The best Event log software and analysis tools

Log is a useful source of information, because it contains records of all actions taken on the network. In fact, when properly exploited, logs can provide detailed information about network performance, usage and management.

In addition, this analysis will certainly help to make the right decisions in important areas, such as security.

However, reading log files is not easy because they come from different devices and in different formats. Reading this information to identify and solve problems can take days. During that time, network loopholes will continue to create potential risks. In addition, such manual analysis can most likely lead to finding the wrong cause and giving wrong handling measures.

To avoid these problems, an event log analysis software is extremely necessary. These specialized tools collect information from different devices and analyze them to provide detailed, meaningful and actionable data. In addition, it helps IT administrators to operate more efficiently, can focus on output data instead of having to choose between a lot of raw and unreadable log data.

Now, readers have understood the importance of log analysis software. The following is a list of the best software and tools on the market today.

The best Event log analysis tools

1. Loggly Analyzer
2. Solarwinds Log & Event Manager
3. ManageEngine EventLog Analyzer
4. InsightOps
5. LOGalyze
6. Splunk

Loggly Analyzer

There are several advantages to Loggly's solution, chief amongst which is its intuitive user interface, which, in combination with its speed, makes it a supremely efficient log analyzer for use in modern operating environments.

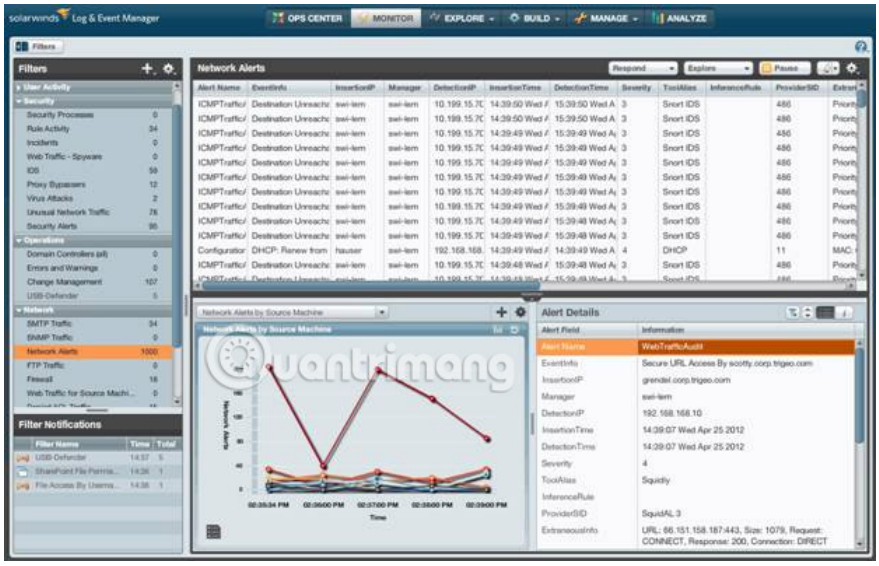
Powered by the cloud, it can manage and analyze log data from servers and apps alike, all within the same UI, which creates a unified approach that will make monitoring less of a chore. Key features include:

1. Proactive monitoring via alerts that pinpoint infrastructural issues in an instant
2. Safe and secure log management to comply with relevant regulations

3. DevOps functionality to ensure that users can collaborate with colleagues seamlessly
4. Detailed diagnostics capabilities allow you to identify errors and troubleshoot them in less time than usual

With a free trial available, Loggly is another analyzer solution that you can put through its paces without needing to make any kind of financial commitment.

Solarwinds Log & Event Manager



Solarwinds Log & Event Manager software collects information from different devices, focuses all on a single log file and links these data to give important details like event name, date of occurrence out and severity.

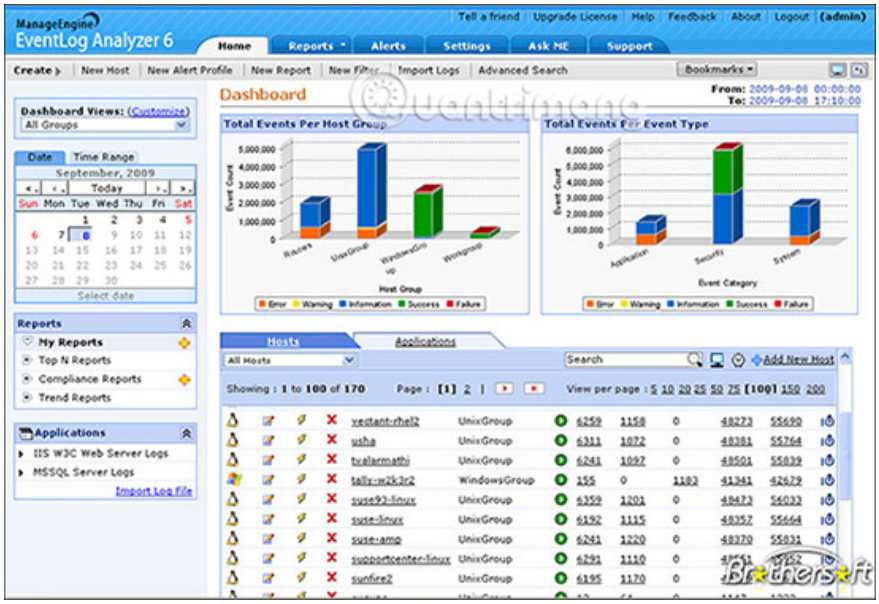
The outstanding feature of this software is that it not only analyzes log files, but also learns from past events to warn users before the same thing happens. Such a proactive approach will definitely store a lot of information about data violations.

Other features include:

1. Improved security
2. Detect suspicious activities and give automated feedback
3. Comes with advanced security measures like LEM, SSO, smart card integration and more
4. Link events and report them in real time
5. Provide corrective solutions in real time
6. Monitor file integrity
7. Comes with USB monitoring feature
8. Provides security against external and internal threats
9. Easy to use interface
10. Centralized logs make it easy to troubleshoot
11. Give a warning about suspicious activities in the feed about possible threats
12. Support more than 1,200 devices, applications and systems

Price: Free trial for the day.

ManageEngine EventLog Analyzer



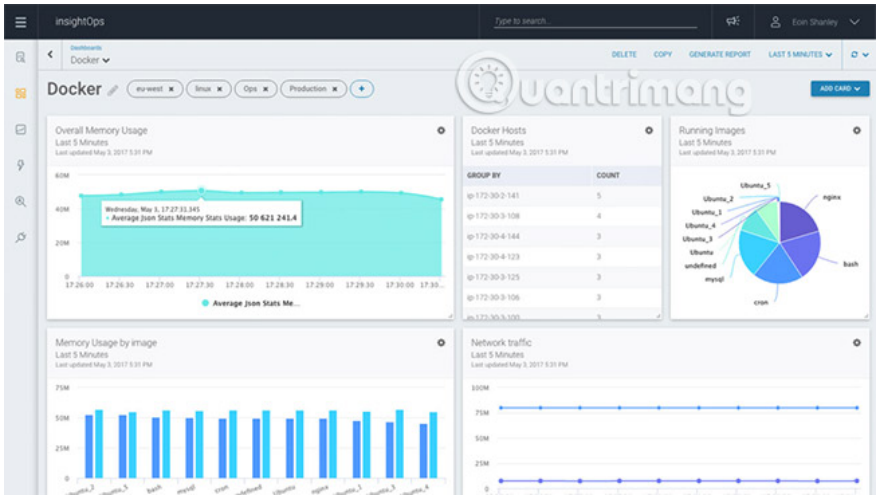
ManageEngine EventLog Analyzer collects data from various sources and saves them in a central repository. This stored data is timestamped and hashed to ensure that the records are not tampered with.

Its main features include:

1. Allow log import from remote server via HTTPS or FTP
2. Follow the rules of various regulatory agencies like HIPAA
3. Allows users to create flexible reports based on different criteria
4. Works well with over 700 devices from more than 30 providers
5. Comes with graphic dashboard containing icons
6. Comes with PostgreSQL by default, but users can also choose MySQL or MS SQL
7. Collect data from data sources with and without agents
8. Point out threats with 70 innovative event correlation rules
9. Comes with advanced features like privileged user monitoring, file integrity monitoring, real-time event linking and more
10. Provide search options through logs to get specific information

EventLog Analyzer has three versions: Free, Premium and Distributed. Free version (free) supports up to 5 log sources, Premium version (premium) supports 10 to 100 source logs and Distributed version supports unlimited number of log sources. The Premium version costs $ 599 , while Distributed version is priced at $ 2,495 .

InsightOps



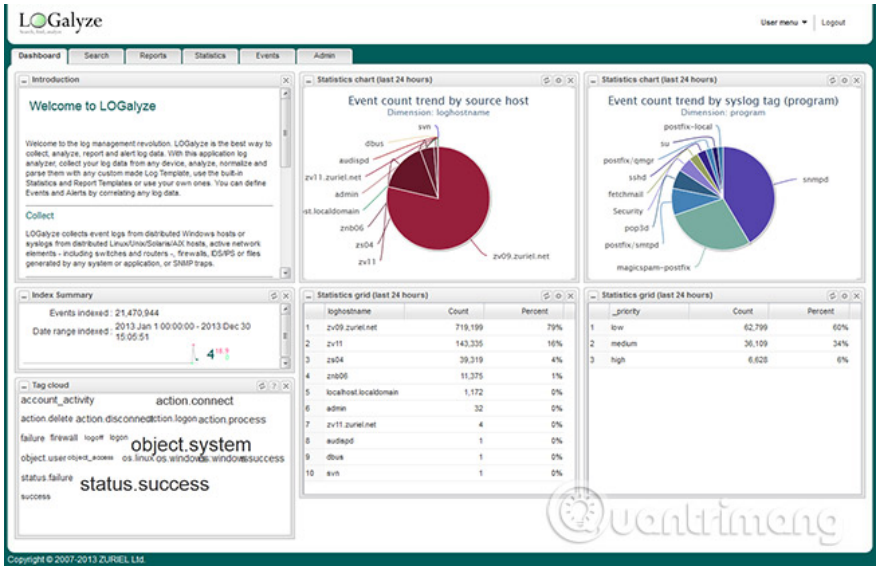
InsightOps is a cloud-based log monitoring and analysis tool that collects and links log data from different devices for fast and detailed analysis. Software-as-a-service product (SaaS) - software in this form of service helps log data to be accessible and useful for different parts of an enterprise.

It comes with a wide range of features to provide valuable log information in today's distributed environment. Some outstanding features of this program are:

1. Works in any data format - including JSON to plain text
2. Organize all records in a centralized location
3. Comes with advanced search features that allow users to search log data based on key words, key value pairs or regular expression patterns.
4. Provides the option to create custom tags to easily identify important events
5. Transfer logs and application data directly for real-time analysis
6. Storage and reporting features are designed to meet compliance requirements
7. Accept data from all environments and in all formats
8. SQL-Like Query Language - SQL-like Query Language - (LEQL) performs advanced calculations like average, sum, min, max, percentile, etc.
9. Provide data visualization for better analysis
10. Graphic dashboards come with column charts, pie charts, line charts, etc. to make it easier to understand data analysis
11. Provides a variety of alerts such as sample-based alerts, inactive alerts, unusual detection and comprehensive notifications
12. Comes with powerful APIs to make the most of the platform
13. Good integration with existing tools like Slack application, OpsGenie and iPhone.

InsightOps has 5 packages - free, starter, pro, team and enterprise. The Starter package starts at $ 39 / month, the Pro package is $ 99 / month and the Team package is $ 265 / month. Enterprise packages are designed to meet the needs of every business.

LOGalyze



LOGalyze is an open source log analysis software, support for UNIX, Linux, Windows and other operating systems. This software collects and analyzes data to identify sources, severity, data types and store them in archives. It analyzes data and provides warnings and reports on compliance with rules.

Important features of LOGalyze are:

1. Create multi-dimensional statistics to help users understand details about events
2. Jute is open source software, free and supported by a large community
3. Analyze all log files with default or custom definitions
4. Allow users to browse or search logs using the GUI
5. Comes with an option to transfer secure logs to syslog devices.
6. Warn users when there are any events that match the specified criteria.
7. Compatible with syslog, rsyslog, syslog-ng and Snare
8. Integrated with AHR ticketing system to better manage incident reporting
9. Create reports that comply with the principles of various regulatory agencies such as HIPAA, PCI DSS and PSZAF-HPT
10. Provides real-time correlations and creative rules.

Splunk

Splunk is a big name in the field of log management. This log analysis software collects, stores, indexes, visualizes, analyzes and reports data generated from any computer and in any format.

Some of its important features are:

1. Indexing data regardless of format or location.
2. Only apply the structure and schema at the time of search, so users can analyze the data without limitation
3. Use the Splunk Search Processing Language exclusively for search queries
4. Provides the option to zoom in and out of timeline in the scrolling time window
5. Provide over 140 commands to perform searches, calculate data and search for specific criteria.
6. Helps easily link events and activities based on time, location or search results.
7. Comes with a unique Pivot interface that makes it easy to discover and share detailed information.
8. Custom reports and dashboards make it convenient and intuitive
9. Help create alerts in real time, so automatic activation notifications can be emailed.
10. Users can access Splunk software through any web-based browser.
11. Easy setup and onboarding (orientation) of data.

Splunk has 3 versions: Splunk Light is ideal for a small IT environment and costs $ 75 / month. Splunk Cloud is a cloud-based service with a starting price of $ 90 / month, and Splunk Enterprise is a complete solution for large businesses and the price depends on the amount of data sent to the platform. platform. Both Splunk Cloud and Splunk Light have a free trial period.

Refer to Splunk.

Event log analyzers are an essential tool for all networked devices today. These log analysis software collects data from different sources and converts them into readable and searchable formats, so users can track events in their networks.

The article listed some of the best products at the moment. Let us know which of these software is your favorite option in the comment section below!

Good luck!