurityManager	Changing modify acls to: yarn,curi
7	17-06-09	20:10:41	INFO	spark.SecurityManager	SecurityManager: authentication disabled; ui acls disabled; users with view permissions: Set(yarn, curi); use
8	17-06-09	20:10:41	INFO	slf4j.Slf4jLogger	Slf4jLogger started
9	17-06-09	20:10:41	INFO	Remoting	Starting remoting
10	17-06-09	20:10:41	INFO	Remoting	Remoting started; listening on addresses :[akka.tcp://sparkExecutorActorSystem@mesos-slave-07:55904]
11	17-06-09	20:10:41	INFO	util.Utils	Successfully started service 'sparkExecutorActorSystem' on port 55904.
12	17-06-09	20:10:41	INFO	storage.DiskBlockManager	Created local directory at /opt/hdfs/nodemanager/usercache/curi/appcache/application_1485248649253_01
13	17-06-09	20:10:41	INFO	storage.MemoryStore	MemoryStore started with capacity 17.7 GB
14	17-06-09	20:10:42	INFO	executor.CoarseGrainedExecutorBackend	Connecting to driver: spark://CoarseGrainedScheduler@10.10.34.11:48069
15	17-06-09	20:10:42	INFO	executor.CoarseGrainedExecutorBackend	Successfully registered with driver
16	17-06-09	20:10:42	INFO	executor.Executor	Starting executor ID 5 on host mesos-slave-07
17	17-06-09	20:10:42	INFO	util.Utils	Successfully started service 'org.apache.spark.network.netty.NettyBlockTransferService' on port 40984.
18	17-06-09	20:10:42	INFO	netty.NettyBlockTransferService	Server created on 40984
19	17-06-09	20:10:42	INFO	storage.BlockManagerMaster	Trying to register BlockManager
20	17-06-09	20:10:42	INFO	storage.BlockManagerMaster	Registered BlockManager
21	17-06-09	20:10:45	INFO	executor.CoarseGrainedExecutorBackend	Got assigned task 0
22	17-06-09	20:10:45	INFO	executor.CoarseGrainedExecutorBackend	Got assigned task 1
23	17-06-09	20:10:45	INFO	executor.CoarseGrainedExecutorBackend	Got assigned task 2
24	17-06-09	20:10:45	INFO	executor.CoarseGrainedExecutorBackend	Got assigned task 3
25	17-06-09	20:10:45	INFO	executor.Executor	Running task 0.0 in stage 0.0 (TID 0)
26	17-06-09	20:10:45	INFO	executor.Executor	Running task 2.0 in stage 0.0 (TID 2)
27	17-06-09	20:10:45	INFO	executor.Executor	Running task 1.0 in stage 0.0 (TID 1)
28	17-06-09	20:10:45	INFO	executor.Executor	Running task 3.0 in stage 0.0 (TID 3)

- ● Thunder Bird Structured Log File

LineId	Label	Timestamp	Date	User	Month	Day	Time	Location	Component	PID	Content
1	-	1131566461	2005.11.09	dn228	Nov	9	12:01:01	dn228/dn228	crond(pam_unix)	2915	session closed for user root
2	-	1131566461	2005.11.09	dn228	Nov	9	12:01:01	dn228/dn228	crond(pam_unix)	2915	session opened for user root by (uid=0)
3	-	1131566461	2005.11.09	dn228	Nov	9	12:01:01	dn228/dn228	crond	2916	(root) CMD (run-parts /etc/cron.hourly)
4	-	1131566461	2005.11.09	dn261	Nov	9	12:01:01	dn261/dn261	crond(pam_unix)	2907	session closed for user root
5	-	1131566461	2005.11.09	dn261	Nov	9	12:01:01	dn261/dn261	crond(pam_unix)	2907	session opened for user root by (uid=0)
6	-	1131566461	2005.11.09	dn261	Nov	9	12:01:01	dn261/dn261	crond	2908	(root) CMD (run-parts /etc/cron.hourly)
7	-	1131566461	2005.11.09	dn3	Nov	9	12:01:01	dn3/dn3	crond(pam_unix)	2907	session closed for user root
8	-	1131566461	2005.11.09	dn3	Nov	9	12:01:01	dn3/dn3	crond(pam_unix)	2907	session opened for user root by (uid=0)
9	-	1131566461	2005.11.09	dn3	Nov	9	12:01:01	dn3/dn3	crond	2908	(root) CMD (run-parts /etc/cron.hourly)
10	-	1131566461	2005.11.09	dn596	Nov	9	12:01:01	dn596/dn596	crond(pam_unix)	2727	session closed for user root
11	-	1131566461	2005.11.09	dn596	Nov	9	12:01:01	dn596/dn596	crond(pam_unix)	2727	session opened for user root by (uid=0)
12	-	1131566461	2005.11.09	dn596	Nov	9	12:01:01	dn596/dn596	crond	2728	(root) CMD (run-parts /etc/cron.hourly)
13	-	1131566461	2005.11.09	dn700	Nov	9	12:01:01	dn700/dn700	crond(pam_unix)	2912	session closed for user root
14	-	1131566461	2005.11.09	dn700	Nov	9	12:01:01	dn700/dn700	crond(pam_unix)	2912	session opened for user root by (uid=0)
15	-	1131566461	2005.11.09	dn700	Nov	9	12:01:01	dn700/dn700	crond	2913	(root) CMD (run-parts /etc/cron.hourly)
16	-	1131566461	2005.11.09	dn73	Nov	9	12:01:01	dn73/dn73	crond(pam_unix)	2917	session closed for user root
17	-	1131566461	2005.11.09	dn73	Nov	9	12:01:01	dn73/dn73	crond(pam_unix)	2917	session opened for user root by (uid=0)
18	-	1131566461	2005.11.09	dn73	Nov	9	12:01:01	dn73/dn73	crond	2918	(root) CMD (run-parts /etc/cron.hourly)
19	-	1131566461	2005.11.09	dn731	Nov	9	12:01:01	dn731/dn731	crond(pam_unix)	2916	session closed for user root
20	-	1131566461	2005.11.09	dn731	Nov	9	12:01:01	dn731/dn731	crond(pam_unix)	2916	session opened for user root by (uid=0)
21	-	1131566461	2005.11.09	dn731	Nov	9	12:01:01	dn731/dn731	crond	2917	(root) CMD (run-parts /etc/cron.hourly)
22	-	1131566461	2005.11.09	dn754	Nov	9	12:01:01	dn754/dn754	crond(pam_unix)	2913	session closed for user root
23	-	1131566461	2005.11.09	dn754	Nov	9	12:01:01	dn754/dn754	crond(pam_unix)	2913	session opened for user root by (uid=0)
24	-	1131566461	2005.11.09	dn754	Nov	9	12:01:01	dn754/dn754	crond	2914	(root) CMD (run-parts /etc/cron.hourly)
25	-	1131566461	2005.11.09	dn978	Nov	9	12:01:01	dn978/dn978	crond(pam_unix)	2920	session closed for user root
26	-	1131566461	2005.11.09	dn978	Nov	9	12:01:01	dn978/dn978	crond(pam_unix)	2920	session opened for user root by (uid=0)
27	-	1131566461	2005.11.09	dn978	Nov	9	12:01:01	dn978/dn978	crond	2921	(root) CMD (run-parts /etc/cron.hourly)
28	-	1131566461	2005.11.09	eadmin1	Nov	9	12:01:01	src@eadmin1	crond(pam_unix)	4307	session closed for user root

- ● Windows Structured Log File

LineId	Date	Time	Level	Component	Content
1	28-09-16	4:30:30	Info	CBS	Loaded Servicing Stack v6.1.7601.23505 with Core: C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e3!
2	28-09-16	4:30:31	Info	CSI	00000001@2016/9/27:20:30:31.455 WcpInitialize (wcp.dll version 0.0.0.6) called (stack @0x7fed806eb5d @0x7fef9fb9b6d @0x7fef9f8
3	28-09-16	4:30:31	Info	CSI	00000002@2016/9/27:20:30:31.458 WcpInitialize (wcp.dll version 0.0.0.6) called (stack @0x7fed806eb5d @0x7fefa006ade @0x7fef9fd
4	28-09-16	4:30:31	Info	CSI	00000003@2016/9/27:20:30:31.458 WcpInitialize (wcp.dll version 0.0.0.6) called (stack @0x7fed806eb5d @0x7fefa1c8728 @0x7fefa1c
5	28-09-16	4:30:31	Info	CBS	Ending TrustedInstaller initialization.
6	28-09-16	4:30:31	Info	CBS	Starting the TrustedInstaller main loop.
7	28-09-16	4:30:31	Info	CBS	TrustedInstaller service starts successfully.
8	28-09-16	4:30:31	Info	CBS	SQM: Initializing online with Windows opt-in: False
9	28-09-16	4:30:31	Info	CBS	SQM: Cleaning up report files older than 10 days.
10	28-09-16	4:30:31	Info	CBS	SQM: Requesting upload of all unsent reports.
11	28-09-16	4:30:31	Info	CBS	SQM: Failed to start upload with file pattern: C:\Windows\servicing\sqm*_std.sqm, flags: 0x2 [HRESULT = 0x80004005 - E_FAIL]
12	28-09-16	4:30:31	Info	CBS	SQM: Failed to start standard sample upload. [HRESULT = 0x80004005 - E_FAIL]
13	28-09-16	4:30:31	Info	CBS	SQM: Queued 0 file(s) for upload with pattern: C:\Windows\servicing\sqm*_all.sqm, flags: 0x6
14	28-09-16	4:30:31	Info	CBS	SQM: Warning: Failed to upload all unsent reports. [HRESULT = 0x80004005 - E_FAIL]
15	28-09-16	4:30:31	Info	CBS	No startup processing required, TrustedInstaller service was not set as autostart, or else a reboot is still pending.
16	28-09-16	4:30:31	Info	CBS	NonStart: Checking to ensure startup processing was not required.
17	28-09-16	4:30:31	Info	CSI	00000004 IAdvancedInstallerAwareStore_ResolvePendingTransactions (call 1) (flags = 00000004, progress = NULL, phase = 0, pdwDisp
18	28-09-16	4:30:31	Info	CSI	00000005 Creating NT transaction (seq 1), objectname [6]"(null)"
19	28-09-16	4:30:31	Info	CSI	00000006 Created NT transaction (seq 1) result 0x00000000, handle @0x214
20	28-09-16	4:30:31	Info	CSI	00000007@2016/9/27:20:30:31.462 CSI perf trace:
21	28-09-16	4:30:31	Info	CBS	NonStart: Success, startup processing not required as expected.
22	28-09-16	4:30:31	Info	CBS	Startup processing thread terminated normally
23	28-09-16	4:30:31	Info	CSI	00000008 CSI Store 4991456 (0x00000000004c29e0) initialized
24	28-09-16	4:30:31	Info	CBS	Session: 30546173_4261722401 initialized by client WindowsUpdateAgent.
25	28-09-16	4:30:31	Info	CBS	Session: 30546173_4262462443 initialized by client WindowsUpdateAgent.
26	28-09-16	4:30:31	Info	CBS	Warning: Unrecognized packageExtended attribute.
27	28-09-16	4:30:31	Info	CBS	Expecting attribute name [HRESULT = 0x800f080d - CBS_E_MANIFEST_INVALID_ITEM]
28	28-09-16	4:30:31	Info	CBS	Failed to get next element [HRESULT = 0x800f080d - CBS_E_MANIFEST_INVALID_ITEM]

- ZooKeeper Structured Log File

LineId	Date	Time	Level	Node	Component	Id	Content
1	29-07-15	17:41:44,747	INFO	QuorumPeer[myid=1]/0	0:0:0:0:0:0:0:2181:FastLeaderElection	774	Notification time out: 3200
2	29-07-15	19:04:12,394	INFO	/10.10.34.11	3888:QuorumCnxManager$Listener	493	Received connection request /10.10.34.11:45307
3	29-07-15	19:04:29,071	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	688	Send worker leaving thread
4	29-07-15	19:04:29,079	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	679	Interrupted while waiting for message on queue
5	29-07-15	19:13:17,524	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	688	Send worker leaving thread
6	29-07-15	19:13:24,282	WARN	RecvWorker	188978561024:QuorumCnxManager$RecvWorker	762	Connection broken for id 188978561024, my id = 1, error =
7	29-07-15	19:13:24,370	INFO	/10.10.34.11	3888:QuorumCnxManager$Listener	493	Received connection request /10.10.34.13:57707
8	29-07-15	19:13:27,721	WARN	RecvWorker	188978561024:QuorumCnxManager$RecvWorker	762	Connection broken for id 188978561024, my id = 1, error =
9	29-07-15	19:13:34,382	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	679	Interrupted while waiting for message on queue
10	29-07-15	19:13:37,626	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	688	Send worker leaving thread
11	29-07-15	19:13:44,301	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	688	Send worker leaving thread
12	29-07-15	19:13:47,731	WARN	RecvWorker	188978561024:QuorumCnxManager$RecvWorker	762	Connection broken for id 188978561024, my id = 1, error =
13	29-07-15	19:13:54,220	INFO	/10.10.34.11	3888:QuorumCnxManager$Listener	493	Received connection request /10.10.34.11:45382
14	29-07-15	19:13:54,399	WARN	RecvWorker	188978561024:QuorumCnxManager$RecvWorker	762	Connection broken for id 188978561024, my id = 1, error =
15	29-07-15	19:14:04,406	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	679	Interrupted while waiting for message on queue
16	29-07-15	19:14:07,559	WARN	RecvWorker	188978561024:QuorumCnxManager$RecvWorker	765	Interrupting SendWorker
17	29-07-15	19:14:07,653	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	688	Send worker leaving thread
18	29-07-15	19:14:24,329	WARN	RecvWorker	188978561024:QuorumCnxManager$RecvWorker	765	Interrupting SendWorker
19	29-07-15	19:14:37,585	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	679	Interrupted while waiting for message on queue
20	29-07-15	19:14:44,256	INFO	/10.10.34.11	3888:QuorumCnxManager$Listener	493	Received connection request /10.10.34.11:45440
21	29-07-15	19:14:47,593	WARN	RecvWorker	188978561024:QuorumCnxManager$RecvWorker	765	Interrupting SendWorker
22	29-07-15	19:14:54,354	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	688	Send worker leaving thread
23	29-07-15	19:15:24,476	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	679	Interrupted while waiting for message on queue
24	29-07-15	19:15:37,647	WARN	RecvWorker	188978561024:QuorumCnxManager$RecvWorker	765	Interrupting SendWorker
25	29-07-15	19:15:37,648	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	688	Send worker leaving thread
26	29-07-15	19:15:54,407	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	679	Interrupted while waiting for message on queue
27	29-07-15	19:15:57,854	INFO	/10.10.34.11	3888:QuorumCnxManager$Listener	493	Received connection request /10.10.34.13:57895
28	29-07-15	19:16:04,412	WARN	SendWorker	188978561024:QuorumCnxManager$SendWorker	679	Interrupted while waiting for message on queue

References

[1] J. H. Andrews: \Theory and practice of log file analysis." Technical-report 524, Department of Computer Science, University of Western Ontario, May 1998.

[2] J. H. Andrews: \Testing using log file analysis: tools, methods, and issues." Proc. 13 th IEEE International Conference on Automated Software Engineering, Oct. 1998, pp. 157-166.

[3] J. H. Andrews: \A Framework for Log File Analysis." http://citeseer.nj.nec.com/159829.html

[4] J. H. Andrews, Y. Zhang: \Broad-spectrum studies of log file analysis." International Conference on Software Engineering, pages 105-114, 2000

[5] J. H. Andrews: \Testing using Log File Analysis: Tools, Methods, and Issues." available at http://citeseer.nj.nec.com

[6] M. Guzdial, P. Santos, A. Badre, S. Hudson, M. Gray: \Analyzing and visualizing log files: A computational science of usability." Presented at HCI Consortium Workshop, 1994.

[7] M. J. Guzdial: \Deriving software usage patterns from log files." Georgia Institute of Technology. GVU Center Technical Report. Report #93-41. 1993.

[8] Tec-Ed, Inc.: \Assessing Web Site Usability from Server Log Files White Paper." http://citeseer.nj.nec.com/290488.html