LOGalyze 4

The best way to collect, analyze, report and alert log data

Welcome to the log management revolution. LOGalyze is the best way to collect, analyze, report and alert log data. With this application log analyzer, collect your log data from any device, analyze, normalize and parse them with any custom made Log Template, use the built-in Statistics and Report Templates or use your own ones. You can define Events and Alerts by correlating any log data.

Collect

LOGalyze collects event logs from distributed Windows hosts or syslogs from distributed Linux/Unix/Solaris/AIX hosts, active network elements - including switches and routers -, firewalls, IDS/IPS or files generated by any system or application, or SNMP traps.

Parse, Store

LOGalyze identifies the collected logs, classifies them by source host, severity, type, splits them into fields and stores for efficient analyzing.

Analyze

Analyzer engine of LOGalyze includes value added capability of analyzing log data. Offers multi-dimensional statistics and correlated event detection real-time. Unique integration with our AHR ticketing system provides straightforward incident management and review capabilities.

Report, Alert

LOGalyze includes predefined compliance reports and possibility of making custom reports based on parsed data. With plug-in style Alert modules it notifies users or other systems when an event matching one or more specified criteria is generated.

Major features

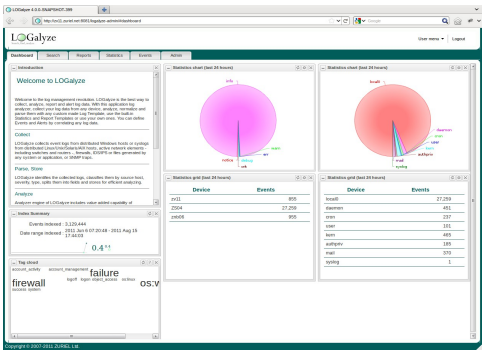
Centralized log collection for everybody

LOGalyze collects, parses, indexes and stores log data from any device, OS or application. With LOGalyze, you can:

- Process log data at a high rate
- Parse any log row with built in or custom made Log Templates
- Ability to analyze custom business application logs
- Browse or search logs with a web based administration GUI like with Google
- Create multi dimensional statistics real-time based on individual fields of log
- Securely transport log data to other LOGalyze engines or syslog devices
- Export reports or lists into CSV, XLS, PDF or HTML
- Alert and notify users or other systems when an event matching one or more specified criteria is generated.
- Compatible with rsyslog, syslog-ng, Lasso, Snare
- Connect remotely to SOAP API service
- The AHR ticketing system provides powerful tool closing your open incidents more quickly.

Log definitions

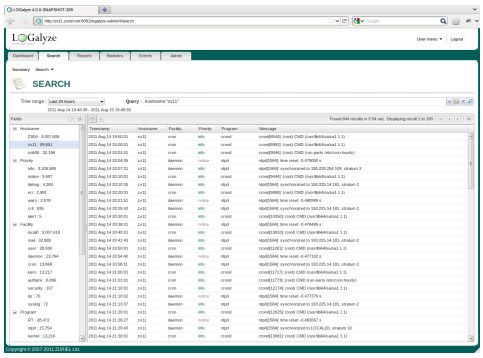
- Windows System, Security, Application event logs
- Firewall logs
- Linux standard events
- OS Audit Subsystem logs (LAuS, AIX audit log, Solaris audit log)
- Network devices (Cisco, Juniper, etc.)
- Oracle audit trail
- System software logs (Apache, Postfix, Sendmail, Squid, etc.)
- Ability to parse custom business application logs



Compliance Audits & Reports

LOGalyze provides reports to help comply with various regulatory acts like:

- HIPAA - Health Insurance Portability And Accountability Act
- PCI DSS - Payment Card Industry Data Security Standard
- Sarbanes-Oxley Act
- PSZAF - HPT



The above reports for various regulatory compliance audits are automatically generated as soon as logs are collected. You can save these reports in multiple report formats, like HTML, PDF or CSV, and schedule them to run periodically, and even get them emailed to multiple users.

More information

Visit http://www.logalyze.com/ for more information.
Contact information can be found at:
http://www.logalyze.com/about-us

LOGalyze
Search, find, analyze