International Journal of Web Portals
Volume 10 • Issue 1 • January-June 2018

Analysis Framework for Logs in Communication Devices

Kiran Mary Matthew, VIT University, Chennai Campus, Chennai, India
Abdul Quadir Md, VIT University, Chennai Campus, Chennai, India

ABSTRACT

This article describes how logging is an important mechanism that is being used in almost all kinds of devices. It is used for tracking events during the running of a software. In this case, programs are developed by the software developers in such a way that whenever an event happens it can be recorded. Among its many uses, system troubleshooting is of greatest importance. Manual methods of logging can be adopted when dealing with a smaller process but mostly log sizes can go from kilobytes to terabytes in size for which log analyzing tools are required. In addition to that, those tools should be capable of extracting all the relevant information so that it becomes easy to highlight the ongoing issues in an effective manner. This article proposes a dedicated analysis framework for deep log analysis in communication devices.

KEYWORDS

Communication Device Logs, Log, Log Analysis, Logging, Tools for Log Analysis

1. INTRODUCTION

In computing, a log is a document that contains the details of events in a particular system. Generally, it includes details like IP address of the device, timestamp, process id and the log message. Its format and content can vary based on the domain it is used in. For ease of analysis, logs are directed to files and stored for later use. The science of log analysis is used for processing the log data ("Log Analysis" 2016). To make the best use of logged data, it is important to have a deep understanding of the structure of the logs and its contents. Since the size of log files can be huge and they can come from multiple sources at the same time, analysis can be done only using a tool. Some of the examples are LOGalyze ("LOGalyze 4," 2013), Splunk (Carasso, 2012) and AWStats ("AWStats log file analyzer 7.4 Documentation," 2015). Some of the challenges of existing tools include limited customization and high cost. Communication devices are hardware devices that transmit digital signals either through wires or wirelessly ("Communication device," n.d.). Walkie-talkie and mobile phones are its examples. This paper proposes an analysis framework that helps developers to point out issues while working with logs of communication devices. The paper has been organized as follows: Section 2 deals with the literature survey on the existing log analyzing tools with a detailed study of their architecture, advantages and disadvantages. Section 3 gives the proposed framework. Section 4 gives the experimental setup. Section 5 gives the conclusion.

2. LITERATURE SURVEY

Research by Hermanowski (2015) talks about Open Source Security Information Management (OSSIM) which is a system built on top of many small and large open source tools to support the

DOI: 10.4018/IJWP.2018010102

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

network administrators in intrusion detection and prevention. It was developed as an initiative of AlienVault Company for the centralized management of their configurations. It consists of four logical components: a server, a database, main framework and sensors. There can be multiple sensors deployed at different physical locations. Roles of the server component include inventory management, policy management, event correlation and task scheduling. The sensor is responsible for vulnerability scanning, network and inventory monitoring. The database stores the collected events. Context for an incident is made from various data sources using logical trees that define the rules. Rules are triggered when at least one of the event is matched. They contain parametres that are either optional or required. Their evaluation sequence is from the root to the leaves. Each rule is assigned a risk value based on their priority and reliability using the formula: Risk = AssetValue * Priority * Reliability / 25. An alarm sets on, each time the threshold value is crossed. Its advantage is that it unifies the common security tools and their management in to a single and consistent user-friendly interface. Its disadvantages include zero documentation for developers due to lack of visibility in the implementation of underlying tools and lack of raw log storage.

Oliner, Adam and Archana (2011) give an overview of various methods of log analysis and its common applications. Applications include optimizing system performance, security applications, prediction, profiling resource utilization and as a logging infrastructure. Some of the challenges include difficulty in using single log file to monitor events in different systems, management of logging process and using the right analytical tool for mining data.

Carasso (2012) explains about Splunk, which is a software for analyzing and monitoring logs using web interface. It finds the cause of system failure by first gathering data from multiple locations and indexing them in a centralized way. This ensures an effortless searching. It can even find out the time of first occurrence of the problem. It also provides data visualization. It is very popular among system and network analysts due to its centralized nature.

Its architecture is explained in ("Splunk Architecture," n.d.). There are two server processes running on the host side: splunkd and splunkweb. Splunkd processes and indexes the data through pipelines, each of which contains a series of processors. Pipelines are single threads configured using XML. Processors are usually C, C++ or Python functions. Pipelines pass data among each other using queues. Splunkweb is a Python-based web user interface. It helps users to search and manage their data easily. It communicates with splunkd via SOAP and the web browser using REST. Splunk's Data Store manage raw data in a compressed format and indexes them. Splunk servers communicate with each other using Splunk-2-Splunk which is a TCP-based protocol. Bundles contain the configuration settings. Modules add new functionalities to Splunk by modifying pipelines and processors. Advantages of Splunk are simplified analysis and troubleshooting, no separate database requirement, reduced costly escalations and faster resolution of issues ("Spluk Advantages - Why to use splunk?," n.d.).

In ("LOGalyze 4" 2013), the main features of LOGalyze, which is a centralized log collection tool, are highlighted. It contains some of the log definitions like Windows 2003 System, Linux standard events, Oracle audit trail and firewall logs. It is compatible with rsyslog, syslog-ng, Lasso and Snare. It creates multidimensional real-time statistics on the basis of individual fields of logs. The reports generated can be exported in to CSV, PDF, HTML or XLS. It can also be scheduled to run periodically.

Balazs Vamos (2013) gives the architecture of LOGalyze. It consists of two main components: a log analyzer engine which is a standalone that runs as a service, collects data and generate automated reports and an RIA web interface for managing the engine, search log data and display reports. Any SOAP client can connect to the engine because it provides a SOAP Web Services interface.

Dukes, Brandon and Piotr (2015) describe a system for parsing raw log data in to structured form, remove duplicates and store in binary format. It speeds up the analysis and reduces the storage. It consists of the following modules: parser module that receives the log data and transforms it in to structured binary format, storage module that stores the parsed data, mapping module that maps between the system identifier and the data storage and a detection module that generates an alert

10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/analysis-framework-for-logs-in-communication-devices/198441

Related Content

Architecture of the Organic.Edunet Web Portal
Nikos Manouselis, Kostas Kastrantas, Salvador Sanchez-Alonso, Jesus Caceres, Hannes Ebnerand Matthais Palmer (2009). *International Journal of Web Portals (pp. 71-91).*
www.irma-international.org/article/architecture-organic-edunet-web-portal/3028

Security Threats in Web-Powered Databases and Web Portals
Theodoros Evdoridis (2007). *Encyclopedia of Portal Technologies and Applications (pp. 869-874).*
www.irma-international.org/chapter/security-threats-web-powered-databases/17978

An Integration Ontology for Components Composition
Sofien Khemakhem, Khalil Driraand Mohamed Jmaiel (2012). *Enhancing Enterprise and Service-Oriented Architectures with Advanced Web Portal Technologies (pp. 142-149).*
www.irma-international.org/chapter/integration-ontology-components-composition/63951

Green Web Services Integration and Workflow Execution within Next Generation CEMIS
Tariq Mahmoud, Barbara Rappand Sebastian van Vliet (2014). *International Journal of Web Portals (pp. 59-74).*
www.irma-international.org/article/green-web-services-integration-and-workflow-execution-within-next-generation-cemis/123174

Do You Need Content Management System?
Jana Polgar (2010). *International Journal of Web Portals (pp. 1-6).*
www.irma-international.org/article/you-need-content-management-system/40314