LogBridge

Overview

This page provides an overview of the Log Analysis tool GroundWork LogBridge.

CONTENTS

RELATED RESOURCES

- RAPID-based Feeders
- Elastic

WAS THIS PAGE HELPFUL?

- Leave Feedback

1.0 About GroundWork Log Analytics

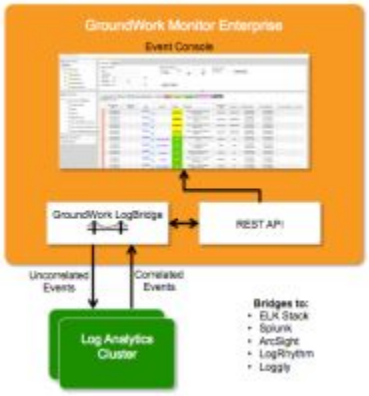
GroundWork's IT OPS Analytics is based on the GroundWork LogBridge and the log analytics product ELK to provide correlations and full compliance reporting for HIPAA, PCINet and Sarbanes-Oxley is available from the GroundWork Monitor custom BIRT Reports. The GroundWork LogBridge connects the monitoring system with the log analytics product ELK. The ELK stack consists of Elasticsearch, Logstash, and Kibana. Although they've all been built to work exceptionally well together, each one is a separate project that is driven by the open-source vendor *Elastic*, which itself began as an enterprise search platform vendor.

- **Elasticsearch** is a distributed, open source search and analytics engine, designed for horizontal scalability, reliability, and easy management. It combines the speed of search with the power of analytics via a sophisticated, developer-friendly query language covering structured, unstructured, and time-series data.
- **Logstash** is a flexible, open source data collection, enrichment, and transportation pipeline. With connectors to common infrastructure for easy integration, Logstash is designed to efficiently process a growing list of log, event, and unstructured data sources for distribution into a variety of outputs, including Elasticsearch. Redis is a queue, a FIFO RAM buffer and ideally it is always empty providing a queuing for Logstash data prior to indexing and sending data to Elasticsearch.
- **Kibana** is an open source visualization platform that allows you to interact with your data through powerful graphics. From histograms to geomaps, Kibana brings data to life with visuals that can be combined into custom dashboards that help you share insights from your data.

LogBridge Concept

- If there is more than one event correlator, there is incomplete correlation
- Log data without correlation is useless, so log analytics systems have good correlators
- Delivering high value unified monitoring events to the log analytics system makes event correlation complete and log analytics better
- Delivering correlated events back to GroundWork for event management, unified information display, alert management, cross reference to other monitoring data and integration with other systems such as service desk, the best possible event management process is obtained

Figure: LogBridge Concept



LogBridge Data Flow and Process Flow

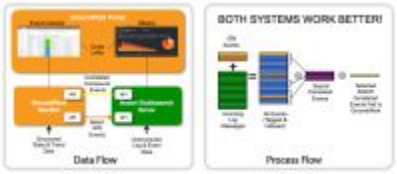
The LogBridge data flow between GroundWork and any Log Analytics product (e.g. Splunk, ELK, ArcSight, Loggly, etc.) is shown in these parallel diagrams.

By ensuring that all event data collected within the entire organization is collected within the Log Analytics system, and that correlated compound events are returned to the GroundWork Event Console for management, GroundWork's LogBridge ensures that both GroundWork and the Log Analytics function will work better that either system by itself.

If you don't have a Log Analytics system in place, GroundWork can provide and support the leading open source log analytics software which is consists of Elasticsearch, LogStash, and Kibana or (ELK) to be used for this purpose unless you prefer to provide a different Log Analytics system in which case GroundWork will adapt its LogBridge for this purpose. LogBridge and the ELK stack are included within the GroundWork subscription at no added cost.

Kibana is the user interface to Elasticsearch which is used to create and maintain correlation rule sets including those used to comply with Sarbanes Oxley, HIPAA, PCINet, and other regulatory requirements for log analysis. Elasticsearch is the tagged noSQL database that provides scale out capacity for unstructured data like log messages.

Figure: LogBridge data and process flow



GroundWork Monitor Architectural Overview

As you can see, the **Log Analytics Collection and Storage** system feeds into the **GroundWork Monitor Parent**. The **GroundWork Monitor Parent** portal contains a link to the **Kibana** interface allowing for a single pane of glass for monitoring and management of log events. Additionally, GroundWork events themselves are fed into the Log Analytics system for event correlation.

Figure: GroundWork Architectural Overview

GroundWork LogBridge and Forensics/Compliance Cluster

This provides another view of the GroundWork LogBridge showing two way communication between it and the Forensics/Compliance cluster.

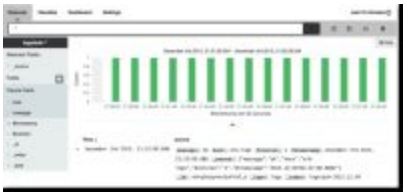
The Curator module selects source data that has regulatory/compliance significance to be written to the Archive Cluster using slow inexpensive storage. Note the scalability of Compliance and Forensics Clusters as a result of the scale out capabilities of Hadoop. All compliance related events and correlated events are returned to GroundWork for use in Incident Management and Reporting processes.

Figure: LogBridge and Forensics/Compliance

2.0 Viewing Kibana

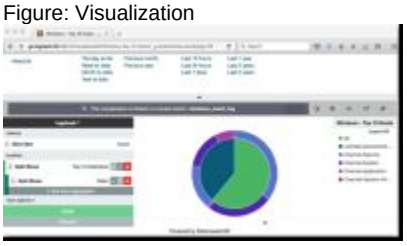
Centralized Log Management - Log Analysis and Troubleshooting

Figure: Centralized Log Management



Kibana Visualization

Figure: Visualization



Kibana Dashboard

Figure: Dashboard